

2013

# Assessing and mitigating information security risk in Saudi Arabia

Abdulaziz Saad Alarifi

*University of Wollongong, [aaa296@uowmail.edu.au](mailto:aaa296@uowmail.edu.au)*

**Assessing and Mitigating Information Security Risk  
in Saudi Arabia**

A thesis submitted in fulfilment of the  
requirement for the award of the degree

**DOCTOR OF PHILOSOPHY**

From

UNIVERSITY OF WOLLONGONG

by

**ABDULAZIZ SAAD ALARIFI**

School of Information Systems and Technology

2013

## **Thesis Certification**

I, Abdulaziz Saad Alarifi, declare that this thesis, submitted in fulfilment of the requirements for the award of Doctor of Philosophy, in the School of Information Systems and Technology, University of Wollongong, is wholly my own work unless otherwise referenced or acknowledged. The document has not been submitted for qualifications at any other academic institution.

Abdulaziz Saad Alarifi

15 May 2013

## **Abstract**

While the Web, cell phone ‘apps’ and cloud computing put a world of information at our fingertips, that information is under constant threat from cyber vandals and hackers. This thesis examines the level of Information Security Awareness (ISA) among the general public and Information Security (InfoSec) practices among IT departments in organizations in Saudi Arabia. This examination was conducted using an online survey that was based on instruments produced by organizations specializing in information security, such as the Malaysian Cyber Security Organization, the Excellence of Information Assurance Centre, and Alelm organization in Saudi Arabia. Due to cultural constraints, it would ordinarily be difficult to gather data from female respondents in Saudi Arabia, however, the use of an online survey helped to collect the data successfully.

The ISA survey attracted 462 respondents from the general public and the InfoSec survey attracted 124 respondent organizations. Results indicated that information security awareness and practices in Saudi Arabia are quite low. Several of the areas of weakness in InfoSec appear to be related to the level of censorship or the patriarchal and tribal nature of Saudi culture.

A new information security model (InfoSec CAP) has been designed based on the findings of the research results. This model provides appropriate solutions and improvements for ISA and InfoSec practices in Saudi Arabia. It will also help embed the identified concepts in information security practice globally.

## **Acknowledgements**

This research would not be complete without the help of many people.

I would like to thank my two supervisors Dr Holly Tootell and Associate Professor Peter Hyland for their help, guidance and support throughout this thesis. They have encouraged me to pass all research challenges and helped me to become a better researcher.

I thank all my family members. To my parents, Saad and Sarah, and brothers and sisters in Saudi Arabia for their encouragement and patience while I was completing my thesis so far from them.

I thank my wife Maha, for her patience, kindness, reassurance, and love at every stage of this thesis.

I have great respect for the assistance of Dr Alison Freeman for the proof-reading of my thesis. Also, I would like to thank all the educational institutions that helped me to complete my thesis. Thank you to King Saud University for their funding of the scholarship for this research and the Center of Excellence in Information Assurance (CoEIA) in Saudi Arabia for their help during the data collection phase. Thank you to University of Wollongong for the great help and services during my study.

Finally, I would like to thank all my friends who supported me and were interested in my progress. Thank you.

## **Publications**

Alarifi, A., H. Tootell and P. Hyland 2012, 'Information Security Awareness in Saudi Arabia' in *Proceedings of the 2012 Information Recourses Management (IRM'2012)*, Vienna, Austria, May 21-23.

Alarifi, A., H. Tootell and P. Hyland 2012, 'A Study of Information Security Awareness and Practices in Saudi Arabia' in *Proceedings of the Second International Conference on Communications and Information Technology (ICCIT'2012)*, Hammamet, Tunisia, June 26-28.

## **List of Acronyms**

CAP	Cultural Adaptation Process
DoS	Denial of Service
HCC	Highly-Censored Countries
ID	Identification
InfoSec	Information Security
ISA	Information Security Awareness
IS	Information System
IT	Information Technology
KPMG	Klynveld Peat Marwick Goerdeler

## Table of Contents

Thesis Certification .....	i
Abstract .....	ii
Acknowledgements .....	iii
Publications .....	iv
List of Acronyms .....	v
Table of Contents .....	vi
List of Tables.....	xii
List of Figures .....	xvii
<i>Chapter 1</i> Research Introduction .....	1
1.1 Introduction .....	1
1.2 Background of study .....	2
1.3 Research objectives .....	5
1.4 Methodology .....	6
1.5 Significance of the study .....	7
1.6 Research limitations .....	8
1.7 Structure of the thesis.....	9
<i>Chapter 2</i> Literature Review.....	11
2.1 Introduction .....	11
2.1.1 Information quality.....	12



2.1.1.1	Confidentiality .....	13
2.1.1.2	Integrity .....	13
2.1.1.3	Availability.....	14
2.1.2	Information threats .....	14
2.1.2.1	Accidental threats.....	16
2.1.2.2	Deliberate threats .....	17
2.1.2.3	Contributory threats .....	18
2.1.3	Consequences of security failures.....	19
2.1.4	Risk management .....	20
2.1.4.1	Risk identification .....	22
2.1.4.2	Risk analysis and evaluation .....	23
2.1.4.3	Risk control .....	24
2.1.5	Information security policies and standards.....	27
2.2	Cultural component of information security .....	31
2.2.1	Legal systems .....	32
2.2.1.1	Data protection law .....	34
2.2.2	Censorship.....	34
2.2.3	Impact of culture on information security.....	36
2.3	Saudi Arabia.....	39
2.3.1	The Culture of Saudi Arabia .....	40
2.3.2	Information use and data protection in Saudi Arabia.....	42

2.3.2.1	History of the Internet .....	42
2.3.2.2	Internet use and impact of culture .....	43
2.3.2.3	Data protection law .....	44
2.3.3	Information security in Saudi Arabia .....	44
2.4	Justification for the study .....	51
2.5	Conclusion .....	52
<i>Chapter 3</i>	<i>Research Methodology .....</i>	<i>53</i>
3.1	Introduction .....	53
3.2	Overview of research methodology .....	53
3.2.1	Quantitative methods .....	54
3.2.1.1	Surveys .....	54
3.2.1.1.1	Information Security Awareness (ISA) survey .....	55
3.2.1.1.2	Information security survey for organizations .....	57
3.3	Research methodology framework .....	59
3.4	Data analysis .....	62
3.5	Conclusion .....	63
<i>Chapter 4</i>	<i>Results and discussion for Information Security Awareness.....</i>	<i>64</i>
4.1	Introduction .....	64
4.2	Background of participants .....	64
4.2.1	Response rate and demographics .....	64
4.2.2	Education.....	66

4.2.3	Sector type and working status .....	66
4.2.4	Living area .....	69
4.3	General Information security practices .....	70
4.3.1	Internet usage .....	70
4.4	Information security issues .....	71
4.4.1	Information security practices.....	71
4.4.1.1	Passwords.....	73
4.4.1.2	Threat awareness.....	75
4.4.2	Information security tools .....	76
4.4.2.1	Backups .....	78
4.4.2.2	Safeguarding personal information.....	79
4.4.2.3	Reporting security .....	80
4.4.3	Privacy level.....	82
4.5	Preferences for promotion of Information Security Awareness .....	83
4.6	Chi-Square Relationships Tests .....	85
4.7	Information Security Awareness studies for comparison purposes .....	88
4.7.1	Information threats and security .....	89
4.7.2	Password practices .....	90
4.7.3	Reporting of security incidents .....	90
4.8	Conclusion .....	91
<i>Chapter 5</i> Results and discussion for Information Security Practices in Saudi Arabian		

Organizations .....	93
5.1 Introduction .....	93
5.2 Background of organizations .....	93
5.3 Information security laws standards and policies in organizations.....	99
5.3.1 Information security laws in organizations .....	99
5.3.2 Information security standards in organizations .....	103
5.3.3 Information security policies in organizations .....	105
5.4 Information assurance in the organization .....	107
5.4.1 Information assurance tool/measures in the organization.....	109
5.4.2 Information security risks in organizations.....	125
5.4.2.1 Culture threat.....	128
5.5 Promotion preferences .....	132
5.6 Chi-Square Relationship Tests .....	135
5.7 Conclusion .....	144
<i>Chapter 6 Summarised Findings Directly Related to Model.....</i>	<i>147</i>
6.1 Research contributions and recommendations.....	147
6.1.1 The Proposed InfoSec CAP Model .....	147
6.1.1.1 Structure of InfoSec CAP model .....	148
6.1.1.1.1 Framework Phase .....	150
6.1.1.1.2 Design Phase .....	151
6.1.1.1.3 Implementation Phase .....	153

6.1.1.1.4 Evaluation Phase .....	155
6.2 Conclusion .....	156
<i>Chapter 7 Conclusion</i> .....	158
7.1 Introduction .....	158
7.2 Research Scope .....	158
7.2.1 Links to Earlier Findings.....	158
7.3 Significance of the research .....	159
7.4 Limitations of the findings .....	159
7.5 Future research .....	160
7.6 Conclusion .....	161
References .....	162
Appendix A: Survey Questions for Public Awareness on Information Security in Saudi Arabia (English).....	178
Appendix B: Survey Questions for Public Awareness on Information Security in Saudi Arabia (Arabic) .....	187
Appendix C: Information Security and Risk Management Policies Survey for IT Department in Saudi Arabia (English).....	196
Appendix D: Information Security and Risk Management Policies Survey for IT Department in Saudi Arabia (Arabic) .....	208
Appendix E: ISA Chi-Square Relationships Tests .....	1
Appendix F: InfoSec Chi-Square Relationships Tests.....	36

## List of Tables

Table 1.1 Incidence of information attacks – highest 20 countries (Kaspersky Lab 2010, 2011) .....	3
Table 1.2 Thesis structure .....	9
Table 2.1 Information threats – percentage effect 2005-2010 (CSI Computer Crime & Security Survey 2011).....	16
Table 2.2 Countries that use BS7799 standard .....	29
Table 2.3 Incidence of information attacks – highest 20 countries (Kaspersky Lab 2010, 2011) .....	37
Table 2.4 Number of Internet users in Saudi Arabia (CITC 2011).....	43
Table 4.1 Participant gender .....	65
Table 4.2 Participant age.....	65
Table 4.3 Participant education level .....	66
Table 4.4 Participant organization type .....	67
Table 4.5 Participant working status.....	67
Table 4.6 Participant industry sector.....	68
Table 4.7 Participant living area .....	69
Table 4.8 Internet use.....	70
Table 4.9 Purpose of Internet use and time spent .....	71
Table 4.10 Device types.....	72
Table 4.11 Device security.....	72
Table 4.12 Device information security.....	73

Table 4.13 Use of passwords on devices .....	73
Table 4.14 Password security.....	74
Table 4.15 Frequency of password change .....	74
Table 4.16 Incidence of password sharing .....	75
Table 4.17 Awareness of information threats .....	76
Table 4.18 Use of protection software .....	77
Table 4.19 Software type and most recent update .....	77
Table 4.20 Use of private web mail for professional purposes.....	78
Table 4.21 Data backup frequency.....	78
Table 4.22 Provision of personal information in response to unsolicited request .....	79
Table 4.23 Security incident report awareness .....	81
Table 4.24 Participant information stolen or hacked .....	82
Table 4.25 Importance of privacy online .....	82
Table 4.26 Responsibility for digital information privacy.....	83
Table 4.27 Sources for learning about information security.....	84
Table 4.28 Communication mechanisms for promoting ISA .....	84
Table 4.29 Chi-Square Test Results.....	86
Table 4.30 Comparison of information security threat awareness.....	89
Table 4.31 Comparison of information security control software use.....	90
Table 4.32 Password practices .....	90
Table 4.33 Comparison of incident security reporting awareness .....	91

Table 5.1 Nature of organization .....	94
Table 5.2 Sector of organization .....	95
Table 5.3 Size of organization .....	95
Table 5.4 Age of organization.....	96
Table 5.5 Presence of IT department in organization .....	97
Table 5.6 Organization IT budget .....	98
Table 5.7 Organization information security budget .....	98
Table 5.8 Availability of staff who are knowledgeable about information security in organization.....	98
Table 5.9 Data protection or information security law in organizations.....	100
Table 5.10 Comfort level with data protection law.....	101
Table 5.11 Quality of data protection law in organizations.....	101
Table 5.12 Comprehensiveness and appropriateness of data protection law in organizations .....	102
Table 5.13 Power of data protection or information security law in organizations.....	103
Table 5.14 Organization distribution according to whether any information security standards are applied .....	104
Table 5.15 Future plans to apply information security standards .....	104
Table 5.16 Perceived sense of security with the application of information security standards.....	105
Table 5.17 Distribution of employee respondents according to perceived existence of personnel tasked with ensuring adherence to adopted information security standards.....	105



Table 5.18 Existence of information security policy in organization .....	106
Table 5.19 Organization enforcement of information security policy .....	106
Table 5.20 Organization risk assessment process .....	107
Table 5.21 Organization procedures and regulations for account creation and management .....	108
Table 5.22 Organization data backup and recovery policy .....	108
Table 5.23 Organization security incident reporting plan .....	109
Table 5.24 Vulnerability assessment in organizations .....	109
Table 5.25 Organization password practice .....	111
Table 5.26 Implementation of two-factor authentication in organizations .....	112
Table 5.27 Organization firewall systems .....	112
Table 5.28 Organization wireless connection restrictions .....	114
Table 5.29 Organization policies on restricting access to specific websites .....	115
Table 5.30 Operation systems and software updates in organizations .....	116
Table 5.31 Strength of anti-virus software in organizations .....	117
Table 5.32 Intrusion detection software in organizations .....	118
Table 5.33 Data encryption systems in organizations .....	120
Table 5.34 Server room physical security in organizations .....	121
Table 5.35 Restrictions on the use of input devices in organizations .....	122
Table 5.36 Information security training offered to employees in organizations .....	124
Table 5.37 IT department staff distribution according to intent to obtain information security certification .....	124

Table 5.38 Computer downtime due to viruses in organizations.....	126
Table 5.39 Incidence of hacker attack on organization website .....	126
Table 5.40 Incidence of hacker attack on organization's information systems .....	127
Table 5.41 Other information security risks faced in organizations .....	127
Table 5.42 Information security and privacy risks involving tribal societies in Saudi Arabia.....	128
Table 5.43 Information security risks in terms of illegal acquisition of information utilizing tribal connections.....	129
Table 5.44 Practice of hiring unqualified relatives .....	130
Table 5.45 Information security risk in relation to women wearing veils .....	130
Table 5.46 Information security risk in relation to lack of picture on identification cards used by Saudi Arabian women.....	131
Table 5.47 Refusing permission to issue picture identification cards to women in Saudi Arabia.....	131
Table 5.48 Challenges of applying information security standards in organizations ...	132
Table 5.49 Obstacles faced in acquiring certifications in information security.....	133
Table 5.50 Benefits that would motivate respondents to acquire additional certification in information security .....	134
Table 5.51 Promotions that would motivate respondents to acquire additional certification in information security.....	134
Table 5.52 Nature of organizations vs InfoSec practices Chi-Square test.....	135
Table 5.53 Organization sectors vs InfoSec practices Chi-Square test.....	136
Table 5.54 Organization size vs InfoSec practices Chi-Square test.....	141

## List of Figures

Figure 2.1 Conceptual framework.....	12
Figure 2.2 Information Security Triangle (Afyouni 2006) .....	13
Figure 2.3 InfoSec threat types .....	15
Figure 2.4 Risk management process (Mantel et al. 2001).....	21
Figure 2.5 Information security policy location (SANS 2010).....	28
Figure 2.6 World map showing countries' basis of law (ICT Regulation Toolkit Organization 2010).....	33
Figure 2.7 World map showing countries' data protection laws (Banisar 2011).....	34
Figure 2.8 World map showing countries' level of censorship (Green & Karolidies 2005) .....	35
Figure 2.9 Filtering types in highly-censored countries (Deibert et. al 2008) .....	36
Figure 2.10 Most spammed countries (Symantec Lab 2011) .....	39
Figure 2.11 Location of Saudi Arabia (Wilson & Douglas 1994) .....	40
Figure 2.12 SETA program.....	46
Figure 2.13 Factor for implementation and adopting IS culture and practices in Saudi Arabia (Alnatheer & Nelson 2009) .....	47
Figure 2.14 Information systems implementation in King Fahd University (Albarrak 2014) .....	47
Figure 2.15 McCumber INFOSEC Model (Maconachy, et al. 2001).....	49
Figure 3.1 Research methodology framework .....	60
Figure 4.1 Participant job position .....	69

Figure 4.2 Participant location .....	70
Figure 4.3 Provision of personal information in response to unsolicited request by gender.....	80
Figure 4.4 Security incident reporting by sector.....	81
Figure 5.1 Vulnerability assessment in organizations frequency histogram.....	110
Figure 5.2 Organization password practice frequency histogram.....	111
Figure 5.3 Organization firewall systems frequency histogram .....	113
Figure 5.4 Organization Internet access restrictions frequency histogram .....	114
Figure 5.5 Organization policies on restricting access to specific websites frequency histogram.....	115
Figure 5.6 Strength of anti-virus software in organizations frequency histogram.....	117
Figure 5.7 Intrusion detection software in organizations frequency histogram.....	119
Figure 5.8 Data encryption systems in organizations frequency histogram .....	120
Figure 5.9 Server room physical security in organizations frequency histogram.....	121
Figure 5.10 Restrictions on the use of input devices in organizations frequency histogram.....	123
Figure 6.1 InfoSec CAP Model for Cultural Adaptation Process.....	149
Figure 6.2 Framework Phase Structure .....	150
Figure 6.3 Design Phase.....	152
Figure 6.4 Implementation Phase.....	153
Figure 6.5 Evaluation Phase.....	156

# **Chapter 1 Research Introduction**

## **1.1 Introduction**

The World Wide Web, mobile computing and Cloud Computing have changed the world by providing access to a wide range of information, anytime and anywhere (Afyouni 2006). Despite the advantages they provide, the development of such technologies also allows new techniques for abusers to misuse or destroy information (Bragg et al. 2004). These ‘cyber vandals’ can illegally access or destroy online information using techniques such as malware programs (e.g. viruses, trojans and worms), hacking or denial of service (DoS) attacks (Easttom 2006).

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

Although this is generally well-understood, some countries do not appear to have understood either the devastating risks of information security (InfoSec) threats or the importance of ISA. This is particularly true in countries that are highly-censored, such as Saudi Arabia. Indeed, Saudi Arabia’s level of information security risk is among the highest internationally. This study aims to understand ISA and InfoSec practice, specifically in the context of high-censored countries such as Saudi Arabia.

This chapter provides an overview of the thesis and defines the terms related to information security. An explanation of the research problem is provided. A description of the research methodology that will be used is also introduced. Finally, a discussion of

the significance of the thesis is provided, the research limitations are presented and the thesis structure is outlined.

## **1.2 Background of study**

Information is regarded as a valuable commodity; in fact, the international finance sector is almost entirely involved in processing and transferring information (Bandi & Russell 2004). However, this valuable commodity is under constant threat. Information threats can be categorised as accidental or unintentional, such as natural disasters; deliberate or intentional, such as malware attacks, denial of service (DoS) attacks and hacking or other intrusions; or contributory or instrumental, such as password issues or failure of backup (Stulz 2003; Afyouni 2006; Easttom 2006). Categorisations allow threats to be identified and managed more effectively. For example, as an accidental or unintentional threat, the risk of natural disasters can be mitigated by storing redundant copies of information in widely dispersed locations so that the risk of all copies being destroyed or damaged is incredibly low.

Human attacks pose the greatest threat to information because these attacks are intentional and the mechanisms for conducting such attacks become more sophisticated every day. Human attacks typically rely on another unsuspecting human agent to allow the attack. Malware attacks rely on people opening email attachments or using contaminated portable devices such as USB drives on multiple computers. Hackers rely on people leaving computers with no or inadequate passwords. DoS attacks use computers that are unprotected by firewalls as intermediaries to send billions of bogus transactions to a targeted computer, thereby denying it the processing power or the communications bandwidth to carry out its intended purpose.

To reduce the incidence and severity of human attacks, it is necessary to raise the levels of ISA and InfoSec within a specific organization and in the general public. Information security policies are the foundation that supports the security of information resources in an organization. Organizations have started to invest in ongoing developments in technological security to face the growing challenges in this area (Ferrari & Thuraisingham 2006; Peltier 2004; Knapp et. al 2006). There are several internationally recognized standards for information security management including BS7799 and

ISO/IEC 17799 (Saint-Germain 2005). Each of these standards is presented in more detail in Chapter 2. Information security policies and procedures are commonplace in most organizations. They seek to give employees clear guidelines on what they should or should not do to increase the security of corporate information. While the general public is also becoming more aware of information security threats, this is not the case in all countries, as shown in Table 1.1.

In 2011, the Kaspersky Lab, a highly-respected information security specialist, reported the following statistics about information security and targeted attacks around the world (Kaspersky Lab 2011). Their statistics “are based on data obtained from Kaspersky Lab products installed on users' computers worldwide and was acquired with the full consent of the users involved” (Kaspersky Lab 2011) . Table 1.1 shows that 86.3% of the known information attacks occurred within twenty countries in 2009. In 2010, the top twenty countries accounted for 82% of the known information attacks internationally.

**Table 1.1 Incidence of information attacks – highest 20 countries (Kaspersky Lab 2010, 2011)**

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

When reflecting on these statistics it is important to understand that the number of attacks will be, to some extent, dependent on the number of people using computers and having access to the Internet within each country. For example, Italy has more than double the number of attacks recorded in Thailand, even although the populations of the

two countries are similar. However, Italy has nearly double the rate of Internet use that Thailand does, so it would be expected that Italy would therefore experience more attacks.

Once the rate of computer and Internet use is factored in, Saudi Arabia has far higher rates of attack than its level of computer/Internet use would suggest. Saudi Arabian networks received 1.81% of the total attacks in 2009. However, Saudi Arabia accounts for only 0.002% of the world's Internet users, which is far less than the percentage of attacks experienced. In 2010, Saudi Arabia's percentage of attacks remained almost constant at 1.77%, which raises the question: why is Saudi Arabia so prone to attack? Furthermore, Trend Micro Smart Protection Network announced in September 2010 that Saudi Arabia had 421,998 hacked computers, which was an increase of 65% in less than a year. Similarly, Symantec Lab found that Saudi Arabia is the most spammed country in the world. In June 2011, there were 39.2 billion spam messages sent. Saudi Arabia's spam rate is 82.2% meaning that 82.2% of emails received on Saudi Arabian networks are spam (Symantec Lab 2011). This is an almost unbelievable figure. Russia is the second most spammed country and China is the third.

It is of interest in this thesis to understand ISA and InfoSec practices and whether it is related to either Saudi Arabia's high level of censorship and cultural or their lack of information security practices.

Saudi Arabia is a highly-censored country. Censorship can be defined as the control of information and ideas circulated within a society by a censor (Green and Karolidies 2005). Saudi Arabia is subject to all three of the major types of filtering (Deibert et al. 2008), namely, political, social and security/conflict filtering. The issue of censorship may contribute to the large number of attacks in Saudi Arabia, and since Iran has the same types of censorship and a far higher rate of Internet use than Saudi Arabia, there must be more distinguishing findings. One possible explanation is that it is some combination of culture and censorship that makes Saudi Arabia prone to attack. This study is concerned with understanding ISA and InfoSec practices in Saudi Arabia.

Given the focus on Saudi Arabia in this thesis, it is important to have an understanding of the country and its people to provide context for the analysis. Saudi Arabia is one of



the largest countries in the Middle East with approximately 28 million inhabitants, 99% of whom are Muslims (Alowain 2012). It is an oil rich country and the income from oil subsidises a welfare state controlled by the government. The government is dominated by the royal family, which numbers many thousands and controls most of the kingdom's important posts (Library of Congress 2006). The Islamic religion plays a huge part in Saudi life and politics. All decisions made by the king must be consistent with Islamic law. Saudis consider religion as the most important element of their identity (Moaddel 2006). The Saudis' interpretation of Islamic law severely constrains the roles of women, and the mixing of the sexes is actually prohibited outside the family. The country is strongly patriarchal.

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

Hofstede's description of Arabic culture may provide a clue, for Saudi Arabia at least.

*"These societies ... are also highly rule-oriented with laws, rules, regulations, and controls in order to reduce the amount of uncertainty" (Hofstede 2009).*

In describing Saudi Arabia's low score for Individualism, he says that Arabic culture is manifested in a

*"close, long-term commitment to the member 'group', [i.e.] a family, extended family, or extended relationships. Loyalty in a collectivist culture is paramount, and over-rides most other societal rules." (Hofstede 2009).*

There is little or no evidence in the literature of any previous studies of the level or causes of ISA among the Saudi general public and InfoSec practices among Saudi Arabian organizations.

### **1.3 Research objectives**

The main purpose of this research is to understand information security awareness and practices in Saudi Arabia, which is a highly-censored country. The thesis will

investigate how information security awareness and practices are impacted by the highly-censored culture in Saudi Arabia. The thesis has the following objectives:

1. Determine the level of Information Security Awareness (ISA) among the Saudi Arabian public.
2. Determine InfoSec expertise in Saudi organizations:
  - a. Determine the use of InfoSec laws, standards and policies.
  - b. Determine InfoSec practices in Saudi organizations.
  - c. Determine InfoSec risks in Saudi Arabia.
3. Understand ISA, InfoSec practices and cultural implication in Saudi Arabia.
4. Develop process model of InfoSec cultural adaptation process (CAP) that can be used to address these weaknesses.

#### **1.4 Methodology**

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

This study involved the conduct of two surveys. The first was designed to measure the ISA in the general public in Saudi Arabia. The second surveyed information technology departments in government and business in Saudi Arabia. Survey questions were selected from instruments developed by the Cyber Security Organization in Malaysia, the Excellence of Information Assurance Centre and the Alelm organization in Saudi Arabia. All questions from each of these surveys were included, except for those that

were deemed to be inappropriate for the Saudi culture.

The questions in this research were semi-closed-ended questions, which allow the respondent to choose from a specified list of answers, but have the option to provide a textual answer if their response is not suitably captured in the list. The survey was translated into the Arabic language because all participants were from Saudi Arabia. The initial survey was subjected to pilot testing by Saudis who were fluent English speakers to ensure both the validity of the questions and the accuracy of their translation into Arabic. Pilot test participants strongly recommended making all questions optional as they believed that many Saudis would simply stop answering the questions if they encountered a compulsory question that they did not want to answer. The survey questions were then uploaded to Survey Monkey with all questions being optional.

To ensure a high response rate, the researcher distributed an online links to the both surveys. The ISA survey distributed using popular Saudi organizational, educational and business websites. The InfoSec survey link has been emailed directly to IT department staff emails. This worked well, resulting in 462 responses to the ISA survey and 124 responses from Saudi Arabian organizations.

### ***1.5 Significance of the study***

Information systems contain very important electronic information that should be protected against serious threats such as the data destruction, data abuse and illegal actions (Thuraisingham 2005; Afyouni 2006). The rapid development of information threat techniques creates a serious hazard for information (Bragg et al. 2004). The development and management of an on-going defence is necessary to keep information as secure as possible. This thesis will consider how such a defence can be developed for Saudi Arabia.

In Saudi Arabia, which is a highly-censored country, many people believe that censorship refers only to the protection of information. This understanding shows an absence of awareness that censorship can also control information risks (Detmar et al. 2003; Farid et. al 2009). Also, the Saudi culture and history impacts on information security, with cultural values (such as the role of tribal societies and women's access to identification) clashing with modern technology and the related information security

issues (Bashir 2006; Albrik 1995). This research will consider whether the combination of being highly-censored and particularly of Saudi culture contributes to country position regarding to ISA and InfoSec practices.

Information systems users require security and privacy for their information, both personally and for business. To overcome the existing information security threats, it is essential for both information providers and information users to have good information security practices. Therefore, there is a need for appropriate policies practices and education about the content of these documents. This study will reflect on the status of such documentation and consider how the situation can be improved.

Other factors that contribute to the importance of this study are:

- i. Fairly new adoption of Internet in Saudi Arabia.
- ii. Regulation of Internet in Saudi Arabia is different to regulation in typical Western countries.
- iii. The cultural impact on information security has not been widely studied in Middle Eastern countries.
- iv. The Saudi Arabian government has made a commitment to identify and understand the challenges that are involved in the current and future use of the Internet. The government is also concerned with raising awareness about and encouraging the use of information and communication technology.

## **1.6 Research limitations**

The main limitation of this study is the lack of existing academic literature in this field examining practices in the Middle East, especially in Saudi Arabia. This problem has been addressed through reference to international sources to achieve the research goals. The data collection phase of the study was extended due to an initially low response rate for both surveys. The reasons for the slow response to the surveys may include Saudis' lack of familiarity with surveys, and Saudi culture in which response rates are typically low. Also, some Saudi Arabian government organizations that are responsible for censorship were unwilling to provide details about information security in Saudi Arabia.

These organizations justified their lack of participation by claiming that the information requested contained ‘government secrets’.

### **1.7 Structure of the thesis**

This thesis consists of seven chapters as illustrated in Table 1.2. Chapter 1 has presented a broad overview of the research including the background of the study, research objectives, methodology, significance of the study and research limitations.

**Table 1.2 Thesis structure**

Chapter	Description
1	Introduction to the research including background of the research, objectives, methodology, research limitations and thesis structure
2	Review of related topics in the literature
3	Description of the methodology used to collect and analyse the data
4	Presentation of the findings and discussion about Information Security Awareness (ISA) among the public in Saudi Arabia
5	Presentation of the findings and discussion about Information Security (InfoSec) practice in Saudi Arabian organizations
6	Summarised Findings Directly Related to Model
7	Conclusion

Chapter 2 presents a review of relevant literature. It first addresses information security, providing brief definitions. Information threats are described and the research in this field is explored from accidental, deliberate or contributory perspectives. Security failures and the risk management process are described in general and in relation to information security. The discussion of current information security standards, policies and legislations provides an understanding of internationally respected laws and standards. The second part of chapter 2 presents the implication of culture on information security in highly-censored countries in general and in Saudi Arabia in particular. The chapter concludes with a historical overview of Saudi Arabia, the impact of its culture and the status of Saudi information security.

Chapter 3 describes the research methodology that was used to achieve the research objectives. It begins with the philosophical underpinnings of quantitative methods,

which are used as the basis of the research methodology. Two surveys have been used: ISA among the general public and InfoSec in organizations. Each of these surveys is described in detail and the steps undertaken in each component are presented.

Chapter 4 is based on the ISA results for the general Saudi public. It analyses and discusses each related component from the ISA perspective. The chapter includes details of participants' backgrounds, ISA, practices and the preferred method that can be used to increase ISA.

Chapter 5 is based on InfoSec practices in Saudi Arabian organizations. It determines and discusses the levels of InfoSec practices in organizations. The chapter includes the organization / IT department staff backgrounds, organizational InfoSec standards/data protection law, organizational information assurance, tools and measurement, information security risks and proposed preferred method that can be used to have better practices.

Chapter 6 draws together the key contributions and recommendations of the study, identifies a suggested InfoSec CAP model for information security in distinctive cultures and provides suggestions for future research arising from the study.

Chapter 7 draws the conclusions of the study, identifies the scope, significance, limitations and the future of the research.

## **Chapter 2 Literature Review**

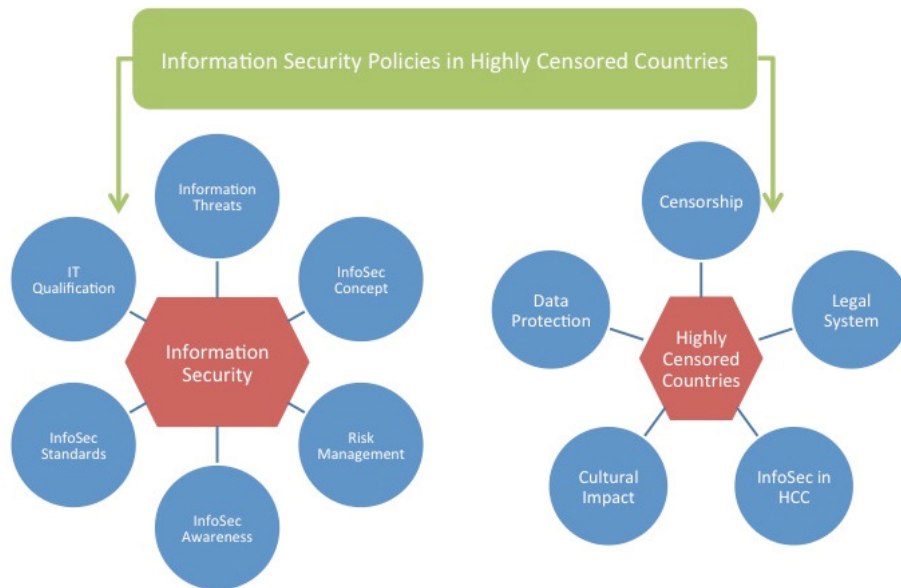
### **2.1 Introduction**

The 19<sup>th</sup> century statesman, Benjamin Disraeli, once said that “As a general rule, the most successful man in life is the man with the best information”. This belief has been reiterated hundreds of times since, by politicians, executives, economists and marketers, and information has become a vital part of the business, social and political world. With the advent of computers and telecommunications, vast quantities of information became available at the touch of a button. By the early 1980s, commentators were writing of an ‘information age’ in which the world’s economic fabric was utterly dependent on information.

However, the information age is not without its problems. It has created new struggles with misinformation, disinformation and information overload. Moreover, the same technologies that give access to all this information also allow unscrupulous people to access private information and copy, damage or destroy it.

While the ‘information super highway’ promises to give the whole world access to information, not all countries have the same ability to access this information or protect their private information. As described in Chapter 1, highly-censored countries (HCC) appear to have a poor track record of protecting their information.

This chapter provides a comprehensive review of the literature on Information Security (InfoSec) in HCC. This thesis aims to understand ISA and InfoSec practices in Saudi Arabia and to develop process model of InfoSec CAP that can be used to address these weaknesses. Figure 2.1 presents a conceptual framework for the current research. Each aspect will be discussed in the following sections.



**Figure 2.1 Conceptual framework**

### **2.1.1 Information quality**

An important aspect of Disraeli's quote above is that, to be successful, one needs the best information. When seeking competitive advantages, information must be readily accessible, as reliable and complete as possible and, preferably, unavailable to competitors. Not surprisingly, these three concepts are found in technical literature on information security.

Information security can be described as protecting information and systems from risks such as unauthorized access, illegal usage, disclosure, disruption, modification or destruction (Ferrari & Thuraisingham 2006; Merkow & Breithaupt 2006). Information security can be defined in terms of the confidentiality, integrity and availability of information (Turban et al. 1996; Stallings & Brown 2008; Whitman & Mattord 2008). Figure 2.2 shows the C.I.A triangle that refer to Confidentiality, Integrity and Availability (Afyouni 2006).





**Figure 2.2 Information Security Triangle (Afyouni 2006)**

#### **2.1.1.1 Confidentiality**

Confidentiality means that information should be protected from unauthorized disclosure, perhaps to a competitor or to the press (Wright & Kakalik 2007). According to Whitman & Mattord (2008), confidentiality is the “quality or state of information that prevents disclosure or exposure to unauthorized individuals or systems”. Breaches of confidentiality for example include, private information being disclosed through an employee’s mistakes or a hacker stealing a client’s information from an organization’s internal database system.

#### **2.1.1.2 Integrity**

Integrity means that information should be protected from unauthorized modification and that information, such as a price list, email contact details and other private institutional information, can be relied upon as being accurate and complete (Burke 1999). Integrity can be also defined as a guarantee of the completeness and accuracy or veracity of the information quality (Whitman & Mattord 2008). For example, many computer viruses and worms create integrity incidents by corrupting data in files. Unauthorized employees that make changes to data also compromise the integrity of information.

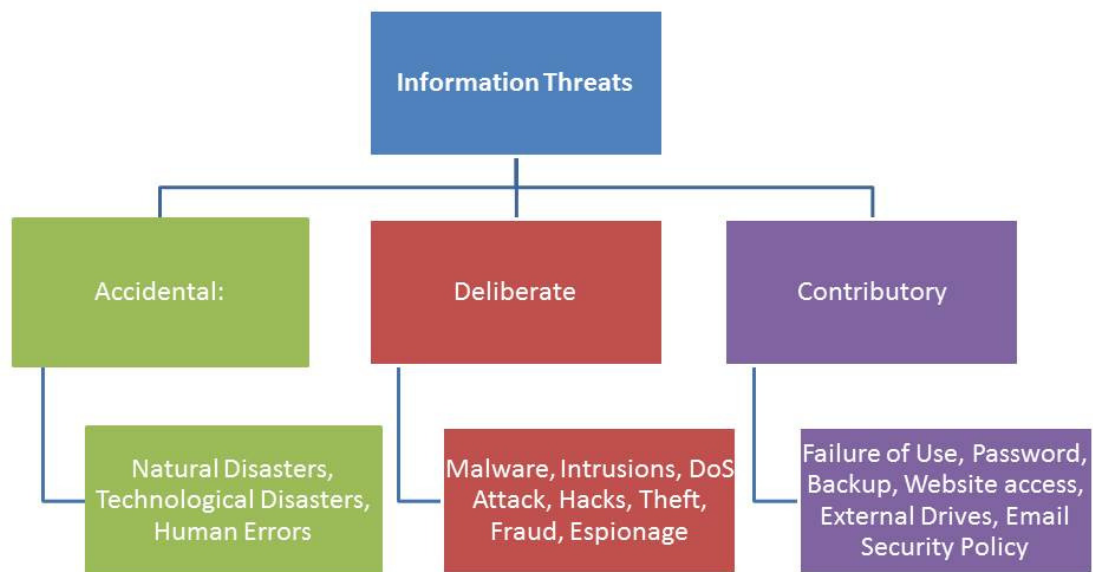
### **2.1.1.3      *Availability***

According to Afyouni (2006) and Whitman and Mattord (2008), availability means that the system should be accessible for those authorized to access it so they can reach the required information. It is concerned with the assurance of information being obtainable when users need it (Sherwood 2000). For example, some computer attacks (such as denial of service (DoS)) can break the visibility and availability of information.

The confidentiality, integrity and availability of private information are under constant threat. Confidential information sources may be leaked to competitors or the public. Information may be corrupted by hard drive failure or by cyber vandals, and required information may be unavailable because of a bottleneck on the web or network failure. To ensure the confidentiality, integrity and availability of information it is important to understand the threats being faced.

### **2.1.2 Information threats**

There are currently many different types of threats to information security that may bring about loss of confidentiality, integrity or availability. Information threats can be categorised as accidental or unintentional, deliberate or intentional, and contributory or instrumental (Stulz 2003; Afyouni 2006). Accidental or unintentional threats are those caused by occurrences outside the IT equipment such as natural disasters, technological disasters and human errors (Shaluf 2007; Hoo 2000). Deliberate or intentional threats may be either malicious or benign. Those designed for malicious purposes to destroy or abuse the targeted information use techniques such as malware, hacks, intrusions, Denial of Service (DoS) attack, theft, fraud or espionage (Easttom 2006; Bragg et al. 2004). Benign threats often contribute to exploration to find flaws in a system or purposefully flaunting system flaws. Contributory or instrumental threats are introduced by the failure or non-existence of adequate procedures. Uncontrolled access to IT equipment would constitute a procedural threat. This could include a failure of use backup, password strengths practices, restriction policies related to websites access, use of external drives or email security policies (Geric & Hutinski 2007). Figure 2.3 shows the types of information threats.



**Figure 2.3 InfoSec threat types**

Whether a threat is accidental, deliberate or contributory, there is usually a human element present, either in the initial introduction of the threat or by increasing the risk through failure to take sufficient precautions. The following sections describe the types of threats. Table 2.1 provides statistics about information threats in the last five years. The data was collected in the CSI Computer Crime & Security Survey (2011) from over 500 security professionals drawn from a variety of organizations. Table 2.1 provides an overview of what will be discussed in the following sections.

**Table 2.1 Information threats – percentage effect 2005-2010 (CSI Computer Crime & Security Survey 2011)**

Threats	2005	2006	2007	2008	2009	2010
Malware infection	74%	65%	52%	50%	64%	67%
Phishing messages			26%	31%	34%	39%
Password sniffing			10%	9%	17%	12%
Financial fraud	7%	9%	12%	12%	20%	9%
Denial of service	32%	25%	25%	21%	29%	17%
Extortion or blackmail associated with threat of attack or release of stolen data					3%	1%
Web site defacement	5%	6%	10%	6%	14%	7%
Other exploit of public-facing Web site					6%	7%
Exploit of wireless network	16%	14%	17%	14%	8%	7%
Exploit of DNS server			6%	8%	7%	2%
Exploit of client Web browser					11%	10%
Exploit of user's social network profile					7%	5%
Instant messaging abuse			25%	21%	8%	5%
Insider abuse of Internet access or e-mail (i.e.pornography, pirated software, etc.)	48%	42%	59%	44%	30%	25%
Unauthorized access or privilege escalation by insider					15%	13%
System penetration by outsider					14%	11%
Laptop or mobile hardware theft or loss	48%	47%	50%	42%	42%	34%
Theft of or unauthorized access to PII or PHI due to mobile device theft/loss				8%	6%	5%
Theft of or unauthorized access to intellectual property due to mobile device theft/loss				4%	6%	5%
Theft of or unauthorized access to PII or PHI due to all other causes				8%	10%	11%
Theft of or unauthorized access to intellectual property due to all other causes				5%	8%	5%

#### **2.1.2.1 Accidental threats**

Accidental or unintentional threats are caused by incidents that are beyond human control, such as natural disasters, technological disasters and human errors (Shaluf 2007; Hoo 2000). According to Erbschloe (2003), natural disasters are one of the main threats to information. The term ‘environmental threats’ is also used by some authors to describe these types of threats. Environmental threats include (Shaluf 2007; Poulsen 2003; Hoo 2000):

- i. Fire, including electrical fires and bush fires.
- ii. Flooding, due to flooded rivers, heavy seas or heavy rain leaking into a building.
- iii. Building collapse or the threat of building collapse, which may be caused by structural failure of the building, by impact from an aircraft or motor vehicle, or as a result of an earthquake.
- iv. Power failure, which may stop or permanently damage computer systems and disrupt security systems, preventing access to buildings.
- v. Computer or telecommunications failure, which may stop or permanently damage computer systems and the information they contain, or create a delay while information and systems are restored from backups.
- vi. Air conditioning failure in data centre server rooms, which may cause computers to overheat and fail.
- vii. Incorrect entry of data by office staff or end users, reducing information integrity.
- viii. Bugs in a software system, leading to generation of incorrect information.
- ix. Sickness or injury of key IT staff, which may affect availability.
- x. Poor location of a computer facility, such as proximity to political demonstrators or industrial disputes, that prevents staff from accessing the facility.

#### **2.1.2.2      *Deliberate threats***

Deliberate or intentional threats can be defined as the threats designed for either benign or malicious purposes to destroy or abuse targeted information. These include malware, hacks, intrusions, Denial of Service (DoS) attacks, theft, fraud, espionage and arson (Ateeq 2012; Easttom 2006).

Malware is software that is designed for a malicious purpose. The software can contain viruses, Trojan horses and spyware (Bragg et al. 2004). Viruses contain malicious code designed to modify files to perform unauthorized actions (Solomon & Chapple 2005). Viruses are deliberately circulated to computer users with the intention of spreading to other users and damaging or destroying their information. The effect can be harmless (for example, a screen message), or it can be a serious corruption of either data or software (Turban et al. 1996). New viruses are constantly being produced and the

effects can be significant. Hackers can create viruses, logic bombs, worms and Trojan horses, each of which can cause a loss of confidentiality of data (Bragg et al. 2004).

Intrusions are attacks using any method to gain unauthorized access to a system (Vacca 2009). Denial of Service (DoS) attacks are designed to prevent legitimate access to systems and cause the unavailability of resources (Kizza 2005). Hacking and tapping occur when someone sets out, without authority, to examine computer-held data. Hacking means breaking into a network while tapping means actually connecting into a cable (Easttom 2006). Hacking is usually performed to prove the technical skill of the hacker but may destroy the confidentiality, integrity and availability of data. Hackers can abuse information by inserting a piece of code into a program. This code operates at some future date to corrupt files or software. Typically, a programmer might insert code to delete a file if his name is removed from it such as when a programmer is sacked and his name is removed from the HR system (Turban et al. 1996).

Laptop theft is a significant threat to users of laptop computers. Victims of laptop theft can lose hardware, software and essential data that have not been backed up. Thieves may also gain access to sensitive data and personal information (Brown 2009). In response to this problem, many methods to protect the data and prevent theft have been developed, including alarms, laptop locks and visual deterrents such as stickers or labels (Mikusch 2006).

Fraud is any intentional or deliberate act to deprive another of property or money by cleverness, trickery or other unfair means. It is one of the threats that can seriously affect information (Action Fraud 2011). Fraud is used in many sectors for different purposes such as financial fraud and Internet fraud. Internet fraud has become one of the easiest ways for vandals to gain money or important information using techniques such as phishing scams. The best way to fight Internet fraud is to learn how to avoid becoming a victim (Crescenzo 2006).

### *2.1.2.3 Contributory threats*

Contributory threats are introduced by the failure or non-existence of adequate procedures. Uncontrolled access to IT equipment would constitute a procedural threat (Poulsen 2003). Procedural threats cause the correct procedures to be by-passed. For

example, an unauthorized person may obtain access to computer equipment or media if there are inadequate checking procedures. If insufficient logical access procedures exist then data may be read or updated by people with no authority. Control over the development of new systems and the amendment of existing ones prevents incorrect programs being put into live use (Geer et al. 2003). All systems are at risk through unreliable personnel. Personnel routines should ensure that only reputable staff are employed in positions of trust. Exit procedures should ensure that staff leaving the organization do not retain their identification or means of access.

Poorly trained staff contribute to information risks because they often do not have the knowledge or skills to prevent or reduce information risks (Huang et. al 2011). According to Shaw et al. (2008) and Huang et. al (2003), the level of risk is increased if there is low awareness or inadequate training for employees. Increased understanding of current risks (such as scams, hacks, attacks, fraud, phishing and ID theft) combined with awareness of the value of data on employees' devices (such as computers, PDAs, thumb drives and smart phones) can reduce the challenges of asset protection. Employees need training to recognize and respond appropriately to real and potential security concerns.

### **2.1.3 Consequences of security failures**

Security breaches can result in a variety of consequences and losses (Slay & Koronios 2006; Jones & Ashenden 2005). These include:

- i. Loss of confidentiality: control of access to the system will not be maintained (for example, unauthorized access to data is possible) (Sherwood 2000).
- ii. Loss of integrity: the data that the system holds and produces will not be accurate.
- iii. Loss of availability: the system will not be operational when required (Poulsen 2003). The destruction of the computer centre represents an extreme and possibly permanent form of loss of availability.

The effect of such losses, either individually or in combination, can have serious consequences for both the information system and for the organization as a whole. Therefore, security threats must be considered within their corporate context. An IT department is an integral part of the operation of an organization, so the activities and

occurrences that directly affect it will influence the organization, possibly to the extent of threatening the organization's existence. For example, a change in the management policy towards staff can lead to discontent amongst the IT staff, and, due to the increased probability of errors or negligence, pose a very real threat to information security (Microsoft Solutions for Security and Compliance 2006). If one of these errors leads to the loss of commercially valuable information or results in a serious delay, this will create problems for the organization (Mantel et al. 2001). The general identification and assessment of relevant factors that contribute to the breach of information security is made difficult by the diversity of organizations and their computing needs. What is considered sufficient or adequate in a system will obviously vary between organizations and over time as circumstances change (Finne 1997). The vulnerability and sensitivity of a system and its data, and the feasibility and costs of safeguards, must be taken into account (Microsoft Solutions for Security and Compliance 2006).

#### **2.1.4 Risk management**

Risk can be formally defined as the probability that an action or event will adversely or beneficially affect an organization's ability to achieve its objectives (Jones & Ashenden 2005; Brotby 2009). Risk management is an ongoing process created to control the possibility of adverse events (Slay & Koronios 2006; Bragg 2004; Dorfman 1998) and can be defined as "the process of identifying vulnerability in an organization's information system and taking steps to assure that losses experienced by the system are within the acceptable loss limits of the organization" (Whitman & Mattord 2008). Risk management represents a systematic approach to the problems posed by threats. Many possible methods, techniques and software tools can assist in the management of risk (Stulz 2003).

Each part in a project or system may have a different set of risks to which it is exposed, or will have a different view of a risk and the alternative actions (Burke 1999; Sherwood 2000). There are many descriptions of the process of risk management in the literature. According to (Erbschloe 2003; Jones & Ashenden 2005; Kliem 1999; Slay & Koronios 2006), the common pattern for risk management is:

- i. Identify hazards
- ii. Assess those hazards





Risk management process models typically follow the general patterns described above. However, some authors describe additional steps or considerations in the process. For example, Caelli et al. (1989) suggest a preliminary step of asset identification, referring to the need to define the resources (i.e. hardware, systems and people) that require protection. Caelli et al. (1989) also include a step labelled selection of countermeasures, concerned with selecting the most cost effective countermeasures that will reduce the risk to an acceptable level. When the countermeasures are in place, risks should be recalculated to ensure that the measures have been effective. Finally, Coyne et al. (2004) include preparation of contingency plans on the basis that contingency plans are required to assist recovery from any unexpected disaster that the countermeasures fail to prevent.

Based on this analysis of risk management models, it can be concluded that, excluding minor variations in terminology and some extensions, the Mantel el al. (2001) model broadly depicts accepted views of risk management and is therefore a useful model. The following sections describe each of the steps in the Mantel el al. (2001) model.

#### *2.1.4.1 Risk identification*

The first step in identifying risks is to identify all the elements, assets and resources that belong to the computing system or are necessary for its operation, and which therefore could be at risk (Raval & Fichadia 2007;Whitman & Mattord 2008). According to Mantel el al. (2001) the system classifications are as follows:

- i. Hardware, e.g. central processor, magnetic disc drives, terminals, modems, shredders, storage cabinets.
- ii. Software, e.g. operating system, compilers, applications programs, audit routines, security dumps, back-up copies.
- iii. Data and media, e.g. master files, input data, output files, software documentation, operating procedure documentation, disc packs, magnetic tapes, cards.
- iv. Communications, e.g. telephone circuits, postal services, private data carrying services, networks, etc.
- v. Environment, e.g. building structure and fittings, power supplies, air

conditioning plant, cleaning services, catering facilities, lift services.

- vi. Organization, e.g. management policy and structure, personnel (IT, technical, administrative and secretarial).
- vii. Support, e.g. maintenance staff, auditors, consultants, delivery services.

Having prepared lists covering all the items at risk, each element, asset or resource should be considered in relation to the types of risk (for example, accidental destruction, deliberate disclosure, etc) and the causes of risk (for example, fire, flood, malicious damage, industrial action, etc.) (Nicholas 2002). Furthermore, whilst considering the possible risks, it should be realized that a single event may place more than one item at risk and may result from the interaction of the occurrence of risks with the various elements that together constitute a computing system. Risks may be broadly classified as follows:

- i. Property losses, e.g. destruction, damage, loss, theft, contamination.
- ii. Liability losses, e.g. breach of contract, breach of copyright, libel, slander.
- iii. Personnel losses, e.g. death, injury, illness, industrial action, resignation, leave of absence.
- iv. Financial losses, e.g. bad debts, dishonest employees.
- v. Business interruption losses, e.g. delayed cash flows, increased cost of working, penalty clauses.

#### *2.1.4.2 Risk analysis and evaluation*

Risk analysis refers to evaluating the possibility and magnitude of the risk. It is used to reduce the possible occurrence of a risk, the consequences of the risk and the methods used to handle each of those individual consequences (Stulz 2003). This implies a means of assessing or measuring risks and the consequences of their occurrence. There are a number of techniques for doing this-some qualitative and some quantitative (Coyne et al. 2004).

A quantitative value, which may be derived for a particular risk, is that of expected loss. It can be expressed in monetary units such as dollars per annum and is obtained by multiplying the mean value of the loss (which would result from an occurrence of the

risk) in monetary terms by the frequency with which the risk is expected to occur per annum. Although a time interval of a year is usually chosen for obvious reasons of convenience, other time intervals may be used as appropriate (Bullen 2000). If the expected loss is to be used to establish both the seriousness of risks and the resultant need for countermeasures, then the values of the two quantities involved—loss (also referred to as impact) and frequency—are obviously critical. The best estimates from the expertise available should be used (Burke 1999). Once the values of expected loss have been estimated for each risk, then the risks should be listed in order of decreasing value of expected loss.

As a general rule, the higher the value of expected loss, the more important it is to counter the corresponding risk (Caelli et al. 1989). However, in selecting appropriate countermeasures, their effectiveness in reducing the expected loss and their cost to implement must both be taken into account. What must be sought is a set of countermeasures which, bearing in mind the amount of money available, reduces to the lowest value the sum of the expected losses due to all the occurrences of risks and the costs of the countermeasures (Nicholas 2002). Of course, the constraints may not be entirely financial and other risks that could also threaten the survival of the organization (for example, the interruption of a vital real-time operation or the disclosure of confidential or secret information) will also have a high priority (Dorfman 1998). Having considered the possible risks and then assessed the likelihood of their occurrence and the gravity of their consequences, attention must be given to possible ways of dealing with the situation. Measures must be selected to handle individual risks and to meet contingencies (Smith 1999). The ways in which these measures are to be implemented, monitored, reviewed and where necessary, updated, must also be decided (O'Harrow et al. 2003).

#### *2.1.4.3 Risk control*

There are four basic ways to control risks (Mantel et al. (2001) ; Stallings & Brown (2008)):

- i. Avoidance: Sometimes a risk can be obviated by, for example, dispensing with or not introducing a particular facility or item of equipment, or by altering the method of working in some way (OECD International Futures Program 2004).

Such a course of action could be voluntary or may be taken because of the difficulty of providing effective countermeasures (Dorfman 1998). However, vigilance must be exercised at all times to ensure any changes in circumstances, either internal or external, that would allow the particular risk to return are identified immediately.

- ii. Retention: If it is considered that a particular risk would have only comparatively minor consequences (i.e. a risk that could be handled without embarrassment), then an organization may decide to take no direct countermeasures. Where this is the case, the full consequences of the risk would be carried by the organization (Caelli et al. 1989). It may be possible to accept the retention of risks having a low cost but high frequency of occurrence, although the retention of a high cost, low frequency risk could prove disastrous. Again, care must be taken to watch for changing circumstances that could increase the threat of retained risks. Conscious retention of risks must not be confused with unwitting retention due to a failure to identify the risk—such a failure could have embarrassing consequences (Caelli et al. 1989).
- iii. Reduction: Many risks may be reduced in their severity by the application of preventive measures, for example, some forms of access control systems may reduce risks associated with the presence of unauthorized personnel in a computer room. In general, such countermeasures are an added expense (Stulz 2003). However, they need not be if, for example, they can be affected by changes of a procedural nature.
- iv. Transfer: Transfer of the risk is usually done by contingency planning, insurance or some form of contract. Although countermeasures may reduce the frequency of occurrence and/or the impact of particular risks, they cannot always be eliminated (OECD International Futures Programme 2004). When they do occur, a well prepared contingency plan can ensure that at least the essential systems remain operational. In addition, insurance can provide some financial recompense for the losses incurred (Smith 1999). However, although the annual cost of the premiums is known in advance, insurance may not be the most cost-effective measure for dealing with many types of risks. Insurance policies commonly contain excess clauses, which effectively exclude cover for the first

part of any claim following the occurrence of a risk (Caelli et al. 1989). In such circumstances, the proportion of the risks not borne by the insurer is another form of retained risk for the insured. Another method for transferring risk is by some form of contractual agreement, such as a warranty or maintenance agreement (Nicholas 2002). It is vital that the organization accepting the risks, whether insurer or contractor, is reputable and likely to stay in business. It is not possible to transfer all the risks in this way; insurance is not a substitute for proper countermeasures (Hoo 2000).

In the information security field, qualified staff and powerful tools can help to prevent, control and reduce risks. For example, poor passwords can be cracked easily by hackers. Hackers have a range of tools and techniques for guessing or cracking passwords, including social engineering. Short or weak passwords or passwords that contain personal identification such as name or date of birth allow vandals to crack passwords easily (Weirich & Sasse 2001; Easttom 2006). Strong passwords that are composed of more than eight characters and include a mixture of numbers, upper and lower case letters and special characters are far more difficult to crack and so can protect information from unauthorized access and theft. However, a strong password alone is not enough to completely secure information; passwords should be changed regularly to ensure that any exposure is limited.

In addition, good Internet security tools can help to control and protect information from threats. For example, anti-virus, anti-spy, anti-spam and firewall software can protect users' privacy and guard against information threats such as viruses, spyware, Trojans and hackers (Bragg et al. 2004).

In the context of information security, risks may occur due to users' carelessness with securing information or because of their lack of awareness about the value of information. However, well trained and highly aware users can prevent and control further risks. Users should be aware of information security standards and policies to secure information against possible risks (Peltier 2004).

The following section discusses information security standards and policies in further detail. It also highlights the benefits of information security policies in both public and

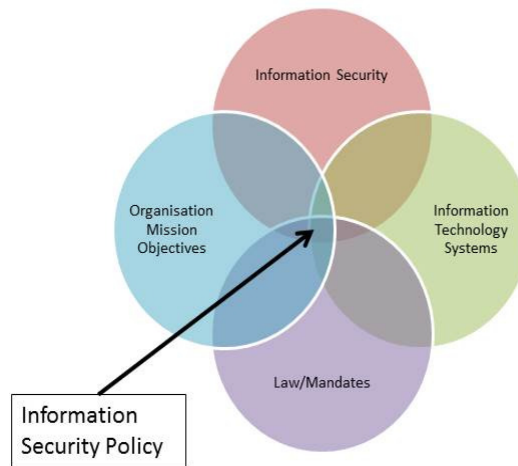
private organizations.

### **2.1.5 Information security policies and standards**

After completing the technical process for managing risks, the next step is the development and implementation of an appropriate policy. Since 1970, there have been several improvements in the field of information security policy specification. Information security policies are the foundation that supports the security of information resources in the organization. Organizations have started to make ongoing developments in technology policy to address the growing challenges (Ferrari & Thuraisingham 2006; Peltier 2004; Knapp et. al 2006).

Information security policy should combine physical, technical and non-technical items to ensure that compliance is sustained over time (Wyllder 2004). Information security policies can be defined as statements that clearly indicate the process of identifying, assessing and controlling risks that arise from operational factors, and making informed decisions that balance risk cost with mission benefits (Fugini & Bellettini 2004; Stamp 2006; Peltier 2004). The formal policy document should include an explanation or statement of security policies, procedures and requirements and a definition of general and specific security responsibilities (Johnson 2011; Stallings & Brown 2008).

Figure 2.5 shows the location of an organization's information security policy in relation to the organization's mission, laws and mandates, the information technology used and the level of information security needed (SANS 2010).



**Figure 2.5 Information security policy location (SANS 2010)**

There are several internationally recognized standards for information security management including BS7799, ISO/IEC 17799, ISO 27001 and ISO 27002. These standards are explained below.

BS7799, which is the British Standard Code of Practice for Information Security Management, was published in February 1995 (Fisk 2002). It is a reference document for those responsible for implementing and maintaining IT security, and provides a sound basis for an organization's IT security policy (Lanza 2000; Siponen et al. 2007). The BS7799 standard addresses a number of areas including assets to be protected, the organization's approach to risk management, control objectives and controls, degree of assurance required, security awareness programs and development of security policies and procedures (Kenning 2001; Fisk 2002). BS7799 provides exploration for information security management. Organizations applying for certification are evaluated according to this document (Bisson & Saint-Germain 2005).

In addition, BS7799 has been adopted by the International Standards Organization (ISO) as an ISO standard and the International Electrotechnical Commission (IEC) as



well. BS7799 is internationally accepted as a set of ‘best practices’ for information security management. Many countries have adopted it as a national standard, including the United Kingdom, Germany, Netherlands, South Africa, Japan, Australia and New Zealand. Some other countries, such as China, use policies developed by the National Information Security Testing, Evaluation and Certification Center (CNISTECC), while others use custom-built policies that have been designed specifically to address their cultural, religious or legal needs. Table 2.2 shows the countries that use the BS7799 standard.

**Table 2.2 Countries that use BS7799 standard**

Country Name		
Australia	Ireland	Singapore
Brazil	Japan	South Africa
Canada	Korea	Sweden
Czech Republic	Malaysia	Sweden
Denmark	Netherlands	Switzerland
France	New Zealand	Taiwan
Germany	Norway	UAE
Iceland	Poland	UK
India	Portugal	

ISO/IEC 17799 or ISO 27002 is presented in the form of guidelines and recommendations that were assembled following consultations with large organizations. The 36 security objectives and 127 security controls contained in ISO/IEC 17799 are divided among ten domains (Saint-Germain 2005). ISO/IEC 17799 has been renamed to be ISO 27002. The following is a brief overview of each of these domains:

- i. Security policy: Provide guidelines and management advice for improving information security.
- ii. Organizational security: Facilitate information security management within the organization.
- iii. Asset classification and control: Conduct an inventory of assets and protect these assets effectively.
- iv. Personnel security: Minimize the risks of human error, theft, fraud or the

abusive use of equipment.

- v. Physical and environmental security: Prevent the violation, deterioration or disruption of industrial facilities and data.
- vi. Communications and operations management: Ensure the adequate and reliable operation of information processing devices.
- vii. Access control: Control access to information.
- viii. Systems development and maintenance: Ensure that security is incorporated into information systems.
- ix. Business continuity management: Minimize the impact of business interruptions and protect the company's essential processes from failure and major disasters.
- x. Compliance: Avoid any breach of criminal or civil law, of statutory or contractual requirements, and of security requirements.

ISO 27001 designed to build the foundations of information security in your organization, and devise its framework, ISO 27002 designed to implement controls. It can be concluded that without the details provided in ISO 27002, controls defined in ISO 27001 could not be implemented; however, without the management framework from ISO 27001, ISO 27002 would remain just an isolated effort of a few information security enthusiasts, with no acceptance from the top management and therefore with no real impact on the organization (Calder 2008).

Given the cost of implementing such international security standards, some organizations are unlikely to adopt these standards unless compelled to by the law of their country. These standards are very good but, like most standards, they are voluntary. In many countries, however, "tech-savvy" governments have realised the benefits of adoption of such standards in private enterprises. Private enterprises may also be required to adhere to some or all of the government's standard operating procedures.

From the discussion above, it can be seen that the role of law and government regulations is important in the widespread adoption of these standards. However,

different cultures adopt different view to world's law and government legislations such as Saudi Arabia gives a chance to look at different culture that may be different in their approach to law.

## ***2.2 Cultural component of information security***

Given the fact that technology being the agent of global integration and collaboration within, it gives the people a more broader opportunity of inter mingling, however the double sword nature of technology makes it equally and highly vulnerable. Through different phases and evolutionary processes of technology, its compatibility with the local environment and culture has often been subjected to testing and hypothesis evaluation (Zakour 2004). Interpersonal skill which is a subjective trait of a culture is taken for as one of the variables of studies of Hofstede Framework.

Individualism or collectivism which is largely reflective of the type of society and culture defines the manner in which I.S operations are undertaken. This often comes in the form of the variables that take into account the diversity and the potential vulnerability of the systems and the technology unleashed.

Hofstede's Framework can be studied in the context of cultural differences between the common users and their responses and the manner in which the overall concepts of technology and security are reciprocated.

Jones and Alony (2007) have undertaken an observational study based on the Framework postulated by Hofstede. According to Jones, Hofstede assessed the different dimensions in terms of the social outlook and the country wise background. In his study Malaysia was given as an example where information system organizational structure is observed in terms of hierarchy (Jones & Alony 2007).

Myers et al. have assessed the variable of Power Distance in terms of the information system network set up in the Malaysian industry (Myers et al. 2002). Hofstede's Framework aims at addressing the manner in which the different cultures respond to information technology, its prerequisites and the overall operational mechanism. With reference to the fourth variable of Uncertainty Avoidance in the Information systems network, Enterprise Resource Planning has been declared as an important variable of

the entire network with regard to the smooth operations.

Harvey and Lausanne (1997) have supported the model and framework with regard to its implementation in the American culture, while in the European culture and background (Harvey & Lausanne 1997), this framework has not been completely approved with regard to its validity and compatibility with the local system of information security.

Hofstede's framework pertinent to culture finds its applications in the different sphere within a society and its modern tools. With one of the modern tools being that of technology, Hofstede tried to assess the manner in which these variables and this technology would inter relate and respond to one another. The roots of Hofstede's research find their traces in one of the works undertaken by Gerard Hofstede himself while he was an employee of I.B.M (Bargiela-Chiappini 2009).

Each of the dimension understated by Hofstede provide an insight into how his theory can be integrated into the security aspect of information systems. One of the variables and dimension stated by Hofstede comes in the form of long term orientation (L.T.O). In the context of technology, this can be interrelated to the manner in which technology progresses and in parallel, the manner in which the security means of technology are needed in a long term orientation.

The variable of masculinity may find little relevance and little importance in the context of information security since information system and security in itself is subject to sensitivity regardless of the gender or the type of user.

An often overlooked perspective on information security is the impact of culture. This will be explained using the structure of legal system and censorship in the following sections.

### **2.2.1 Legal systems**

All countries are governed through some form of legal system. The 'law' can be defined as the principles and regulations established in a community by some authority and applicable to its people, whether in the form of legislation or of customs and policies recognized and enforced by judicial decision (David & Brierley 1988). However, the

basis of the law is different in different countries. Figure 2.6 shows the different legal foundations in countries around the world.



**Figure 2.6** World map showing countries' basis of law (ICT Regulation Toolkit Organization 2010)

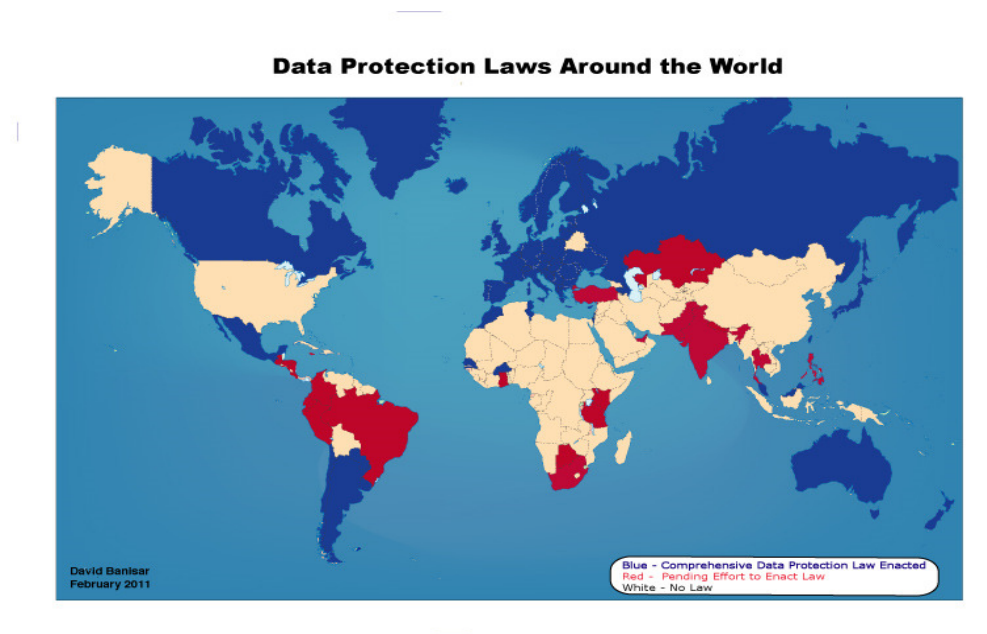
The existence of the five different bases for legal systems is often not common knowledge in Western developed nations. The United States, the United Kingdom, Australia, South Africa, Canada and India use Common Law, which the law is created by decisions of justice (Holmes 2009). European countries and some Asian countries such as Japan, Taiwan and South Korea use Civil Law, which is a legal system inspired by Roman law. The primary feature of Civil Law is that laws are written into a collection and codified, rather than being determined by judges as in Common Law (Glenn 2007). Other countries such as Saudi Arabia and Iran use Islamic Law (Sharia). This is a religious law that comes from the Holy Quran and the prophets (Hussain 2004). In addition, some countries use two laws. For example, China uses both Civil Law and Social Law (Wang & Yi 2009). These differences in legal codes between countries have developed because of their different needs or for cultural reasons. Despite the variations in basis all laws share many similarities, such as the condemnation of crimes and illegal actions. Areas of differences include the types and severity of punishment (David & Brierley 1988; Glenn 2007).

The law should incorporate all required legislation. This should include information

security legislation such as data protection law. With the ongoing development in data transmission, data protection law has become one of the important foundations for information security. One might assume that legislated countries would also have strict data protection and data privacy laws. While this is often the case, it is not always true, as the next section demonstrates.

### 2.2.1.1 *Data protection law*

Data protection is designed to protect personal data and to ensure privacy and security (Stallings & Brown 2008; Straub et. al 2008). Figure 2.7 clearly shows that many countries do not have data protection laws (Peltier 2004).



**Figure 2.7** World map showing countries' data protection laws (Banisar 2011)

Some of these countries without data protection laws are not only legislated but highly-censored countries. Such countries include Saudi Arabia, China, Syria, Ethiopia and Iran.

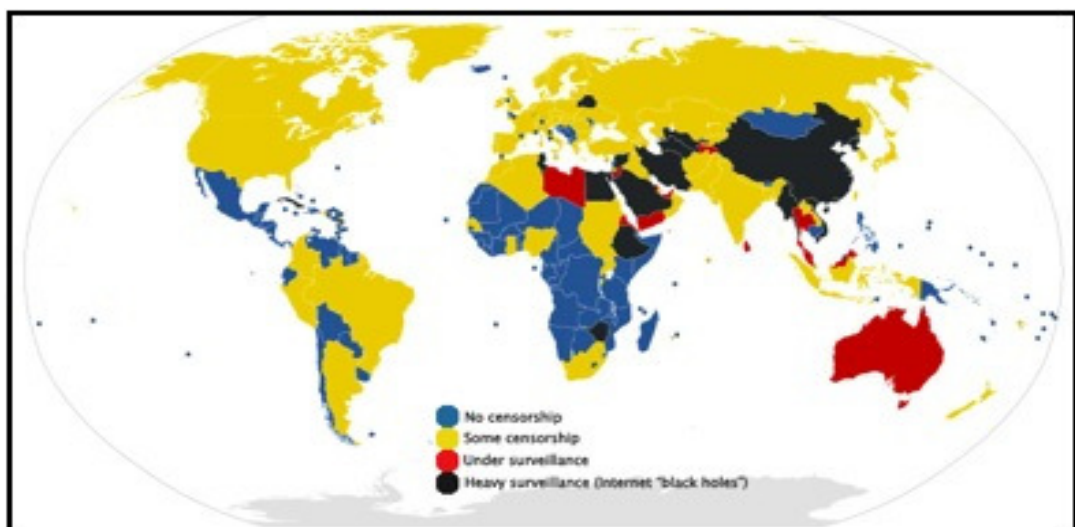
### 2.2.2 **Censorship**

One of the common concepts in all the legal codes is censorship, which can be defined as the control of information and ideas circulated within a society by a censor (Green & Karolidies 2005). The censorship rates and levels are related to countries' cultures and

legislation systems. Commonly censored information and ideas often relate to violence or criminal acts, national security, political activities or ideas, human rights, the use of alcohol, pornography, gambling or Internet use (Hannabuss & Allard 2001; Green & Karolidies 2005).

#### 2.2.2.1 Internet censorship

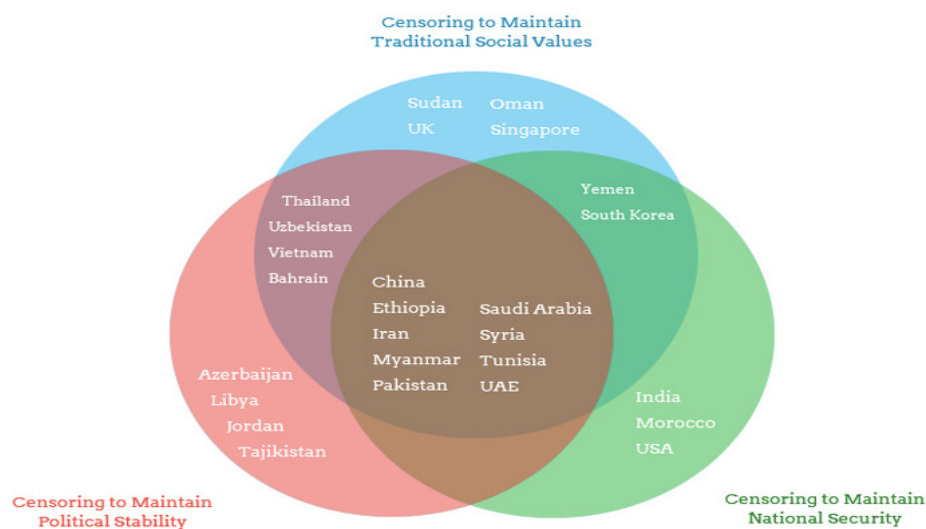
Internet censorship refers to technical and non-technical measures taken by government organizations to limit users' freedom to access information on the Internet. Such measures include, but are not limited to: monitoring of users' Internet activities, denying users access to certain websites (blocking), tracking and filtering users' data flow and disciplining website operators to tailor their content to comply with censorship regulations (Green & Karolidies 2005). Internet censorship is also commonly referred to as Internet blocking or jamming (Global Internet Freedom Consortium 2007; Hamade 2008; Edwards 2010). Internet service providers in censored countries are responsible for the required censorship under the countrys' law (Alhajiri 2004; Hamade 2008). There are some filtration techniques available to block access to Internet webpages. These techniques, such as IP blocking, DNS tampering and URL blocking using a proxy, are used to block access to specific webpages, domains or IP addresses (Hamade 2008). Figure 2.8 shows the level of Internet censorship around the world.



**Figure 2.8** World map showing countries' level of censorship (Green & Karolidies 2005)

Censorship can be imposed for legal, cultural or religious reasons. Internet censorship

can be applied to webpages that include political, criminal, pornographic, religious or unethical content (Borns 1996; Green & Karolidies 2005; Peace 2003). According to Deibert et. al (2008), censorship can be divided into three categories: political, social and security. Political filtering can be applied to stop people getting access to fake, distorted or falsified information. Social filtering can be used for cultural reasons such as the management of pornography or gambling. Security filtering can be used for national security or to stop criminal acts or to identify information threat sources. Figure 2.9 highlights some highly-censored countries and indicates the category of filtering applied.



**Figure 2.9 Filtering types in highly-censored countries (Deibert et. al 2008)**

Many countries provide strong protections against censorship by law, but none of these protections are absolute and it is frequently necessary to balance conflicting rights in order to determine what can and cannot be censored. For example, China, Ethiopia, Iran, Myanmar, Pakistan, Saudi Arabia, Syria, Tunisia and the United Arab Emirates are highly-censored countries that combine political, social and security filtering.

High censorship may occur in these countries because of their cultures. The following section will described the impact of culture on information security.

### **2.2.3 Impact of culture on information security**



Research shows that China, Saudi Arabia, Ethiopia, Iran and Syria are all highly-censored countries that lack data protection laws. Their highly-censored status might lead us to believe that their information security policies would be strongly enforced and that information security would be high in these countries. However, the unexpected lack of a data protection law might lead us to expect low levels of information security.

Kaspersky, one of the leading companies that specialise in information security, reported statistics about information security and targeted attacks around the world (Kaspersky Lab 2011). Table 2.3 shows the twenty most frequently attacked countries.

**Table 2.3 Incidence of information attacks – highest 20 countries (Kaspersky Lab 2010, 2011)**

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

To understand these statistics we must realise that the number of attacks will be, to some extent, dependent on the number of people using computers and having access to the Internet. Thus, Italy has more than double the attacks than Thailand does, even they have similar populations. However, Italy has nearly double the rate of Internet use that Thailand does, and so has more attacks.

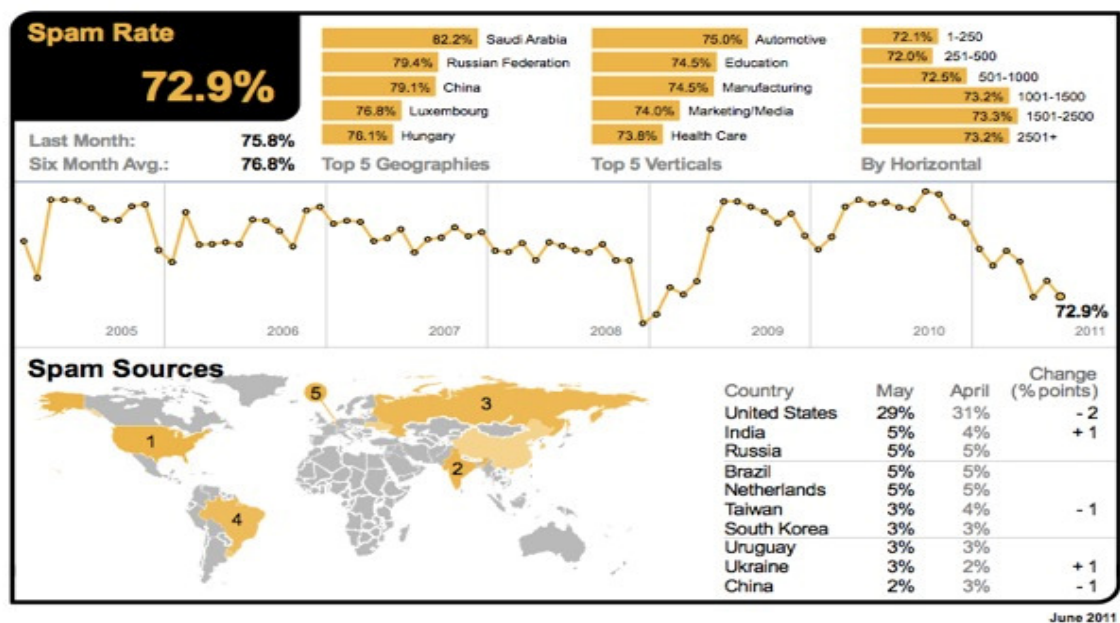
China was attacked 12,708,285 times in 2008, accounting for 53.665% of information attacks internationally. By 2009, this percentage had reduced to 46.75% of all attacks

(Kaspersky Lab 2010). Given that there are around 2 billion Internet users internationally, China only accounts for 21% of Internet users, which is far less than the percentage of attacks China experienced in either 2008 or 2009. By 2010, China's information attacks had dropped to 19.05% of all attacks (Kaspersky Lab 2011). This can be considered as a significant improvement against attack threats.

Saudi Arabian networks received 1.213% of total attacks in 2008, slightly increasing to 1.81% in 2009 (Kaspersky Lab 2010). However, Saudi Arabia accounts for only 0.002% of international Internet users, which is far less than the percentage of attacks experienced. So, Saudi Arabia has a vastly greater number of attacks than its population would suggest. In 2010 Saudi Arabia had nearly the same percentage of attacks (1.77%) (Kaspersky Lab 2011) as it had in 2009 and significantly more than it did in 2008. So, although China and Saudi Arabia both had extremely high rates of attack in 2008, China's attacks have reduced by 12%, and Saudi Arabia's attacks have increased by 45%.

This data leads to a number of questions. For example, what has caused these anomalies? Are these reasons related to either or both of the countries' high levels of legislation and censorship or their lack of data protection laws?

In addition, not only are the attack threats relatively high in the highly-censored countries; Symantec Lab identified Saudi Arabia and China in the top three most highly spammed countries. In June 2011, there were 39.2 billion spam messages sent. Saudi Arabia remained the most highly spammed country by percentage of total emails, with a spam rate of 84% and China was third (Symantec Lab 2011). Figure 2.10 shows the most spammed countries in the world.



**Figure 2.10 Most spammed countries (Symantec Lab 2011)**

We see in Kaspersky Lab data that huge differences occur in the way countries manage their information security and we wonder since all technologies are available for every one, what is about these countries are national level that makes them very so much in term of their response to information security. It is our contention that is some national cultural aspects, some behaviours that exist the national level that causes that variation. One of our purposes in this research is to assess the impact of national culture on information security and to propose the model which might address the problems that creates.

While the case of China is interesting, its sheer size and multiple languages make it difficult to study. This research therefore focuses only on exploring the reasons that Saudi Arabia is so prone to information security threats, and that the rate of threats shows little sign of falling.

The next section provides a brief background on Saudi Arabia.

### **2.3 Saudi Arabia**

Saudi Arabia is one of largest countries in the Middle East with approximately 28 million inhabitants, 99% of whom are Muslims (Alowain 2012). It has the two holiest places in Islam which are AlMasjid AlHaram (Alkaaba) in Mecca and AlMasjid Alnabaway (The mosque of the Prophet Mohamed Peace upon him) in Medina. It is an

oil rich country and the income from oil subsidises a welfare state controlled by the government (Jones 2011). The government is, in turn, dominated by the royal family, which numbers many thousands and controls most of the kingdom's important posts (Library of Congress 2006). Figure 2.11 shows Saudi Arabia's location (Wilson & Douglas 1994).



Figure 2.11 Location of Saudi Arabia (Wilson & Douglas 1994)

### 2.3.1 The Culture of Saudi Arabia

While a detailed analysis of the culture of Saudi Arabia is beyond the scope of this thesis, it is possible that some of the more obvious aspects of Saudi culture may influence ISA and InfoSec practices in Saudi Arabia. The Islamic religion plays a huge part in Saudi life and politics, and all decisions made by the King must be consistent with Islamic law. Saudis consider religion as the most important element of their identity (Moaddel 2006). The Saudis' interpretation of Islamic law severely constrains the roles of women and the mixing of the sexes is prohibited outside the family.

Tribes are one of the most influential factors in Arab life, particularly in the Arabian Peninsula. Reflecting their Bedouin heritage, a person's tribe offers protection from other hostile tribes or foreigners. While the tribes within Saudi Arabia are no longer hostile to one another, a person's tribe is still seen as a source of security (Alhagil 2001; Alothimin 2009).

Hofstede's description of Arabic culture is most enlightening:

*“These societies ... are also highly rule-oriented with laws, rules, regulations, and controls in order to reduce the amount of uncertainty” (Hofstede 2009).*

In describing Saudi Arabia’s low score for Individualism, he says that Arabic culture is manifested in a:

*“close, long-term commitment to the member 'group', [i.e.] a family, extended family, or extended relationships. Loyalty in a collectivist culture is paramount, and over-rides most other societal rules.” (Hofstede 2009).*

Although Saudi Arabia is now considered to be a modern country and is governed by Saudi laws, tribal culture still has a strong influence across Saudi society. For example, Saudi citizens still remain loyal to their tribes as a part of their culture and life style. Recently, several books and references that discuss genealogies of Saudi families and the tribes to which they belong have been published (Alhagil 2001). Moreover, there are books and websites specialising in specific tribes, including details of their ancestors, news, historical and current poets and poetry, areas, wars, rules and history of the tribe. This tribal level of information is often considered more important than the history of the country even though each tribe’s members are considered to be Saudi citizens (Aldosari 2009). Tribal culture mostly emphasises the role of men within the tribe. Several researchers believe that tribal culture has a negative impact on Saudi women because it assigns men more important roles in the society than women, despite the fact that both religion and Saudi law give women equal rights to men (Alfozan 2008).

Women in Saudi Arabia have lost some of their rights because of tribal culture rather than due to the culture of Islam (Alfozan 2008; Abuayen 2006; Refat 1998). There are some important variations between the culture of Islam and the Western culture. While some Islamic clerics believe that women should be veiled, most believe that women should not wear a veil and should cover only their hair (not their face). As a result of this conflict, not all women in Saudi Arabia have an independent ID card. Currently, the majority of Saudi women identify themselves using their family’s ID card, which does not include pictures for women. This weakness in the identification system for women in Saudi Arabia can introduce huge risks in various matters, including in relation to information security. In contrast, women in Western countries have independent ID cards with clear pictures to use in their activities (Bashir 2006; Albrik 1995).

This research investigates information security in Saudi Arabia as a highly-censored

country. The followings sections discuss some related aspects of information security in Saudi Arabia, such as Internet censorship and data protection policy.

## **2.3.2 Information use and data protection in Saudi Arabia**

### **2.3.2.1 *History of the Internet***

The Internet was introduced into Saudi Arabia in January 1999 after extended discussions and consultations within Saudi authorities (Alhajiri 2004; Khaild 2003). King Abdulaziz City for Science and Technology (KACST), an independent scientific organization administratively reporting to the Prime Minister of Saudi Arabia, was the provider and was responsible for the Internet at that time. It operated the Internet backbone as well as the local registry address space (KACST 2010). In 2004, the provision and filtering of the Internet was transferred to another government commission, the Communications and Information Technology Commission (CITC). CITC still provides and filters Saudi Internet (Alhajiri 2004; CITC 2012; KACST 2010). In 2005, CITC permitted the Saudi Telecom Company (STC) to build the required infrastructure to provide better communications (CITC 2012). The Internet in Saudi Arabia is censored and filtered against unethical or illegal websites (such as pornography). This is done with the permission of the Saudi government.

The introduction of the Internet faced various cultural, religious and political obstacles in the beginning (Alminshawhi 2003; Alhajiri 2004; Farid et. al 2009). In December 2000 the number of Internet users was only approximately 200,000. Usage has significantly increased in the last five years because of the spread of new technologies such as personal digital assistants (PDA) and smart phones. Now, the number of Internet users in Saudi Arabia is approximately 11 million which represents 39.2% of the Saudi population. Table 2.4 shows the number of Internet users in Saudi Arabia (CITC 2011).

**Table 2.4 Number of Internet users in Saudi Arabia (CITC 2011)**

<b>Date</b>	<b>Internet users</b>
December 2000	200,000
December 2003	1.462,000
December 2005	2,540,000
December 2008	4,800,000
December 2010	11,400,000

### *2.3.2.2 Internet use and impact of culture*

In comparison to other Arab countries, public access to the Internet in Saudi Arabia has been granted very recently. For example, public use of the Internet in the United Arab Emirates started in 1996, and earlier in some other Arab countries. The reason behind this delay in providing the Internet for public use in Saudi Arabia was the fear of possible negative impacts of the Internet on Saudi society, especially in matters relating to the culture of the society (Detmar 2003; Farid et. al 2009). The Saudi government sought the advantages of public Internet access while avoiding the possible negative impacts of the Internet on Saudi society. Therefore, a committee was formed to consider the possible methods to achieve this aim. Filtration of Internet websites was chosen as a solution to receive the benefits afforded by the Internet while protecting the Saudi culture from undesirable impacts (Alhajiri 2004; Khaild 2003). Filtered websites include those containing sexual matters, content conflicting with Islamic culture and content conflicting with the rules of Saudi Arabia. Governmental agencies, like KACST and CITC, have responsibility for managing and monitoring the filtration program. From time to time, these agencies receive requests from the public to close or filter websites that have sexual references and that have not already been closed by existing filtration. There are some difficulties associated with filtering websites, especially those with sexual references, because of their rapid development and spread (Alhajiri 2004; Khaild 2003).

There are several other issues associated with the impacts of the Internet on Saudi society and culture. The most frequent complaints about the Internet relate to the spreading of rumors and defamation of people from both genders. These occurrences can create more risks, especially in tribal societies. Of particular concern to Saudi

culture is that photos of women cannot be published on websites as it might invade their privacy or their family's privacy. This can lead to further social problems for affected families, particularly in tribal societies (Carol 2006; Alqahtani 2006).

Based on all of these facts regarding the Islamic culture and tribal culture, both of which are central to Saudi culture, it can be seen that there are significant cultural differences between the Saudi and Western cultures. These differences are most notable in issues related to women and tribes. Also, there are problems related to the privacy and identification of Saudi women on the Internet. Hence, this issue should be taken into consideration when discussing how to get the benefits from the Internet while protecting the Saudi culture from the undesirable impacts of Internet and ensuring the security of usage.

#### **2.3.2.3      *Data protection law***

Data protection is designed to protect personal data and to ensure privacy and security (Stallings & Brown 2008; Straub et. al 2008). While the need of data protection law in the country is necessary; Saudi Arabia does not have data protection laws. Recently, Saudi Arabia has only the electronic crimes law but not for data protection law.

The Saudi Ministry of the Interior proclaimed on 26 March 2007 the first statement about the electronic crimes law and penalties for illegal usage (Ministry of Communication and Information Technology 2009).

### **2.3.3 Information security in Saudi Arabia**

Saudi Arabia, like the rest of the world has embraced global digital technologies. As a result of this expansion it is bound to incorporate steps and actions that will allow for secure and safe operations of information systems. With more than three quarters of the Saudi population and businesses engaged in the use of modern technology, it becomes imperative to introduce measures and mechanisms which allow for safer functions and better utilization of information system technologies.

Over 40 percent of the total Saudi population comprises of youth and young professionals (Alnatheer & Nelson 2009), and the usage of the information systems and other digital devices have become more frequent, therefore there is a need for increased



security and use.

At present, in Saudi Arabia, the government has enacted the National Communication and Information Technology Plan. The aim and objective of this entity's existence and establishment is to equip Saudi Arabia with the means to compete with developed countries. Saudi Communication and Information Technology is another major entity constituted for administration over Information Technology based organizations (HSBC 2010).

### **Review of Existing Models**

#### **Balanced Scoreboard Model:**

This model was introduced for the purpose of determining the areas of improvement and areas where there is need for government assistance. The test of available resources and infrastructure was also undertaken under this model. This model study was taken for as a recommendation work towards future progress in Saudi industries (Abu-Musa, 2007).

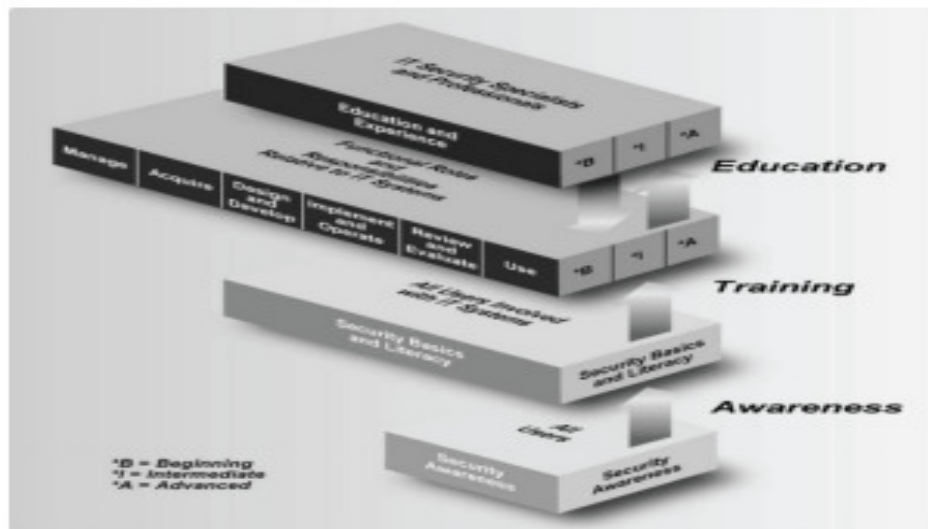
Lawton has assessed the effect of this model with regard to the correlation establishment between the strategies to be structured and the practical actions taken in the light of these strategies. Balanced scoreboard model is introduced as an initiative towards integrating the previously existing functions of finance with that of the modern methods through the aide of information technology and information systems (Lawton 2002).

Balanced scoreboard model serves as a litmus test to determine the business affectivity and coherently with the goals and objectives that understated against a given set of project and business activity.

### **SETA**

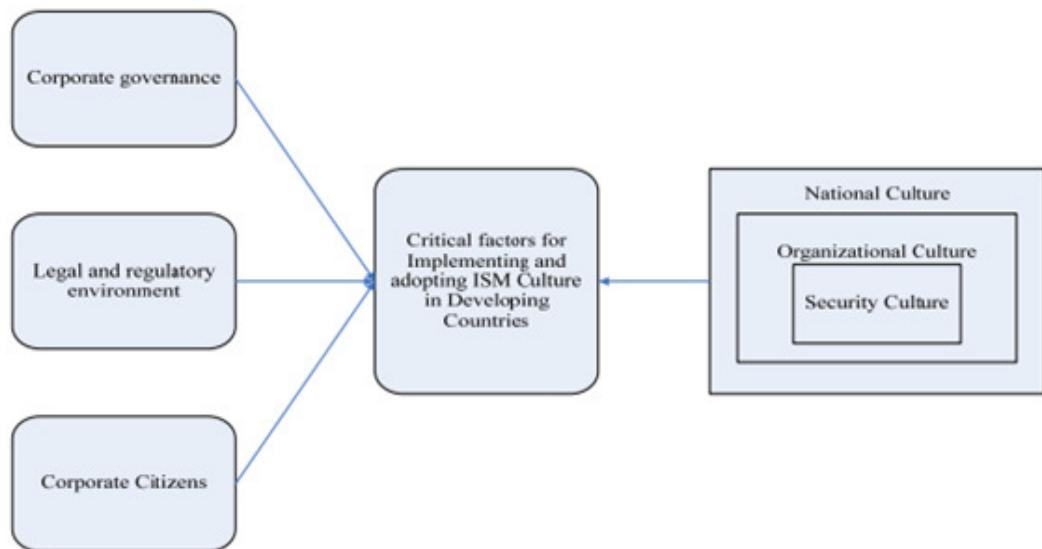
In collaboration with the more established countries with regard to Information system networks, Saudi Arabian government has initiated systematic working schemes. SETA is acronym for Security, Education, Training and Awareness program. The multi-dimensional program has been initiated for the purpose of bringing about reforms and

development with regard to the information system functioning in the different sectors of Saudi Arabia.



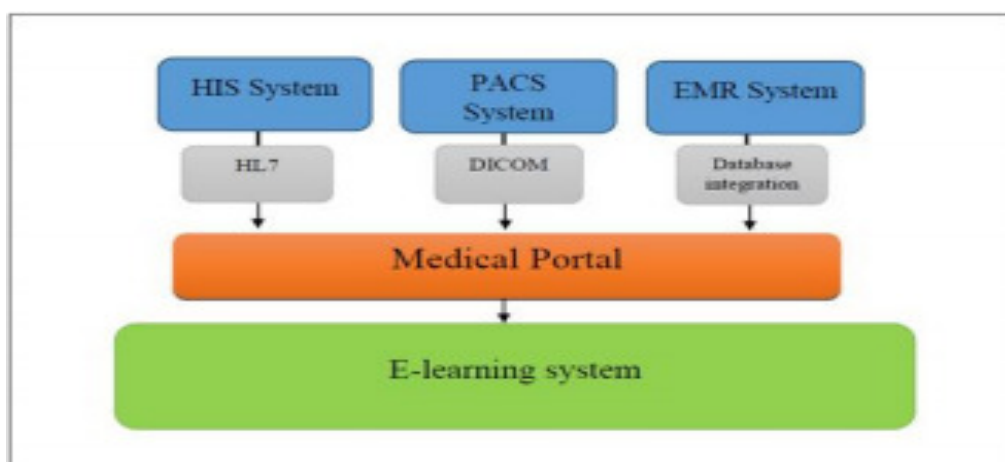
**Figure 2.12 SETA program**

The fragile nature of information system is a serious concern expressed globally. SETA is put in place for the purpose of minimizing such events and accounts and making the working of information systems more secure with regard to professional and financial decisions and activities undertaking.



**Figure 2.13 Factor for implementation and adopting IS culture and practices in Saudi Arabia (Alnatheer & Nelson 2009)**

The Saudi Arabian government has taken steps towards implementing information systems in the educational sector. One of the key examples in this regard is that of King Fahd University where electronic means are used towards the lecture delivering process and other online resources facilities for the students. Further improvement is aimed at through its implementation on grass root level in the academic disciplines of Saudi education sector (Chen et al. 2005).



**Figure 2.14 Information systems implementation in King Fahd University (Albarrak 2014)**

Albarrak has conducted research with regard to the implementation of the same information system enabled support in the hospital and medical health care sector. College of Medical and King Saud University is assessed for the integration of information system. The aim is to implement it in different sectors of the hospital and research center. The model aims at introducing a model based learning program which will allow for practical execution of the plans undertaken (Albarrak 2014).

Mohammed Boujettif has undertaken research with regard to the means and measures necessary towards creating awareness and enhancing the daily routine activities which will allow for improved information systems functioning (Boujettif & Wang 2007). The research is directly addressed towards the Middle East business environment. Stanton et al. has supported the fact that the human side of intelligence and careful handling of information technology is an integral part towards successful operations of e- businesses and educational institutions (Stanton et al. 2003).

Information system as whole consists of number of sub units within the information technology paradigm. These include security management, data security and network operations and security. Various models are used for the purpose of ensuring standardized operations. Each of these models has its characteristic functions and application domain.

### **InfoSec Models:**

Acronym for Certified Authorization Professional is a program and model that allows understanding the operations and functions of the information enabled environment in a more flexible and effective manner minimizing the possible breaches in the network (Willett 2008).

### **McCumber InfoSec Model:**

John McCumber is widely known for the model he presented in the field of information technology. It was introduced towards the early 1991. Since its development and the overall progress in the field of information systems, it has become an essential tool towards establishing the security and information assurance functions. The central idea is to interlace the basic intertwined functions within and allow for a robust system

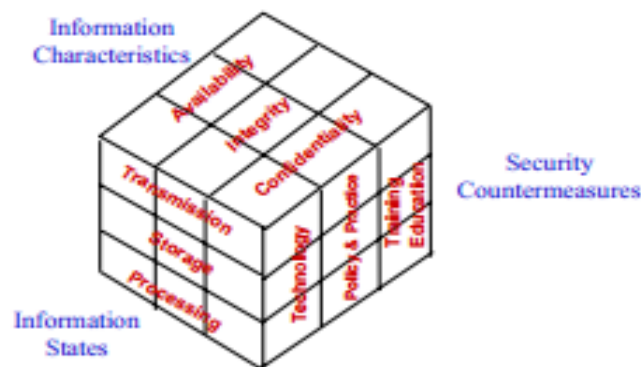
supportive of effective security network based system (Maconachy et al. 2001).

This model was developed at the time when the information systems were relatively less equipped with security means and mechanism. As a result an effective system of operations and security activities was needed. Overcoming the threats and online hazards that are present in the different forms both internally and external of a network are addressed in this particular model.

This model addresses the cross network security, LAN enabled computer systems security and personal desktop based computer systems and as a result finds large scaled applications.

### McCumber INFOSEC Model

---



**Figure 2.15 McCumber INFOSEC Model (Maconachy, et al. 2001)**

Based on its generic and large scaled application ability, it is structured as cuboids covering multiple domains of information technology and systems. The security services rendered by this model allow for timely operations and timely activity and node connection of the client with the servers. This timely function makes it more effective with regard to minimizing the external threats faced in form of spammers and other malicious online content. Other functions and features entailed in this model include confidentiality of the information shared across the network, non-repudiation, authentic connection key words, integrity and counter measures.

**NSTISSC Model:**

Acronym for National Security Telecommunications and Information Systems Security Committee is an American based concept aimed at providing more effective support system towards protecting the online information and online activities. It was formally administered over and guided by the Federal Government of United States of America. George W. Bush was the front runner leader in this entire activity approving it's working (Armistead 2007). This model is basically a continuation and development of the previously existent models established for secure online operations (NSA 2000).

The scope of this particular model is expanded to the application domain of military intelligence services, coding and decoding of the data and controlling over the sensitive information of the military and defense units of United States of America. With gradual progress taking place in the security network of American intelligence, NSTISSC model has been revamped as Committee on National Security Systems (CNSS).

NSTISSC is also dubbed as the C.I.A model based on its scope and function of covering the areas of Confidentiality, Integrity and Availability.

**GRC Model:**

GRC is acronym for Governance, Risk Management and Compliance based model is set of three major variables that work together towards a successful information system model and operations. It is one of the emerging models in the field of e-governance implemented towards improved services delivery by the government at large level. Governance pertains to the use of electronic means and information technology aimed at improving the performance of the employees and other online clients. Management is the adjustment of the resources associated within (Schönthaler et al. 2012).

Within the GRC model, the aim is to bring about reforms and improvement in E-administration, e- management, e-financial handling, legal handling in the electronic context and domain and quality control and audits.

Further specialization within GRC model includes I-GRC (Integrated GRC) model aimed at providing further enhanced security and management system in the e-environment.

## **IA-CMM:**

Acronym for InfoSec Assurance- Capability Maturity Model is another set of system that aims at providing best solutions and guidelines towards successful implementation of Information System based environment. Bell and LaPadula Model of Information Security System is another model used for the Information system assurance (McLean 2000).

Unfortunately, information security in Saudi Arabia has come under threat because the country is suffering from several types of risks. As described in section 2.2.3, Saudi Arabia has very high levels of information threats.

By considering the number of Internet users in Saudi Arabia in the context of the statistics from Kaspersky, NetWitness, Trend and Symantec, it is clear that Saudi Arabian users need further help to be more aware of Internet security and information threats. Introducing and publicising a new data protection is necessary to increase users' awareness and reduce further risks.

### ***2.4 Justification for the study***

Although the literature review has shown that InfoSec varies from country to country, InfoSec must be understood as a global phenomenon, not a national one. The fact that InfoSec is quite demonstrably low in Saudi Arabia, China, Russia etc. is not a problem solely for these countries. Poor InfoSec in any of these countries means that their computers and networks are available to be used to launch attacks on computers any where in the world. So, it is vitally important to understand why such countries are so much at risk and to help them develop strategies to reduce that risk.

Almost all previous studies of InfoSec have focussed on technical or organizational issues associated with InfoSec. However, despite the enormous variations from country to country, few have focussed on the social, cultural or legal differences that exist between countries. It appears that, several of these at-risk countries are highly-censored countries, and that various cultural and social issues within these countries may have influenced their low level of InfoSec. So, it is worth while to explore these possible relationships.

Finally, most studies of InfoSec have focussed on ISA within organizations or InfoSec practices within organizations. It appears that this is the first study to undertake a broad ranging analysis of the ISA of the general public and the ISA and InfoSec of multiple organizations across a whole country. Having access to both sets of data allow relationships to be found between behaviours of the general public and impact on organizations.

This study focuses on Saudi Arabia because it combines a number of almost unique characteristics. Firstly, Saudi Arabia has one of the highest rates of InfoSec attack per Internet user in the world and the rate of attack is only beginning to show small signs of falling. Secondly, it is one of the most recent entrants to the Internet, so it is possible to observe behaviours and interactions that almost certainly do not occur in more advanced Internet-using countries. Thirdly, there are marked social, cultural and legal differences between Saudi Arabia and most other countries, and it appears that these differences may influence InfoSec. Finally, Saudi Arabia is in the process of introducing a new data protection law, which allows us to see, to some small extent, the impact that this new law is likely to have or what is a chronic InfoSec problem.

## **2.5 Conclusion**

It can be concluded that InfoSec in HCC is a serious problem that warrants further investigation. Consequently, exploring the causes of these problems and providing appropriate solutions are the main objective of this research. The literature review has highlighted some of the information security problems in Saudi Arabia. The poor understanding of these problems motivated this research. The shortage of literature about InfoSec in HCC countries can be addressed through the application of a rigorous methodology to gather data and identify existing problems. The next chapter describes the methodology used to achieve the research objectives.



## **Chapter 3 Research Methodology**

### **3.1 Introduction**

A review of the relevant literature has shown that there are few, if any, studies of Information Security (InfoSec), from both an organizational perspective and from an end-user perspective, especially in regard to a Highly-Censored Country like Saudi Arabia. The central research question of this thesis is “How are information security awareness and practices impacted by the highly-censored culture in Saudi Arabia?”

The specific objectives of this research are to:

1. Determine the level of Information Security Awareness (ISA) among the Saudi Arabian public.
2. Determine InfoSec expertise in Saudi organizations:
  - a. Determine the use of InfoSec laws, standards and policies.
  - b. Determine InfoSec practices in Saudi organizations.
  - c. Determine InfoSec risks in Saudi Arabia.
3. Understand ISA, InfoSec practices and cultural implication in Saudi Arabia.
4. Develop process model of InfoSec CAP that can be used to address these weaknesses.

The purpose of this chapter is to describe the philosophical and methodological foundations of this research, which will be used to achieved the objectives above.

### **3.2 Overview of research methodology**

A research methodology describes and develops the stages that will be used to achieve the research objectives (Creswell 2003; Johnson & Christensen 2004; Tashakkori & Teddie 1998). It is used to link theoretical frameworks and the collection of source material (Alvesson & Deetz 2000). This research uses a quantitative approach to data

collection. The following sections will detail the research methodology.

### **3.2.1 Quantitative methods**

The main concerns of the quantitative paradigm are to ensure that measurement is reliable and valid (Cassell & Symon, 1994; Hancock & Algozzine 2006). Quantitative methods achieve high levels of reliability in gathered data via controlled observations, laboratory experiments, mass surveys or other research manipulations (Kealey & Protheroe 1996).

This thesis used a survey method to gain a greater understanding of the problem and hence to find appropriate solutions.

#### **3.2.1.1 Surveys**

This thesis used electronic surveys to collect data from Saudi Arabia. The research involved two surveys. The first survey was designed to measure awareness of information security among the general public in the studied country. In the second survey, staff in Information Technology (IT) departments in both government and business in Saudi Arabia were surveyed.

##### **3.2.1.1.1 Survey design**

The purpose of a survey is to gather data from a sample of the population with a view to discover or measure a certain issue (Creswell 2003; Hancock & Algozzine 2006). Survey methods can cover very large samples over large distances. Flexibility in collecting data and reliability are two justifications for using a survey method. In addition, culture can produce obstacles to using other methods such as interviews or observation. In this study, for example, Saudi Arabian women are not permitted to speak to unrelated men for cultural reasons. Therefore, an electronic survey administered over the Internet can help to collect a large sample in a short time and to involve women.

The survey method incorporated four phases:

- i. **Select the survey type:** In general, there are two common types of surveys: cross sectional, which are concerned with one point in time; and longitudinal,

which are concerned with study over time (Creswell 2003). This research used cross sectional surveys because it is concerned with examining the situation at one point in time. Another use for the cross sectional survey technique is comparing and contrasting two or more samples to identify similarities and differences (Creswell 2002).

- ii. **Design the survey:** The first component of the survey design was writing all appropriate questions that related to the topic. All questions used were semi-closed-ended questions that combined the advantages of closed-ended questions and open-ended questions because the respondents have to answer the questions and in some question there are other option to give them some space to write and add some more information if they want. Once all potential survey questions were developed, a pilot study was conducted to test the survey. Feedback was used to enhance the quality of the questions, to avoid further problems such as respondents' misunderstanding a question and to ensure the time taken to complete the survey was acceptable.
- iii. **Design instruments for data collection:** Instruments were very important to achieve high quality data collection in this research. Designing the questions to be distributed via online web pages and having the surveys ready for distribution to the public and IT Staff was essential. The Survey Monkey website was used to deliver the surveys to people because it provided access anytime and anywhere. It also afforded the advantage of storing the data securely and in a format that was easy to extract for analysis.
- iv. **Obtain a high response rate:** To ensure a high response rate, reminder messages were sent to respondents who were expected to complete each of the surveys. This method was particularly useful for the IT support department staffs who were asked to complete the InfoSec survey. The survey was open to respondents for three weeks, with one reminder sent each week to staff who were yet to complete the survey.

#### 3.2.1.1.1 Information Security Awareness (ISA) survey

The ISA survey administered in this research was designed to measure awareness of

information security in the general public in Saudi Arabia, thereby providing a better understanding of the research problem. The survey questions were selected from an instrument developed by the Cyber Security Organization in Malaysia in consultation with KPMG. All of the questions were included except in the case where they would have been inappropriate for the Saudi culture. The focus of the Cyber Security Organization instrument was very similar to the focus of this research's investigation of ISA within the general public. While the Cyber Security Organization questions were developed in Malaysia, they were deemed to be the most appropriate for use in this research due to the absence of other related existing studies and instruments internationally. Some questions from the Cyber Security Organization survey instrument were omitted from this research because it included questions about children's levels of ISA as perceived by parents while this research is entirely targeted at adults. Other minor modifications, such as the ordering of questions, were also made.

The survey was translated into the Arabic language because Arabic is the native language of the target respondents. The survey was accessible via online links placed on popular Saudi educational and business websites and forums with a letter that informs potential participants about this study with a clear announcement that it is to be completed by "only Saudi Arabian people". This worked well, resulting in 462 responses from adults.

Copies of the survey in both English and Arabic are presented in Appendix A and Appendix B. The survey is divided into three sections:

- i. **General background:** This section contained general questions about the participants, such as gender, age, education, organization type, organization sector, job position and location (i.e. urban or rural). This information provided background knowledge about each participant and was used to analyse the impact of background on ISA (Approx 4 minutes).
- ii. **General practice and perception / confidence level:** This section contained 19 questions about general information security practices. Questions addressed issues such as the purpose of Internet use, electronic device security, information threat awareness, password security level, data backup, the use of information security software and security incident report awareness. This section included a

variety of InfoSec practices questions to establish an understanding of the awareness level of each participant. In addition, this section recorded participants' confidence level about information obtained via the Internet and their data privacy needs (Approx 6 minutes).

- iii. **Promotion preferences:** This section was designed to determine which communication methods the respondents believed would be most effective for promoting awareness of InfoSec to the Saudi public (Approx 3 minutes).

#### 3.2.1.1.2 Information security survey for organizations

The second survey was designed to investigate and determine InfoSec practices in Saudi Arabian organizations. Survey respondents were recruited from IT departments across the public sector, private sector and non-profit organizations. The survey questions were selected from instruments developed by various expert organizations: the Cyber Security Organization in Malaysia in consultation with KPMG; the Center of Excellence in Information Assurance in Saudi Arabia; and the Al-Elm Information Security Company which is a national company owned by the Public Investment Fund (PIF) in Saudi Arabia.

Survey questions were selected from these existing instruments using best practice guidelines. Some questions were omitted because they were not directly associated with the goals of this research or were inappropriate for the Saudi culture. Because of questions number limit; some repetitive questions that can examine one aspect for confirm purposes have been omitted and replaced with direct questions that can examine some Saudi culture practices in InfoSec (questions 42-47 in section C3: Information security risks in organization). Also, some questions were modified to ensure they were appropriate and easily understood within the Saudi culture. These changes were made to ensure that the survey provided an accurate record of the understanding of InfoSec in Saudi Arabia.

The survey was translated into the Arabic language because Arabic is the native language of the target respondents. The survey was accessible via online links emailed to Saudi Arabian organizations with a clear announcement that it is to be completed by "IT department people". This worked well, resulting in 124 responses from

organizations.

Copies of the survey in both English and Arabic are presented in Appendix C and Appendix D. The survey is divided into four sections:

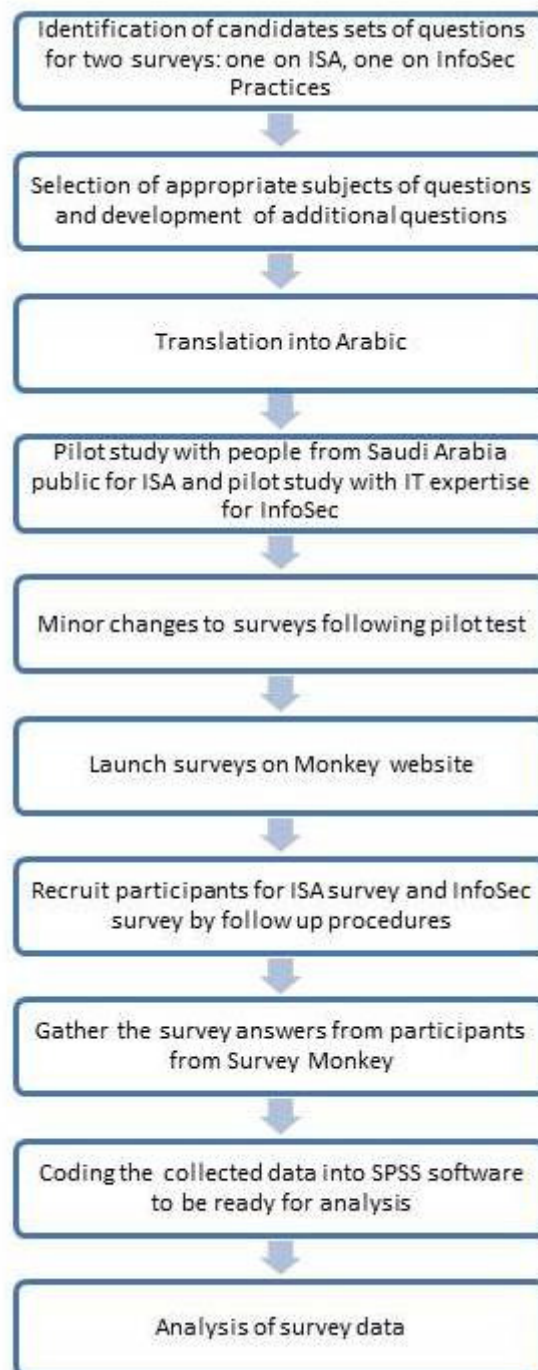
- i. **Organization background:** This section contained questions recording the nature, sector, size and name of the organization, and whether it had an IT department existence and its budget. This information was required to establish an understanding of the participating organizations and respondents from within the IT department. This information provided background knowledge about each organization and respondent. Information about the organization could be used to analyze the impact of organizational characteristics on InfoSec (Approx 6 minutes).
- ii. **Organizational information security data protection laws, standards & policies:** This section contained 12 questions designed to investigate the existence, appropriateness and power of InfoSec laws, standards and policies in Saudi Arabian organizations. It included an examination of applied InfoSec law, standards and polices (Approx 4 minutes).
- iii. **Information assurance, tools & measures in organizations; Information security risks:** This section was divided into two parts: InfoSec assurance and InfoSec threats. The first part was designed to examine the strengths and weaknesses of InfoSec tools (e.g. vulnerability assessment, password strength, firewalls, limitations of Internet access, software updates, encryption, anti-virus software, server physical security, device security, data backup policies and InfoSec incident reports) in Saudi Arabian organizations. Questions in the second part investigated common InfoSec threats. Additional questions were included to investigate the impact of the Saudi culture on InfoSec. Issues considered include the impact of the tribal society's connections in facilitating information access and the current limitations on female identification (Approx 7 minutes).
- iv. **Promotion preferences:** This section was designed to identify the challenges of applying information security standards and staff training in Saudi Arabian

organizations to identify the best methods that respondents believed would be most effective for promoting and increasing InfoSec practices to the Saudi organizations (Approx 3 minutes).

### ***3.3 Research methodology framework***

A research framework describes the combination of research methods used for conducting the research successfully (Hancock & Algozzine 2006).

This research was conducted in ten phases. Figure 3.1 shows the phases in the research process. Each of these steps and the methods used are explained below.



**Figure 3.1 Research methodology framework**

**Identification of candidates and sets of questions for two surveys:** The first phase was the identification of candidate and sets of questions for each of the two surveys: one on ISA and one on InfoSec practices. Best practice questions from well known information security organizations were used to enhance the survey quality.



**Selection of appropriate questions and development of additional questions:** In this phase, some questions in both surveys were modified to ensure they are appropriate for participants' background and culture. Some questions were also added to each of the surveys to allow the research objectives to be achieved.

**Translations into Arabic:** Both surveys were translated into Arabic (the participants' native language) and then translated back into English. This process was completed to ensure that the meaning of questions did not change. All identified misunderstandings resulting from the translations were corrected.

**Pilot study with people from Saudi Arabian public (ISA survey) and IT experts (InfoSec survey):** The pilot study was conducted to enhance the quality of the survey questions and reduce the likelihood of further problems. Also, the time for survey completion was measured to ensure that it was reasonable. The pilot tests involved 12 people from the Saudi Arabian public for the ISA survey and with 7 IT experts for the InfoSec survey.

**Minor changes to surveys following pilot test:** After the pilot study, the feedback was reviewed and enhancements were made to some questions in each of the surveys. These changes were made so the surveys were more appropriate, logical and realistic.

**Launch surveys on Survey Monkey website:** Survey Monkey website was used to facilitate electronic data collection. This website provided the relevant people with access to the surveys anytime and from anywhere during the data collection period. It also provided secure data storage and data management that facilitated the data analysis.

**Recruit participants for ISA survey and InfoSec survey using follow up procedures:** URLs for both the ISA survey and InfoSec survey were generated and sent to potential participants. The ISA survey link was advertised in forums that were popular in Saudi Arabia (e.g. hawaa, Saudi employees and educational forums). The InfoSec survey link was directly emailed to many IT departments in Saudi organizations. Participants followed the links and completed the surveys online via the Survey Monkey website.

**Gather participants' survey answers from Survey Monkey:** All participants' responses to the ISA and InfoSec survey questions were extracted from the Survey Monkey database and all responses were translated into English.

**Code the collected data into SPSS software to prepare for analysis:** All responses to the ISA and InfoSec surveys were coded into SPSS data analysis software. A check of all entries was conducted to ensure that all responses were generally as expected (i.e. that all responses were genuine).

**Analysis of survey data:** Finally, the tools within SPSS were used to analyse the ISA and InfoSec survey responses and conduct statistical tests. Section 3.4 describes this analysis in further detail.

### **3.4 Data analysis**

Analysis is necessary to understand the collected data and use it effectively. Analysis of the data obtained through the two surveys was required to obtain a clear picture of the current Information Security practices in Saudi Arabia, as an example of a highly-censored country.

The data analysis involved bivariate descriptive analysis, which is a technique that sits on the spectrum between univariate and explanatory analysis. It establishes similarities or differences between characteristics, or the connection between them (Blaikie 2003). In this research the collected data was categorized and coded. Similar answers were then matched and a description was developed.

SPSS was the statistical computer software package used to analyze the data collected from the surveys. SPSS enables data to be coded, retrieved and stored flexibly and effectively. It provides tools for classifying, sorting and arranging information and also for analyzing data, identifying themes and determining patterns. Use of SPSS reduces the analysis time and provides automated and accurate results.

Descriptive statistical analyses and Chi-Square test techniques were used to achieve the research objectives. The data analysis and results of the surveys are presented in detail in the following two chapters.

### **3.5 Conclusion**

This chapter has explained the processes and procedures that were used to collect and analyse data in this study to achieve the research objectives. This research aims to determine the level of ISA among the Saudi public and to understand current InfoSec practices in organizations in Saudi Arabia. The chapter began by identifying a suitable methodology. A quantitative approach was taken to meet the research objectives, with a survey method used to gain a greater understanding of the problem and hence to find appropriate solutions. The following chapter (Chapter 4) presents the analysis and results of the ISA survey. Chapter 5 presents the analysis and results of the InfoSec survey.

## **Chapter 4 Results and discussion for Information Security Awareness**

### **4.1 Introduction**

This chapter presents and discusses the results of the ISA survey. This survey was completed by members of the general public in Saudi Arabia. The first section describes the participants' characteristics including gender, age, education, sector type and living area. The second section discusses the participants' general practices related to ISA such as information threat awareness, password strength, password changes, data backup, anti-information threat software and information security incidence report awareness. The final section presents effective methods for promoting information security awareness based on participant feedback.

The questions in this survey were semi-closed ended questions. This type of question combines the advantages of closed-ended questions and open-ended questions. Consequently, survey answers will include some data which cannot, on any logical basis, be ordered numerically, hence there is no possibility of using parametric statistical tests which require numerical data. The information in this chapter was created through the application of descriptive statistical analyses and Chi-Square test techniques were used to achieve the research objectives.

### **4.2 Background of participants**

#### **4.2.1 Response rate and demographics**

There were 462 adult participants in this study, however, the number of respondents to questions varied significantly because all of the questions were optional. An inspection of the data does not suggest that there is any systemic reason for non-completion, i.e. no particular group of respondents chose not to answer particular sets of questions. Although the non-response rate was sometimes as high as 50%, for an individual question there were still over 300 respondents for every question which is sufficient for the purposes of this research. However, the non-response rate itself is interesting; given the high level of censorship of the Internet in Saudi Arabia, it is possible that Saudis are not familiar with online surveys or the expectation that all questions should be

answered.

Response rates are often used to evaluate the quality of survey data. Equality of responses based on gender can reduce study bias. However, non-response bias will occur if respondents and non-respondents differ on the dimensions or variables that are of interest to the research. This study involved 164 males (representing 35.5% of respondents) and 298 females (representing 64.5% of respondents). The most likely reason for this difference is that Saudi females have more time to participate in this study because they are housewives at home or unemployed, while males have less available time due to work commitments. Table 4.1 shows the number and gender of participants.

**Table 4.1 Participant gender**

What gender group do you belong to? (N=462)				
		Frequency	Percent	Valid Percent
Valid	Male	164	35.5	35.5
	Female	298	64.5	64.5
	Total	462	100.0	100.0

Participants were asked about their age because this was an interesting consideration in relation to level of awareness. Table 4.2 shows that the majority of respondents were aged 23 to 42 years.

**Table 4.2 Participant age**

What age group do you belong to? (N=462)				
		Frequency	Percent	Valid Percent
Valid	18-22	65	14.1	14.1
	23-27	120	26.0	26.0
	28-32	137	29.7	29.7
	33-42	103	22.3	22.3
	43-59	35	7.6	7.6
	60-100	2	0.4	0.4
	Total	462	100.0	100.0

#### 4.2.2 Education

Since ancient times, education has been vital in the spread of knowledge and awareness. The purpose of recording each participant's education in this study is to understand the education of the participants providing feedback and consider the impact of the level of participant education on ISA. Table 4.3 shows that 51.5% of participants had an undergraduate degree, 12.1% held a diploma and 24% had a high school qualification. The remaining percentage was shared between doctoral degrees (1.7%), master degrees (6.3%) and intermediate school degrees (4.1%). It seems participants were well educated considering that nearly 60% of participants held an undergraduate degree or higher. Given that 92% of respondents were aged 42 or less, it would be reasonable to assume that much if not all of their education took place in the 'information age'. Coupled with reasonably high education levels, this might lead us to expect reasonably high levels of ISA.

**Table 4.3 Participant education level**

What is your highest education level? (N=462)				
		Frequency	Percent	Valid Percent
Valid	Doctoral Degree	8	1.7	1.7
	Master Degree	29	6.3	6.3
	Undergraduate Degree	238	51.5	51.5
	Diploma	56	12.1	12.1
	High School	111	24.0	24.0
	Intermediate School	19	4.1	4.1
	None	1	0.2	0.2
Total		462	100.0	100.0

#### 4.2.3 Sector type and working status

Questions were asked about organization type (government or private), industry sector (e.g. employed, unemployed, student etc.) because it was thought that these characteristics might be associated with different levels of ISA. Results will also be presented to show areas of strength and weakness in awareness between organizational types. Table 4.4 shows that 39.6% of respondents belonged to the government sector and 15.8% belonged to the private sector. The rest of the participants (44.6%) were not employed, self-employed or students as shown in Table 4.5.

**Table 4.4 Participant organization type**

Please select the appropriate type of organization that you are currently working for: (N=462)				
		Frequency	Percent	Valid Percent
Valid	Government	183	39.6	39.6
	Private	73	15.8	15.8
	Other	206	44.6	44.6
	Total	462	100.0	100.0

Table 4.5 shows that, of the 206 participants who chose 'other' in the previous question, 61.7% were not employed and 24.6% were students. 6.9% of respondents were self-employed. They are assumed to be working in the private sector.

**Table 4.5 Participant working status**

What is your current working status? (N=248)				
		Frequency	Percent	Valid Percent
Valid	Self employed	17	3.7	6.9
	Not Employed	153	33.1	61.7
	Student	61	13.2	24.6
	Other	17	3.7	6.9
	Total	248	53.7	100.0
Missing	System	214	46.3	
Total		462	100.0	

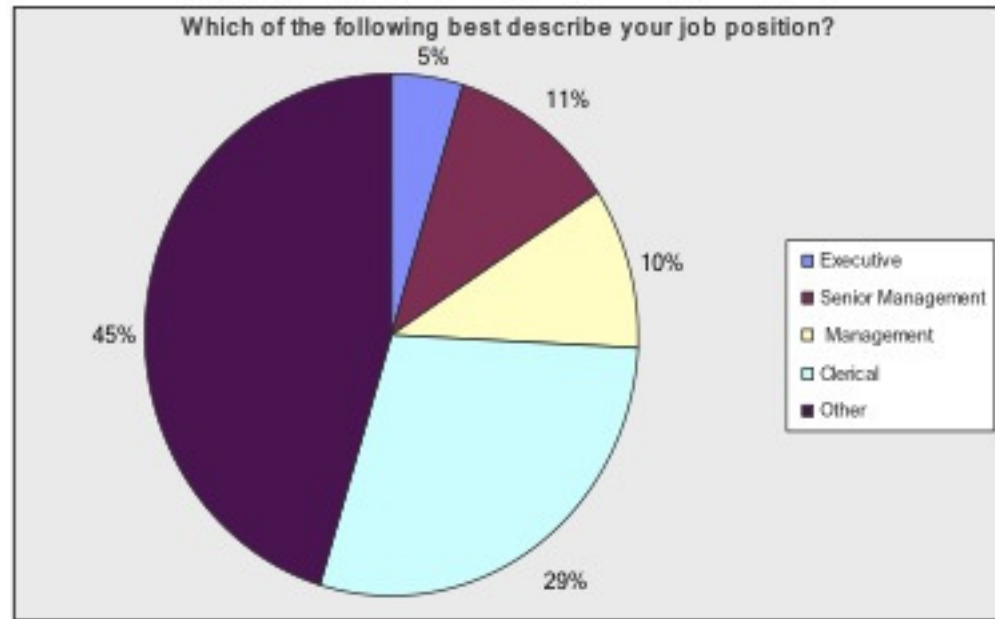
Table 4.6 shows the participants' distribution across industry sectors. Education was the most common sector (32%), followed by the military sector (10.6%) and then similar distributions of participants in the health services and trading and contracting sectors (4.3% each). The banking and finance sector both had the same percentage of responses (1.3%). Overall, the highest percentage of response at 36.8% was 'other'. As identified in the previous questions, these responses were from participants who had already indicated they were unemployed or were students.

**Table 4.6 Participant industry sector**

<b>Please select the appropriate type of industry that your organization belongs to: (N=462)</b>				
		Frequency	Percent	Valid Percent
Valid	Education	148	32.0	32.0
	Military	49	10.6	10.6
	Health Services	20	4.3	4.3
	Trading & Contracting	20	4.3	4.3
	Banking & Finance	6	1.3	1.3
	Social Affairs	6	1.3	1.3
	Justice	6	1.3	1.3
	Media	6	1.3	1.3
	Food & Agriculture	5	1.1	1.1
	Industry Services	5	1.1	1.1
	Transportation	4	0.9	0.9
	Energy	3	0.6	0.6
	Tourism	3	0.6	0.6
	Islamic Affairs	2	0.4	0.4
	Water	2	0.4	0.4
	Foreign Affairs	2	0.4	0.4
	National Economy	2	0.4	0.4
	Planning and Housing Sector	1	0.2	0.2
	Labour	1	0.2	0.2
	Information & Communication	1	0.2	0.2
	Other	170	36.8	36.8
	Total	462	100.0	100.0

The last question in this section was concerned with the role or job position for those participants who were employed. This question allows examination of whether people in high level positions are more aware of information security. Usually, regulation tracking (i.e. ensuring compliance with government regulations) is the responsibility of one of the highest level positions in an organization. If people in high level positions do not have adequate awareness, this can lead to problems in relation to information security. Figure 4.1 describes responses from 462 participants about their job position. There were 253 respondents in specified roles: 5% as executive managers, 10% senior management, 11% management and 29% clerical staff. The other 45% of respondents are not employed or are students. They are shown below as “Other”.





**Figure 4.1 Participant job position**

#### **4.2.4 Living area**

The final question asked participants about the type of area in which they lived to examine whether people in big cities have a better awareness than people in small cities and towns. They were also used to avoid bias that can occur if all responses come from a particular city. Table 4.7 shows that 92% of responses were from cities and towns and 8% of respondents were from villages. This result is consistent with the population as a whole because people in Saudi Arabia are migrating from villages to cities seeking jobs, education and health services.

**Table 4.7 Participant living area**

Do you live in a rural or urban area? (N=462)				
		Frequency	Percent	Valid Percent
Valid	Urban	425	92.0	92.0
	Rural	37	8.0	8.0
	Total	462	100.0	100.0

However, it is still desirable that the urban population in Table 4.7 be spread across both large and small cities. Riyadh, which is the capital city of Saudi Arabia with a population of around 5 million, was the source of 37.4% of responses. Of the other responses, 10.2% were from Jeddah, 9.1% from Almadinah, 7.1% from Qasim, 6.3% from Dammam, 5.4% from Makkah, 3% from Abha and 0.6% from Arar. The

remaining 20.8% of responses were from 27 different cities and towns in Saudi Arabia. It therefore appears there is a good distribution of respondents across large cities, small cities and other towns (see Figure 4.2).

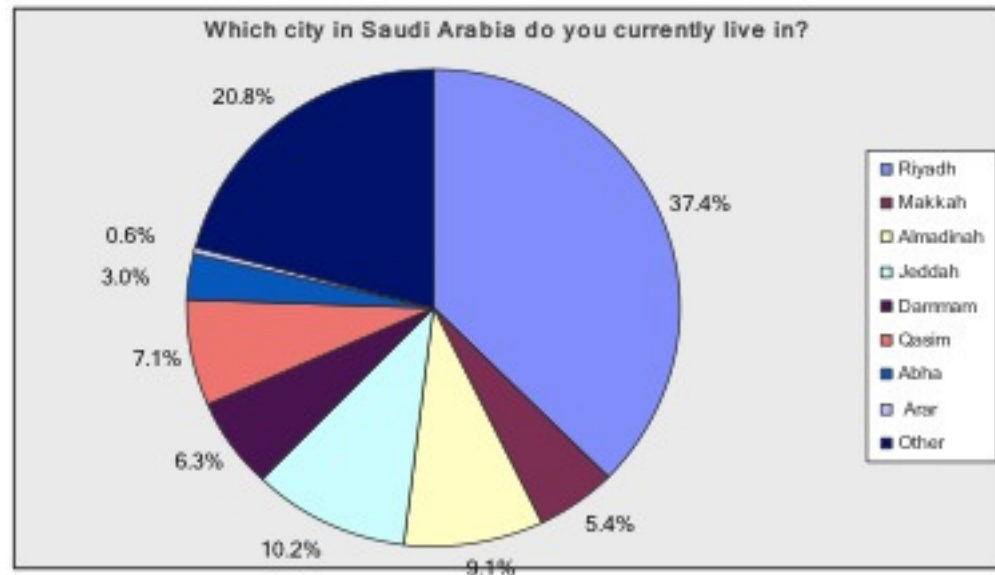


Figure 4.2 Participant location

### 4.3 General Information security practices

#### 4.3.1 Internet usage

Table 4.8 shows that 100% of participants (i.e. all 462 participants) used the Internet. This is to be expected, as all respondents were completing an online survey.

Table 4.8 Internet use

Have you ever used the Internet? (N=462)				
		Frequency	Percent	Valid Percent
Valid	Yes	462	100	100
	No	0	0	0
	Total	462	100.0	100.0

Participants in this study were asked about their purpose(s) for using the Internet and the number of hours spent per week for each purpose. The question was optional and it is possible that some participants may have chosen not to respond to all the purposes listed. Table 4.9 shows that, in the case that participants indicated they used the Internet for a specific purpose, the time spent ranged from 1 hour up to over 25 hours per week.

However, many participants used the Internet for no time (i.e. 0 hours) each week for some very common activities such as email.

**Table 4.9 Purpose of Internet use and time spent**

<b>For what purpose do you spend your time online? Please indicate the amount of time spent in hours on each purpose per week. (N=456)</b>							
<b>Answer Options</b>	<b>0</b>	<b>1-6</b>	<b>7-12</b>	<b>13-18</b>	<b>19-24</b>	<b>25 &amp; more</b>	<b>Response Count</b>
Email	48	284	51	26	10	14	433
Instant Messaging	131	174	25	25	20	24	399
Shopping	225	130	33	8	4	2	402
Blogging	21	170	95	49	31	69	435
Social Networking	253	75	17	12	20	14	391
Online transactions	251	114	19	5	6	2	397
Online games	249	73	32	17	13	13	397
File downloading	102	179	52	31	25	17	406
Video sharing	250	74	22	16	16	9	387
Latest news	100	188	68	31	14	18	419
Researching information	30	216	72	31	22	38	409
Online courses and distance learning	253	89	16	6	5	5	374
<b>Total</b>							<b>456</b>

#### **4.4 Information security issues**

In this section, the results have been organised into three categories: information security practices, information security tools and confidence level.

##### **4.4.1 Information security practices**

The first question asked about the type of devices owned or used by participants. Table 4.10 shows that 97.6% of participants use desktops/laptops, 46.5% use mobile phones, 13.2% use smart phones/PDAs, 4.3% use portable video game consoles, 13.9% use flash drive and 4.8% use GPS. The use of desktop/laptop use among Saudi people is high suggesting the need for strong physical security to protect information stored on these devices.

**Table 4.10 Device types**

<b>What type of devices do you currently use? (Please tick all that are applicable) (N=462)</b>		
<b>Answer Options</b>	<b>Response Percent</b>	<b>Response Count</b>
Desktop/ Laptop	97.6%	451
Mobile phone	46.5%	215
Smart phone/ PDA	13.2%	61
Portable video game console	4.3%	20
USB Flash Drive	13.9%	64
GPS	4.8%	22
<b>Total</b>		<b>462</b>

The next question asked if respondents physically secured their portable computer devices (e.g. laptops, mobile phones). Table 4.11 showed that only 29% of respondents kept their portable devices in secure places all the time. A further 43.1% of respondents sometimes keep their devices secure, 1.5% of respondents do not have such devices and 3.7% do not know whether they secure their devices or not. However, 22.7% of respondents never keep their devices secure showing a surprising lack of care for these devices or the information that they contain.

**Table 4.11 Device security**

<b>Do you keep your mobile devices (PDAs, laptop, USB keys) in a secured place and do you practice precautions to keep it secured (i.e. use locking devices) when not used? (N=462)</b>		
<b>Answer Options</b>	<b>Response Percent</b>	<b>Response Count</b>
Yes, all the time	29.0%	134
Sometimes	43.1%	199
No	22.7%	105
I don't have such devices	1.5%	7
I do not know	3.7%	17
<b>Total</b>		<b>462</b>

The next question asked respondents to indicate on a six-point scale about the level of information security for their devices. Incredibly, 252 respondents (54.5%) rated this as poor, very poor or non-existent. 12.8% of respondents evaluated information security in their devices as not there at all, 15.6% said it was very poor and 26.2% classified it as poor. 12.6% of respondents believed that information in their devices was protected by a good level of security and 14.5% responded that such information had a very good security level. Table 4.12 shows the level of security for information on participants'

devices.

**Table 4.12 Device information security**

<b>How secure do you think information is on your computer/mobile device? If it is secure please select the security level (N=462)</b>				
		<b>Frequency</b>	<b>Percent</b>	<b>Valid Percent</b>
Valid	not exist	59	12.8	12.8
	very poor	72	15.6	15.6
	poor	121	26.2	26.2
	neutral	85	18.4	18.4
	good	58	12.6	12.6
	very good	67	14.5	14.5
	Total	462	100.0	100.0

#### **4.4.1.1 Passwords**

Respondents were asked if they secured their devices using login passwords. Table 4.13 shows that 55.2% of respondents used passwords to login into their devices, 7.2% have a password on their screensaver and 39.7% do not use passwords in either situation.

**Table 4.13 Use of passwords on devices**

<b>Do you have passwords for the following on your device(s)? (N =458)</b>		
	<b>Percent</b>	<b>Count (N)</b>
Login/Switch On	55.2%	253
Screensaver	7.2%	33
Neither	39.7%	182

Hackers use a range of tools and techniques, such as social engineering and password cracking, to gain access to users' passwords. Short or weak passwords and passwords that contain personal identification (such as name or date of birth) allow passwords to be cracked easily. However, strong passwords composed of more than 8 characters including a mixture of numbers, upper and lower case letters and special characters are far more difficult to crack and so can protect information from unauthorized access or theft.

Table 4.14 indicates the level of participants' password security. 45% of the respondents used passwords less than 5 characters long and 49% used passwords that were 5 to 8 characters. Neither of these is very secure. Conversely, 111 respondents used more than 8 characters in their passwords. The multi-part nature of the question allowed respondents to indicate specific characteristics of their passwords (e.g. use of capital letters). Table 4.14 shows that the use of capital letters (25%) and special

characters (29%) is significantly less than the use of lower case letters (41%) and numbers (77%). This is unfortunate as the use of capital letters or special characters significantly improves password strength. At first glance, the use of numbers in passwords seems positive, as the inclusion of numbers greatly strengthens a password. However, anecdotal evidence suggests that many Saudis use only numbers as passwords, specifically their mobile phone numbers or their date of birth. The structure of this question does not allow us to say definitively, but it is likely that many of the numerical passwords less than 5 characters or between 5 and 8 characters (59%) are mobile numbers or birthdays and therefore are among the most ineffectual passwords.

**Table 4.14 Password security**

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

Having a good password is still not enough to completely secure information; passwords should be changed regularly. Table 4.15 shows participants' responses to the question "How often do you change your password?" Notably, 65.7% of respondents have never changed their passwords. This is a major security risk.

**Table 4.15 Frequency of password change**

<b>How often do you change your password? (N=353)</b>				
		Frequency	Percent	Valid Percent
Valid	Daily	8	1.7	2.3
	Weekly	8	1.7	2.3
	Monthly	29	6.3	8.2
	Quarterly	34	7.4	9.6
	Annually	42	9.1	11.9
	Never	232	50.2	65.7
	Total	353	76.4	100.0
Missing	System	109	23.6	
Total		462	100.0	

In an organizational context, many organizations require staff to change their passwords regularly. However, Table 4.14 and Table 4.15 suggest that Saudis are either unaware of the value of strong passwords that are changed regularly or, if they are aware of it, simply do not see it as their responsibility. This abrogation of responsibility is reflected

in later responses and may be associated with a patriarchal society in which ‘those in charge’ are responsible and individuals are not. In either case the finding indicates a low level of ISA. Even more alarming is that the data suggests that system administrators in Saudi Arabia are not aware of this problem either; it can be assumed that if they were, systems would automatically force users to select strong passwords and to change those passwords regularly.

The responses to the next question are notable in identifying the extent of extremely poor information security. Table 4.16 shows that 35.8% of 363 respondents shared their access passwords with family members. Similar ISA studies conducted in South Africa suggest that password sharing is close to 0% (Kruger et al. 2010). Conversely, Saudis’ password sharing with colleagues or with a system administrator is very low, which raises the question, why share with family members but not with others outside the family? The high level intra-familial password sharing may be linked to the Saudi’s tribal culture in which members of the tribe are seen as trustworthy but those outside the tribe are not. Regardless of the association with tribal culture, the security risk associated with password sharing is serious. Password strength and the frequency with which a user changes a password is irrelevant if that password is distributed to others.

**Table 4.16 Incidence of password sharing**

<b>The password used to access your account or data is known: (N = 363)</b>		
	Percent	Count (N)
Only by you	63.6%	231
By family members	35.8%	130
By a few colleagues	9.6%	35
By a system administrator	2.8%	10

#### **4.4.1.2 Threat awareness**

While it can be expected that many people are aware of the threat of viruses, there are a other less well-known information security threats that may cause loss of confidentiality, integrity or availability of information. Information threats can be categorised as natural disasters, malware, hacking, intrusions and Denial of Service (DoS) attacks.

Table 4.17 shows participants’ awareness of some the main information threats. As expected, awareness of virus attacks was high as was awareness of spam emails.

However, only 7.4% of 462 participants are aware of DoS attacks. The threats of vulnerability probing, harassment or cyber bullying, and cyber stalking were only familiar to about 19% of participants, while awareness of system intrusion was slightly higher at 20.8%. Only 25.5% of participants were aware of the risk of identity theft.

**Table 4.17 Awareness of information threats**

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

#### **4.4.2 Information security tools**

Faced with a number of different information security threats, educated computer users have a number of security tools at hand. Participants were asked which types of security tools they used. Given the high level of awareness of viruses shown in Table 4.17, it is not surprising that Table 4.18 shows that over 86% of participants used antivirus software. However, probably because they are unaware of the other potential threats, the use of all other protection mechanisms was far lower. From 452 respondents, only 16.2% used Internet security software and 13.9% used anti-spam software. Only 10.4% used anti-spy software.

It is interesting to note that the use of protection was in all cases lower than the awareness of related threats. For example, over 25% of respondents in Table 4.17 were aware of fraud and identity theft but only 16.2% of respondents in Table 4.18 used Internet security. It appears then that there are two related problems: lack of awareness of the threat and lack of appropriate response. It is still unclear whether the lack of response is because Saudis do not know what the correct response is or whether they simply do not think the response is warranted.



**Table 4.18 Use of protection software**

<b>What protection software do you currently use? (N = 452)</b>		
	Percent	Count (N)
Antivirus	86.7%	392
Firewall	22.3%	101
Internet Security	16.2%	73
Anti-spam	13.9%	63
Anti-spy	10.4%	47

Of course, it is not enough simply to install protection software; one must also keep it up to date. Mechanisms to control threats such as viruses, trojans, spy attacks or spam need regular and frequent updates. Table 4.19 clearly shows the low awareness of the need for such updates for both freeware and licensed software.

**Table 4.19 Software type and most recent update**

<b>What is the type of software used and when did you last update it? (N = 462)</b>							
	One day ago	Last month	3 months ago	6 months ago	Last year	Never	Count (N)
Freeware	57	80	57	30	34	94	352
Paid License	56	54	33	22	29	41	235

Surprisingly, over 53% of users of both freeware and licensed protection software had not updated their software in more than 3 months. Possibly the cost of update was a contributing factor, however, updates to freeware are free, but participants still did not update that software either.

While having protection software to secure your information is an important step, people also need to be aware of the way risks are transmitted, including by the users themselves. Sometimes the risk can come from email, especially for people who have a private email account that they use for both private and work purposes. This shared usage can seriously increase the risk to an employer's organizational network. Table 4.20 indicates that 67.7% of the 462 respondents used their private web mail for professional purposes at least sometimes and 21.2% used private mail for business purposes frequently or everyday. This represents a serious security risk to the majority of Saudi businesses.

**Table 4.20 Use of private web mail for professional purposes**

<b>Do you use private web mail for professional purposes? (N = 462)</b>		
	Percent	Count (N)
Never	32.3%	149
Sometimes	46.5%	215
Frequently	17.3%	80
Everyday	3.9%	18

#### **4.4.2.1 Backups**

In the case that an information attack damages or destroys data, a backup can often be used to restore the lost data. Indeed, many individuals and companies do not really value their own information until it is successfully attacked and they need to restore it somehow. It was possible that, even though responses suggested that Saudis were not good at protecting their data, perhaps their backup procedures would provide a fall-back position. Unfortunately, Table 4.20 clearly shows that 43.9% of participants never did a backup of their data. If their data was corrupted by an attack, they had no mechanism to restore it. All corrupted data would need to be re-entered by hand. Only 15.2% of respondents did a backup frequently or everyday, so over 80% of participants had an ineffective backup procedure which places them enormously at risk (see table 4.21).

**Table 4.21 Data backup frequency**

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

In organizations and businesses, data backup is very important because files may be accidentally deleted, mission-critical data can become corrupt and natural disasters can occur. With a solid backup and recovery plan, it is possible to recover from any of these threats. There is a relationship between access to backup facilities (such as USB backup drives) and data backup. Table 4.10 above showed that only 13.9% of respondents had a USB to store data, indicating a clear low awareness about the need for data backup hardware to save data from unexpected loss.

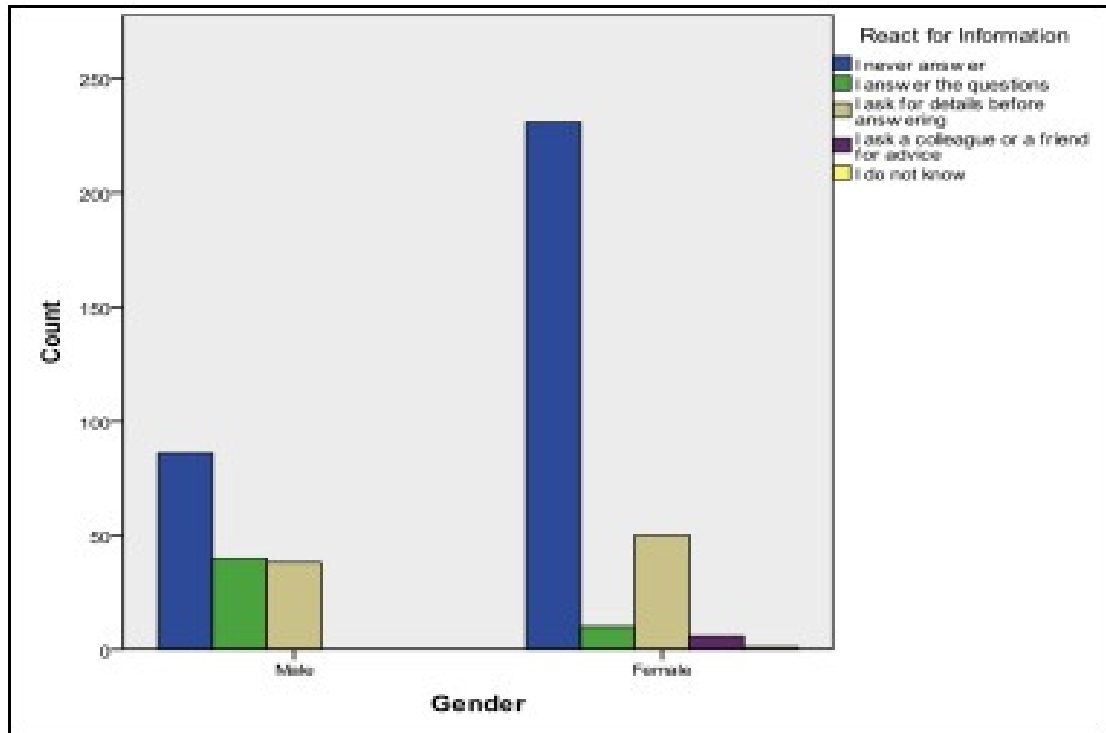
#### 4.4.2.2 *Safeguarding personal information*

One of the questions asked was a participant's reaction to a phone call or email asking for information. This question was included because some information threats such as fraud can be introduced by asking for personal details using email or the phone. Table 4.22 shows that 68.6% of respondents would never answer such a request, 19% would ask for details before answering and 1.3% would ask friends for advice. Only 10.8% of respondents said they would answer the questions. Saudi culture is a very private culture and perhaps this influences Saudis reluctance to share any information outside the family. The data summarised in Table 4.16 shows that Saudis share passwords with their family more than other people in other countries share passwords.

**Table 4.22 Provision of personal information in response to unsolicited request**

<b>How would you react if you received a phone call or an email asking for information (i.e. mobile number, personal email address)? (N = 462)</b>				
		Frequency	Percent	Valid Percent
Valid	I never answer	317	68.6	68.6
	I answer the questions	50	10.8	10.8
	I ask for details before answering	88	19.0	19.0
	I ask a colleague or a friend for advice	6	1.3	1.3
	I do not know	1	0.2	0.2
	Total	462	100.0	100.0

However, there are several possible reasons for the high percentage of respondents who said they would not respond to emails and telephone calls that asked for personal information. Figure 4.3 shows that 231 of the 317 respondents who would not answer were female (72.8%). Only 20% of respondents who said they would answer the questions were female; 80% of respondents willing to provide this personal information were male. For cultural reasons, Saudi women are very careful about their privacy when interacting with people outside their family circle.



**Figure 4.3 Provision of personal information in response to unsolicited request by gender**

#### 4.4.2.3 *Reporting security*

Reporting security incidents is a useful practice as it allows the user to find better protection solutions. It also provides a service to the whole community as it allows security providers to address particular threats and reduce the likelihood of similar information security incidents in the future. Unfortunately, Table 4.23 shows that 80.5% of respondents were not aware of how or where they could report security incidents. This low awareness can reduce the opportunities for users to increase their own security knowledge and to make a contribution to information security in Saudi Arabia generally.

Table 4.23 Security incident report awareness

Do you know if you can report security incidents (i.e. illegal content, inappropriate websites, spam, harassment, hack threat) and where you can report them? (N = 462)		
	Percent	Count (N)
No	80.5%	372
Yes	19.5%	90

Figure 4.4 shows the awareness of InfoSec reporting, grouped by industry sector. It can be seen that only the banking and finance sector demonstrated an awareness about the reporting of incident security with more respondents replying ‘yes’ than ‘no’.

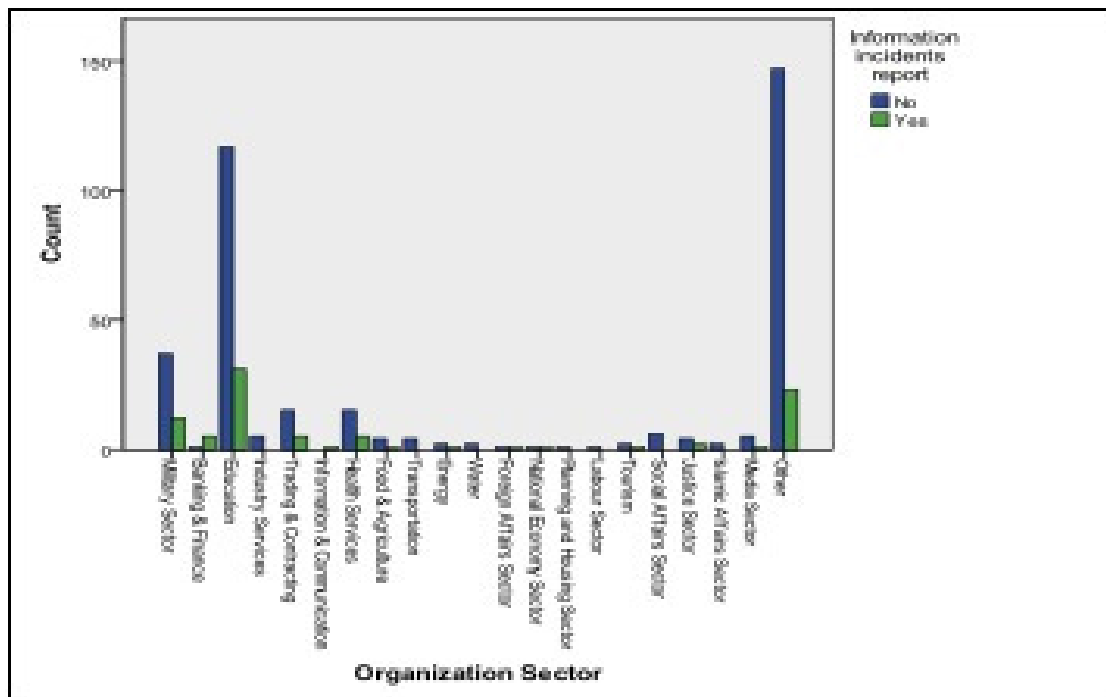


Figure 4.4 Security incident reporting by sector

Respondents were asked if their data had ever been attacked via hacking or theft. Response options were ‘yes’, ‘no’ or ‘do not know’. Table 4.24 shows that 60.4% of respondents indicated that had not experienced these threats, 28.1% had no idea whether they had been hacked or had data stolen, and only 11.5% responded that their information had been hacked or stolen. In reality many of the people who responded ‘no’ probably have no idea whether their data had been copied because they had no security software to tell them. Some may have had files stolen but assumed that they had just deleted them accidentally. Some may have had files deliberately corrupted but just assumed that it was a ‘bug’. It is difficult to know whether information has been hacked

or stolen from a computer unless information is exposed or the user has good physical security tools that can report hacking incidents.

**Table 4.24 Participant information stolen or hacked**

<b>Has your information has been hacked or stolen from your mobile/computer? (N = 462)</b>				
		Frequency	Percent	Valid Percent
Valid	Yes	53	11.5	11.5
	No	279	60.4	60.4
	Do not know	130	28.1	28.1
	Total	462	100.0	100.0

#### 4.4.3 Privacy level

The final question in this section asked participants whether they felt that privacy was important when online. Protecting online privacy is an important goal in and of itself but it is also an important step in avoiding identity theft, which can take place in the real world as well as the cyber world. Given that Saudi culture emphasises the idea that a person is only safe within a family or tribe and that women in particular are required to maintain a high level of physical ‘privacy’ (e.g. wearing a veil and only being able to travel if accompanied by a male family member), it could be expected that privacy would be a significant issue for Saudis. Indeed, it is, with the vast majority (91.7%) of participants either agreeing or strongly agreeing that online privacy is important as shown in Table 4.25. Unfortunately, although it is important, much of the previous data suggests that Saudis do not know how to ensure their online privacy.

**Table 4.25 Importance of privacy online**

<b>I feel privacy is important during online activities: (N = 433)</b>		
	Percent	Count (N)
Strongly Disagree	2.8%	12
Disagree	4.8%	21
Agree	54.7%	237
Strongly Agree	37.0%	160
N/A	0.7%	3

While much of the previous data suggests that lack of knowledge gives rise to information security risks, another explanation might be that Saudi Arabia’s patriarchal culture does not encourage Saudis to take responsibility for themselves. Participants were asked who was responsible for their digital privacy and were allowed

to nominate more than one person or agency. Table 4.26 shows that 67.6% of participants believed that they were responsible for their own privacy. However, 22.8% also believed that the government was responsible, reflecting their patriarchal culture. At the same time, 35.2% of respondents believed that the company that had their digital information was responsible for its security. It is possible that the tribal nature of Saudi culture assumes that other trusted parties should take responsibility rather than individuals themselves assuming responsibility.

**Table 4.26 Responsibility for digital information privacy**

<b>Who do you think is responsible for the privacy of your digital information? (N = 429)</b>		
	Percent	Count (N)
Myself	67.6%	290
The government	22.8%	98
The company I divulge my digital information to	35.2%	151

#### ***4.5 Preferences for promotion of Information Security Awareness***

From the data presented so far, there is a clear need to increase the level of ISA in Saudi Arabia. In order to reduce the risks and increase the efficiency of information security systems, the final two survey questions considered the mechanisms by which such awareness could be raised. Table 4.27 shows that the Internet is, by far, the most popular source of information about information security (69.2%). Not only is the Internet convenient, it is also particularly appropriate for Saudi culture for two reasons. Firstly, the country is very large and much of the population lives in relatively remote locations. The Internet provides distance education which addresses this problem. Secondly, the Internet is particularly suited to Saudi women who cannot attend seminars or courses unless accompanied by a male relative.

**Table 4.27 Sources for learning about information security**

<b>Have you ever been to or used one of the following sources to learn about information security? (Please tick from the options below) (N=412)</b>		
	<b>Response Percent</b>	<b>Response Count</b>
Exhibitions or seminars	4.4%	18
Courses	8.3%	34
Books	11.7%	48
Articles	17.2%	71
Internet Websites	69.2%	285
N/A	21.8%	90
<b>Total</b>		<b>412</b>

Table 4.28 shows the list of communication mechanisms that participants believe can be effective in promoting information security awareness. Participants were asked to indicate their three most preferred options. 75% of respondents selected the Internet in their top three options. 50.7% also liked newspapers. However, the very high preference for the Internet as a distribution mechanism may be biased by the fact that 100% of respondents were Internet users.

**Table 4.28 Communication mechanisms for promoting ISA**

<b>Which communication do you think is effective in promoting awareness of information security for the public? (N=412)</b>		
	<b>Response Percent</b>	<b>Response Count</b>
Web portals	75.0%	309
Newspapers	50.7%	209
Educational Programs (i.e. Documentaries)	35.2%	145
Advertisements	30.3%	125
E-Books/ e-Magazines	29.1%	120
Billboard/ Posters	28.9%	119
Seminars	21.1%	87
Books	16.3%	67
Cartoon series	14.8%	61
Exhibitions	14.1%	58
Talks	13.1%	54
Magazines	12.1%	50
Web based games	8.7%	36
Other	0.7%	3
<b>Total</b>		<b>412</b>



#### **4.6 *Chi-Square Relationships Tests***

This survey included semi-closed ended questions to combine the advantages of closed-ended questions and open-ended questions. Consequently, survey answers include some data which cannot, on any logical basis, be ordered numerically, hence there is no possibility of using parametric statistical tests that require numerical data. The general pattern of nonparametric procedures is much like that seen with parametric tests, namely, certain sample data are treated by a statistical model which yields a value or statistic. This value is then interpreted for the likelihood of its chance occurrence according to some type of statistical probability distribution. With the chi-square procedure, a value is calculated from and then compared to a critical value from a chi-square table with degrees of freedom corresponding to that of the data. If the calculated value is equal to or greater than the critical value (table value), the null hypothesis is rejected. If the calculated value is less than the critical value, the null hypothesis ( $H_0$ ) is accepted. This procedure is similar to that used with the T-test and F-test (Greenwood 1996).

Chi-square is employed to test the difference between an actual sample and another hypothetical or previously established distribution such as that which may be expected due to chance or probability. Chi-square can also be used to test differences between two or more actual samples (Greenwood 1996). The chi-square goodness of fit test is used to determine whether a relationship exists between two categorical variables. For the purpose of the research, a result will be considered significant if it has a p-value less than 0.05 of significance.

This section applied the chi-square test to determine the relationships and differences between certain questions. Chi-square test was conducted to check the significance relationship between each participant's background and some ISA practices. A copy of the chi-square test tables are presented in Appendix E. Table 4.29 has shown there is a statistically significant difference between:

**Table 4.29 Chi-Square Test Results**

	Devices security place	Devices security level	Password change	Private web mail use	Information react	Backup	Reporting security incidents
<b>Gender</b>	0.182	0.030	0.533	0.000	0.000	0.291	0.320
<b>Age</b>	0.282	0.100	0.642	0.606	0.522	0.191	0.102
<b>Education</b>	0.060	0.000	0.024	0.091	0.060	0.263	0.140
<b>Organization Type</b>	0.199	0.057	0.192	0.000	0.000	0.004	0.127
<b>Organization Sector</b>	0.469	0.192	0.000	0.000	0.001	0.000	0.024
<b>Living area</b>	0.894	0.765	0.670	0.575	0.253	0.420	0.165

**1. Gender:**

A statistically significant relationship exists between gender and device security level, p-value  $0.030 < 0.05$ . The proportion of males who have non-existent, poor or very poor level device security totals 63.4% while the proportion of females is 49.6%. It can be concluded that more males have a poor level of device security than females.

In addition, a statistically significant relationship exists between gender and private web mail use, p-value  $0.000 < 0.05$ . The percentage of males using private web mail for professional purposes frequently and daily is 32.3% while the percentage for females is 15.1%. It can be concluded that males use their private email address for professional purposes more often than females. This could be explained by the societal characteristic that males work more than females in Saudi Arabia.

Also, a statistically significant relationship exists between gender and reaction including personal information, p-value  $0.000 < 0.05$ . The proportion of females was 77.5% while the proportion of males 52.4%. It can be assumed that males share their private information more often than females because of culture reasons; in Saudi Arabia, females cannot have communication with irrelevant people.

## 2. Education:

A statistically significant relationship exists between education and device security level,  $p\text{-value } 0.000 < 0.05$ . Device security level indicates that people who have a higher level of education are more aware than people who have achieved only a diploma or high school completion. Education can therefore be a good way to raise awareness.

Moreover, a statistically significant relationship exists between education and password change practice,  $p\text{-value } 0.024 < 0.05$ . The relationship between education and password practices shows that people who have never changed their password are likely to be less educated, with 61% of the respondents in this category having a low level of education (i.e. high school or less). More education can therefore also lead to better password practices.

## 3. Organization Types

A statistically significant relationship exists between organization types and device security level,  $p\text{-value } 0.000 < 0.05$ . In government, 21.3% have good or very good levels of device security while the private sector records 27% of respondents as having good or very good device security. The private sector is slightly better.

In addition, a statistically significant relationship exists between organization type and private web mail use,  $p\text{-value } 0.000 < 0.05$ . The proportion of people who never use private web mail for professional purposes is similar in both the government and private sectors; 22.4% in government and 20.5% in private sector.

Also, a statistically significant relationship exists between organization type and reaction about personal information,  $p\text{-value } 0.000 < 0.05$ . The proportion of people who never answer or share their information is 64.4% in government and 50.6% in private sector. Again, gender and cultural factors (females in Saudi Arabia cannot have communication with irrelevant people) may impact on this.

Furthermore, a statistically significant relationship exists between organization type and data backup,  $p\text{-value } 0.004 < 0.05$ . The proportion of people who never do a data backup is 33.8% in government and 54.7% in private sector. This

indicates that the government sector has a small advantage in data backup over the private sector.

#### 4. Organization Sector:

A statistically significant relationship exists between organization sector and password change practice,  $p\text{-value } 0.000 < 0.05$ . When considering which sectors included respondents who never changed their password, almost all sectors recorded over 50% of respondents in this category. The exception to this were banking and finance and information and communication sectors; these sectors has less than 17% of respondents never changing their password. These same sectors also have good practices in data backup.

A statistically significant relationship exists between organization sector and data backup,  $p\text{-value } 0.000 < 0.05$ . The results shows that all sectors have poor data backup practices, except the banking and finance sector (only 16% reported never performing data backup). This was to be expected with the banking sector also having the best password practice.

Moreover, a statistically significant relationship exists between organization sector and private web mail use,  $p\text{-value } 0.000 < 0.05$ . All sectors reported using private web mail for professional purposes.

Also, there is a statistically significant relationship between organization sector and the reaction for personal information,  $p\text{-value } 0.001 < 0.05$ . All sectors were shown to share their information.

A statistically significant relationship exists between organization sector and reporting security incidents,  $p\text{-value } 0.024 < 0.05$ . All sectors have poor reporting security incidents practices except for the banking and finance and information and communication sectors, which have more than 83% of incidents reported.

#### ***4.7 Information Security Awareness studies for comparison purposes***

Few large studies have been conducted and published in the Information Security Awareness field. While some studies are conducted prior to 2007, these are considered too old to inform a meaningful comparison with 2011 data in this field. Two studies were identified as appropriate and useful comparisons in considering the ISA level of

Saudi Arabia relative to other countries. The first study selected was titled *A Vocabulary Test to Assess Information Security Awareness* (Kruger et al. 2010). It was conducted in South Africa in 2010. The second study selected was *An Analysis of Information Security Awareness within Home and Work Environments*. It was a global study conducted in 2010 (Talib et al. 2010). The next two sections will describe the results of the studies for comparison purposes.

#### 4.7.1 Information threats and security

In the first study (Kruger et al. 2010), the majority of respondents understood the threats linked to information security such as viruses, worms, spyware, spam and phishing (89%). Only 9.1% of respondents did not know of any threats. The study also showed that 77% of respondents understood aspects of IT security. The results from global study by Talib et al.'s (2010) showed a significant difference between the awareness of participants globally and that of Saudi Arabian participants (see Table 4.30).

**Table 4.30 Comparison of information security threat awareness**

Information Security Threats	Global Study	Saudi Arabia
Viruses	92%	87.2%
Spam	90%	57.8%
Phishing	70%	29.7%
Denial of Service (DoS) attack	56%	7.4%
Identity theft	81%	25.5%

From the previous table, it can be seen that Saudi Arabian participants had a very low level of awareness of information security threats relative to global awareness. Only 7.4% were aware of DoS attacks compared with 56% in the global study. Identity theft threat awareness was only 25.5% in Saudi Arabia compared with 81% globally. Phishing threat awareness among participants in Saudi Arabia was only 29.7% compared with 70% in the global study. Spam awareness was 57.8% among Saudis compared with 90% globally. Finally, awareness of viruses in Saudi Arabia was 87.2% compared with 92% in the other study.

After understanding the threats, the next step is to set up the control tools used to prevent further risks. Based on the level of awareness of information security threats as recorded in the previous table, it is possible that Saudi Arabian participants were using control software less than participants in the global study because Saudis do not know

or understand the threats. Table 4.31 shows that Saudi Arabian participants used this software significantly less than participants in the global study.

**Table 4.31 Comparison of information security control software use**

Information Security Control Software	Global Study	Saudi Arabia
Antivirus	98%	86.7%
Firewall	78%	22.3%
Anti-Spyware	75%	10.4%
Anti-Spam	67%	13.9%

Examination of the data clearly shows that Saudi Arabian participants had a low information security awareness level in terms of understanding information security threats and using control software to stop or reduce related risks. Consequently, information threats can spread faster in Saudi Arabia because of the low level of information security awareness.

#### **4.7.2 Password practices**

Table 4.32 compares some passwords practices between participants in Saudi Arabia and South Africa.

**Table 4.32 Password practices**

Questions	South Africa	Saudi Arabia
I never change my password	27.3%	65.7%
I choose a simple and easy password	9.1%	Nearly 45%
I share my password with others	0%	35.8%

It is clear that password practices in South Africa are stronger than password practices in Saudi Arabia. For example, 27.3% of South African respondents said they never changed their password compared with 65.7% of Saudi Arabian participants. Saudi Arabians were much more likely to choose a simple and easy password than South Africans. The most notable and concerning comparison was that 35.8% of Saudi Arabian people shared their passwords with others compared to 0% in South Africa.

#### **4.7.3 Reporting of security incidents**

Table 4.33 shows that 80.5% of Saudi respondents were not aware of how or where they could report security incidents compared with only 4.5% of unaware respondents in South Africa. This low awareness can reduce the opportunities for users to contribute to

decreasing the hazards surrounding information security.

**Table 4.33 Comparison of incident security reporting awareness**

Question	South Africa	Saudi Arabia
I do not know where I can report security incidents	4.5%	80.5%

It can be concluded that Saudi Arabian participants clearly have a lower level of awareness of both information threats and security, a lower level of password practices and lower reporting of security incidents compared with participants in other similar studies. This lack of information security awareness increases the potential information threats and risks in Saudi Arabia.

#### **4.8 Conclusion**

Saudi Arabia has become one of the ten countries in the world most affected by information security attacks (Kaspersky Lab 2011). Saudi Arabian networks received 1.77% of total attacks in 2010, even though Saudi Arabia accounts for only 0.002% of Internet users worldwide. Saudi Arabian websites were the third most highly attacked by country after Egypt and the US based on 2010 data (NetWitness 2010). The reasons for the high attack incidence in Saudi Arabia were identified as low awareness of Internet crimes and low security requirements in the Saudi Arabian society. In September 2010, Saudi Arabia had 421,998 hacked computers which was an increase of 65% in less than a year (Trend Micro Smart Protection Network 2010).

Saudi Arabia is also consistently rated as the most frequently spammed country around the world, with a spam rate of 82.2% in June 2011 (Symantec Lab 2011). This situation is unusual given the country's relatively small population and level of Internet adoption.

This study has suggested that the high level of attacks on Saudi information networks may be due to a lack of Information Security Awareness (ISA) among the general Saudi public. It has also been suggested that the lack of ISA may be due to the highly-censored, patriarchal and tribal nature of Saudi culture.

The survey of 462 Saudis presented in this chapter confirmed that ISA is in fact very low and that a number of information security risks may be related to Saudi culture. These include the sharing of passwords, which can be explained in the context of the Saudi tribal society. Similarly, the expectation that the government or other information

providers are responsible for information security reflects the patriarchal nature of Saudi life.

An analysis of the frequency with which passwords were changed and the strength of passwords themselves supported the conclusion that the general public either does not know about recommended security procedures or simply chooses not to follow them. Moreover, it is apparent that companies or government departments being accessed by Saudis do not enforce these recommended procedures. Also, there is a shortage of physical security tools (such as defence software, data backup or security incidents reports) being implemented by the public in Saudi Arabia.

Therefore, this study has confirmed that a problem exists within the general public but also suggests that problems may exist within the IT practices of many Saudi organizations. The next chapter of this research will examine the IT practices in Saudi Arabia to determine whether Saudi IT departments are aware of recommended practices and standards, whether Saudi organizations have specialist IT security staff and whether Saudi IT practitioners are sufficiently qualified in information security.



## ***Chapter 5 Results and discussion for Information Security Practices in Saudi Arabian Organizations***

### ***5.1 Introduction***

This chapter presents and discusses the results of the InfoSec practices survey completed by representatives of organizations in Saudi Arabia. Section 1 of the InfoSec survey recorded the background of the organization, including information such as the nature of the organization, sector, size, number of years of operation and whether an IT department existed and its budget. Section 3 had three parts: questions about the data protection laws, the information security standards and information security policies in the organization. Section 4 included three parts covering information assurance in the organization, information assurance tools and measures and information security risks. Section 5 presents the information security promotions that participants believed would be effective for increasing InfoSec practices and awareness.

This survey involved 124 respondents from organizations across different industry sectors. The survey used 51 semi-closed ended questions. The information in this chapter was created through the application of descriptive statistical analyses and Chi-Square test techniques were used to achieve the research objectives.

### ***5.2 Background of organizations***

Descriptive analysis of the background of participating organizations in terms of the nature of the organization, industry sector, size, length of operation, existence of an IT department and IT budget existence is provided.

Table 5.1 presents a frequency distribution of the organizations according to their nature: public sector or government agency, private sector or business, and non profit organization.

**Table 5.1 Nature of organization**

Nature of Organization (N=124)				
		Frequency	Percent	Valid Percent
Valid	Public sector / Government agency	75	60.5	60.5
	Private sector / Business	43	34.7	34.7
	Not-for-profit organization	6	4.8	4.8
	Total	124	100.0	100.0

As depicted in Table 5.1, 60.5% of participating organizations belonged to the public sector and 34.7% were classified as private sector. 4.8% of the organizations were non-profit institutions. As Pittman (2012) maintained, some specific areas of information security are unique to organizations based on their nature.

Table 5.2 presents a frequency distribution of the participating organizations grouped according to their industry sector. Sectors considered in this study included: military, banking and finance, education, industry services, trading and contracting, information and communication, health services, food and agriculture, transportation, electricity, water, foreign affairs, labour, tourism, social affairs, justice, Islamic affairs and media. Organization sectors were recorded in this study to allow discovery of the strengths and weaknesses in InfoSec practices among specific industry sectors.

**Table 5.2 Sector of organization**

Organization's Sector (N=124)				
		Frequency	Percent	Valid Percent
	Education	29	23.4	23.4
	Military Sector	13	10.5	10.5
	Trading & Contracting	13	10.5	10.5
	Banking & Finance	11	8.9	8.9
	Health Services	10	8.1	8.1
Valid	Industry Services	8	6.5	6.5
	Information & Communication	6	4.8	4.8
	Media Sector	5	4.0	4.0
	Food & Agriculture	4	3.2	3.2
	Transportation	4	3.2	3.2
	Tourism	4	3.2	3.2
	Social Affairs Sector	4	3.2	3.2
	Electricity	3	2.4	2.4
	Water	3	2.4	2.4
	Labour Sector	2	1.6	1.6
	Justice Sector	2	1.6	1.6
	Islamic Affairs Sector	2	1.6	1.6
	Foreign Affairs Sector	1	0.8	0.8
	Total	124	100.0	100.0

As shown in Table 5.2, organizations from the education, military, trading and contracting, and banking and finance sectors represented 23.4%, 10.5%, 10.5% and 8.9% of the total number organizations in the study respectively.

Table 5.3, shows a frequency distribution of the organizations, grouped with respect to size. The organizations were categorized into five groups: 1-50 employees, 51-100 employees, 101-500 employees, 501-1000 employees and more than 1000 employees.

**Table 5.3 Size of organization**

Size of your organization (N=124)				
		Frequency	Percent	Valid Percent
Valid	1 - 50 Employees	17	13.7	13.7
	51 – 100 Employees	25	20.2	20.2
	101 – 500 Employees	27	21.8	21.8
	501 - 1000 Employees	11	8.9	8.9
	More than 1000 Employees	44	35.5	35.5
	Total	124	100.0	100.0

It can be seen from Table 5.3 that 35.5% of the respondents' organizations were relatively large institutions employing more than a thousand personnel. About 21.8% of the organizations employed 101-500 employees, while 20.2% had 51-100 employees. 13.7% of the organizations had 50 employees at the most, whereas 8.9% of the organizations engaged the service of 501-1000 employees. Organizational size is an important concern for information security because employees of larger organizations tend to engage in better management (Stanton et al. 2006), and so are more likely to have better InfoSec policies and practices. With 66.1% of organizations having over 100 employees, we might expect good InfoSec practices.

Table 5.4 presents a frequency distribution of the organizations grouped according to number of years the organization has been in operation: less than one year, 1-5 years, 6-10 years, 11-20 years, 21-30 years, and more than 30 years.

**Table 5.4 Age of organization**

Age of the organization (N=124)				
		Frequency	Percent	Valid Percent
Valid	Less than 1 year	3	2.4	2.4
	Between 1 to 5 years	17	13.7	13.7
	Between 6 to 10 years	23	18.5	18.5
	Between 11 to 20 years	16	12.9	12.9
	Between 21 to 30 years	15	12.1	12.1
	More than 30 years	50	40.3	40.3
	Total	124	100.0	100.0

As illustrated in Table 5.4, 40.3% of the organizations have been in operation for more than 30 years. Meanwhile, organizations operating for 6-10 years represented the second largest group (18.5% of the total organizations). The rest are represented by organizations operating for 1-5 years (13.7%), 11-20 years (12.9%), 21-30 years (12.1%), and less than a year (2.4%). Although we might expect all organizations to employ InfoSec as soon as they commence operation, there are reasons to believe the level of InfoSec is affected, positively or negatively by age of the organization (Murphy 2012).

Table 5.5 shows whether each organization had an existing information technology (IT) department.

**Table 5.5 Presence of IT department in organization**

Does your organization have an IT department? (N=124)				
		Frequency	Percent	Valid Percent
Valid	Yes	85	68.5	68.5
	No	39	31.5	31.5
	Total	124	100.0	100.0

It can be seen from Table 5.5 that 68.5% of the respondent organizations had IT departments, whereas 31.5% did not yet have an IT department. Given the significance of safeguarding an organization's sensitive information, effective information security control is critical for all organizations (United States Government Accountability Office 2007). Thus, departments processing and handling important information files need to coordinate with the IT department to ensure that all data protection measures are applied appropriately (Purser 2004).

Coincidentally 66.1% of organizations were large, employing over 100 people. It is probable that the majority of organizations with an IT department were also large organizations.

Table 5.6 shows that 56.5% of the participating organizations provided a specific budget for IT. In both theory and practice, the potential value of IT infrastructure in organizations is recognized. Considering that expenditure for IT infrastructure accounts for over 58% of a typical organizational IT budget (Byrd & Turner 2000), it is very important for organizations to set aside a specific budget for information technology. However, the size of organizations in the survey includes many small organizations which may have quite simple financial / budgetary process. Even in the large organizations, funding of IT can take many forms including charge back, individual budget etc. So, the fact that there is not an IT budget in 31.5% of organizations is not necessarily a problem.

**Table 5.6 Organization IT budget**

<b>Does your organization have a specific IT budget? (N=124)</b>				
		Frequency	Percent	Valid Percent
Valid	Yes	70	56.5	56.5
	No	39	31.5	31.5
	Not Sure	15	12.1	12.1
	Total	124	100.0	100.0

Table 5.7 revealed that 62.1% of participating organizations did not have a specific budget for information security. 19.4% of the respondents were unsure whether they had a specific budget and approximately the same proportion of respondents affirmed that there was a specific budget for information security in their organization. These findings may not be considered negative because, an organization may actually depend a lot on InfoSec and take InfoSec seriously even if InfoSec does not have it's own budget. It may be part of IT budget or it may be part of general expenditure, particularly in small organizations.

**Table 5.7 Organization information security budget**

<b>Does your organization have a specific Information Security budget? (N=124)</b>				
		Frequency	Percent	Valid Percent
Valid	Yes	23	18.5	18.5
	No	77	62.1	62.1
	Not Sure	24	19.4	19.4
	Total	124	100.0	100.0

Table 5.8 presents a frequency distribution of the organizations grouped according to the existence of at least one member of information security personnel.

**Table 5.8 Availability of staff who are knowledgeable about information security in organization**

<b>Is there at least one person in the organization who is knowledgeable about information security who tries to take care of information security matters? (N=124)</b>				
		Frequency	Percent	Valid Percent
Valid	Yes	73	58.9	58.9
	No	51	41.1	41.1
	Total	124	100.0	100.0

Table 5.8 shows that 58.9% of the organizations employed at least one person who was knowledgeable about and in charge of information security matters. However, the

remaining 41.1% of organizations did not have anyone taking care of information security issues. This can be a risk factor for organizations. Information security personnel are required to assess, manage and implement information security measures in an organization. Usually, a chief information security officer is assigned by an organization to perform these tasks (Whitman & Mattord 2012).

In the discussion of Table 5.7, it was suggested that InfoSec practices could still be good in the 81.5% of organizations which were either unsure about an InfoSec budget or did not have an InfoSec budget. Clearly, if 58.9% of organizations have InfoSec personal, their practices could still be good even if many of these had no specific budget.

### ***5.3 Information security laws standards and policies in organizations***

Laws often force organizations to deal with InfoSec where they might otherwise ignore it. Standards provide guidelines for how organizations should best address InfoSec. Sometimes organizations adopt standards to improve customer perception. Policies are the implementation of either law or standards, although some organizations may have policies that are not based on either laws or standards. While such policies may be better than nothing, an ad hoc policy, may not be very effective. The final components in this process are process for risk assessment and policy enforcement. Even if an organization has a comprehensive policy, it will be useless unless it is enforced and based on an accurate risk assessment.

#### **5.3.1 Information security laws in organizations**

Table 5.9 presents a frequency distribution of organizations according to the application of any data protection or information security law.

**Table 5.9 Data protection or information security law in organizations**

<b>Does your organization apply any data protection or information security law? (N=124)</b>				
		Frequency	Percent	Valid Percent
Valid	Yes	36	29.0	29.0
	No	88	71.0	71.0
	Total	124	100.0	100.0

As depicted in Table 5.9, 71% of the organizations included in the study had not applied any data protection or information security law, which is a serious concern for both private organizations and government. The absence of any law can increase electronic crimes and be a direct threat for information security. Meanwhile, the rest of the organizations (29%) have applied at least one data protection or information security law. Currently, the Kingdom of Saudi Arabia has no laws pertaining to data protection (Chambers & Rand 2010). However, Shari'ah law contains several provisions that award compensation to persons who suffer loss or harm as a result of unauthorized disclosure of personal information. Liability and penalties are handled on a case by case basis, with the possibility of severe penalties in cases of non-compliance to Shari'ah law (Albosaily & Rinker-Morris 2012).

Table 5.10 presents a frequency distribution of respondents according to their comfort level in relation to data protection laws. Only 77 of 124 participants provided a response about if they feel comfortable with the laws because respondents who marked NO have been asked to skip the next 5 questions which about Laws evaluation. Among those who responded, 41 of 77 respondents indicated (N/A) option and 36 responded to the other question options which is exactly the same number of respondents who choose yes in the previous question. The reasons of having N/A response in this question and the next 4 questions which are about the quality, comprehensiveness and power of the laws may be because the respondents who do not have an InfoSec law in their organizations have marked N/A as their response since the question is not applicable to them. In this case, "an actual percent" column has been added in this section in Tables 5.10, 5.11, 5.12 and 5.13 and in some other questions in section 5.4.2 to have correct statistics about these questions.



**Table 5.10 Comfort level with data protection law**

<b>I feel comfortable with this law (N=77)</b>					
		Frequency	Percent	Valid Percent	Actual Percent
Valid	Strongly Disagree	5	4.0	6.4	13.9
	Disagree	16	12.9	21.0	44.4
	Agree	10	8.1	13.0	27.8
	Strongly Agree	5	4.0	6.4	13.9
	N/A	41	33.1	53.2	
	Total	77	62.1	100.0	36
Missing	System	47	37.9		
Total		124	100.0		

As indicated in Table 5.10, 44.4% and 13.9% expressed their disagreement and strong disagreement respectively regarding their comfort with the data protection law being applied in their organizations. Meanwhile, 27.8% and 13.9% of the respondents indicated their agreement and strong agreement respectively with comfort with the data protection law. Employee comfort level in adhering to data protection laws and policies needs to be considered since it can influence actual compliance. The use of complex, confusing and incomprehensible language can cause comfort levels of IT staff to drop significantly. In addition, the number of information security policies should be tracked since an increasing number of policies can also cause staff comfort levels to go down (Wright 2008).

Table 5.11 presents a frequency distribution of respondents according to level of comfort in relation to the quality of data protection laws.

**Table 5.11 Quality of data protection law in organizations**

<b>I feel comfortable about the quality of this law (N=77)</b>					
		Frequency	Percent	Valid Percent	Actual Percent
Valid	Strongly Disagree	5	4.0	6.4	13.9
	Disagree	18	14.6	23.4	50.0
	Agree	10	8.0	13.0	27.8
	Strongly Agree	3	2.4	4.0	8.3
	N/A	41	33.1	53.2	
	Total	77	62.1	100.0	36
Missing	System	47	37.9		
Total		124	100.0		

As illustrated in Table 5.11, 50% of the respondents expressed their disagreement with

the quality of existing data protection laws and 13.9% showed their strong disagreement. On the other hand, 27.8% of the respondents expressed agreement that they were comfortable with the quality of the data protection law and 8.3% showed strong agreement. Table 5.11 has shown that 63.9% are not comfortable about the quality of the law. So, it would appear that either the law is not appropriate or the organization's implementation of it is poor. Data protection laws all over the world have remained unclear in terms of who and what these laws actually protect. This is attributed to the sheer complexity of having a wide range of information types and contexts to consider (Bygrave 2002).

Table 5.12 presents the frequency and percentage distribution of respondents grouped according to comfort level in relation to the comprehensiveness and appropriateness of data protection laws.

**Table 5.12 Comprehensiveness and appropriateness of data protection law in organizations**

<b>I feel comfortable about the comprehensive and appropriate of this law (N=77)</b>					
		Frequency	Percent	Valid Percent	Actual Percent
Valid	Strongly Disagree	6	4.8	7.8	16.7
	Disagree	19	15.3	24.7	52.8
	Agree	8	6.5	10.4	22.2
	Strongly Agree	3	2.4	3.9	8.3
	N/A	41	33.1	53.2	
	Total	77	62.1	100.0	36
Missing	System	47	37.9		
Total		124	100.0		

As shown in Table 5.12, 52.8% and 16.7% expressed their disagreement and strong disagreement respectively with the comprehensiveness and appropriateness of current data protection laws. In contrast, 22.2% and 8.3% of the respondents showed their agreement and strong agreement respectively with the comprehensiveness and appropriateness of data protection laws. Table 5.12 has shown that 69.5% are not comfortable about the comprehensiveness and appropriateness of the law. So, it would appear that either the law is not appropriate or the organization's implementation of it is poor. An information security law should be comprehensive, appropriate and meet the needs of the organization.

Table 5.13 presents a frequency distribution of respondents grouped according to level

of comfort in relation to the power of data protection laws.

**Table 5.13 Power of data protection or information security law in organizations**

I feel comfortable about the power of this law (N=77)					
		Frequency	Percent	Valid Percent	Actual Percent
Valid	Strongly Disagree	6	4.8	7.8	16.7
	Disagree	17	13.7	22.1	47.2
	Agree	9	7.3	11.7	25.0
	Strongly Agree	4	3.2	5.2	11.1
	N/A	41	33.1	53.2	
	Total	77	62.1	100.0	36
Missing	System	47	37.9		
Total		124	100.0		

As shown in Table 5.13, 47.2% of the respondents indicated their disagreement with the position of being comfortable with the power of data protection laws and 16.7% showed their strong disagreement. On the other hand, 25% of respondents expressed agreement and 11.1% showed strong agreement. Table 5.13 has shown that 63.9% are not comfortable about the power of the law. So, it would appear that either the law is not appropriate or the organization's implementation of it is poor.

However, it is not necessary to have or follow a law if there are appropriate standards. The next section discusses the InfoSec standards in the respondents' organizations.

### **5.3.2 Information security standards in organizations**

Although Saudi organizations do not generally apply laws, the following section looks at how they apply standards. Table 5.14 presents a frequency distribution of organizations according to adherence to any information security standard. As shown in Table 5.14, 65.3% of the organizations considered in the study had not applied any information security standard. The rest of the organizations (34.7%) had applied at least one information security standard. A higher proportion of organizations follow standards (34.7%) compared to law (29%). Although the percentage following standards is still low, standards are probably better to implement as policies. This can be considered as a risk factor for organizations.

**Table 5.14 Organization distribution according to whether any information security standards are applied**

Does your organization apply any InfoSec standards? (N=124)				
		Frequency	Percent	Valid Percent
Valid	Yes	43	34.7	34.7
	No	81	65.3	65.3
	Total	124	100.0	100.0

Table 5.15 shows a frequency distribution of organizations without information security standards, in terms of whether they intend to apply any InfoSec standards in the future. Table 5.15 shows that 57.4% of 108 respondents were unsure whether their organization had plans to apply information security standards in the future. 22.2% of organizations surveyed did not have future plans for the application of information security standards, while 20.4% of the organizations intended to apply information security standards in the future.

**Table 5.15 Future plans to apply information security standards**

Does your organization plan to apply information security standards in the future? (N=108)				
		Frequency	Percent	Valid Percent
Valid	Yes	22	17.7	20.4
	No	24	19.4	22.2
	Not Sure	62	50.0	57.4
	Total	108	87.1	100.0
Missing	System	16	12.9	
Total		124	100.0	

Table 5.16 shows frequency distribution of organizations with applied information security standards in terms of whether these standards have increased the perception of security. 48.8% of the respondents felt that their sense of security had improved 'somewhat' with information security standards in place. Respondents who expressed a sense of security accounted for 23.3% of the total while 27.9% indicated a lack of it.

**Table 5.16 Perceived sense of security with the application of information security standards**

<b>If your organization has already applied information security standards, do you feel more secure in your organization? (N=108)</b>					
		Frequency	Percent	Valid Percent	Actual Percent
Valid	Yes	10	8.1	9.3	23.3
	No	12	9.7	11.1	27.9
	Somewhat	21	16.9	19.4	48.8
	N/A	65	52.4	60.2	
	Total	108	87.1	100.0	43
Missing	System	16	12.9		
Total		124			

Table 5.17 presents a frequency distribution of respondents according to existence of personnel tasked with ensuring adherence to adopted information security standards. As shown in Table 5.17, 54.8% of respondents indicated that their respective organizations did not have any personnel assigned to ensuring that employees adhered to their organization's information security standard so perhaps that is why organizations do not feel more secure. Meanwhile, 29.8% of respondents revealed that their organization did have personnel assigned to the aforementioned task. 15.3% of the respondents expressed uncertainty as to whether their organizations had personnel assigned for information security standard adherence.

**Table 5.17 Distribution of employee respondents according to perceived existence of personnel tasked with ensuring adherence to adopted information security standards**

<b>Is there someone in your organization who is responsible for ensuring that adopted standards are being adhered to? (N=124)</b>				
		Frequency	Percent	Valid Percent
Valid	Yes	37	29.8	29.8
	No	68	54.8	54.8
	Not Sure	19	15.3	15.3
	Total	124	100.0	100.0

It is clear that organizations have very poor uptake of laws and poor uptake of standards. But organizations can develop a policy even without a law or standard. However, there is a danger that such policies may be ad hoc and of little value. The next section looks at policies in the respondents organizations.

### **5.3.3 Information security policies in organizations**

This section discusses information assurance in the participating organizations in terms

of the existence of information security policies, data backup, risk assessment and reporting of security incidents.

Table 5.18 presents a frequency distribution of organizations grouped according to existence of an information security policy. Table 5.18 indicates that most of the organizations (61.3%) did not have an information security policy in place. Meanwhile, 38.7% of respondents have policy adoption. Although there is marginally higher rate of policies than either laws or standards, it is still low. This can be a risk factor because information security policies are the foundation that supports the security of information resources in organizations.

**Table 5.18 Existence of information security policy in organization**

<b>Does your organization have an information security policy? (N=124)</b>				
		Frequency	Percent	Valid Percent
Valid	Yes	48	38.7	38.7
	No	76	61.3	61.3
	Total	124	100.0	100.0

To determine the effectiveness of the policy we need to know if it is enforced and well-planned. If it is not enforced, it may be useless. Table 5.19 presents a frequency percentage distribution of respondents organizations grouped according to enforcement of an existing information security policy.

**Table 5.19 Organization enforcement of information security policy**

<b>If there is an information security policy, does your organization enforce it? (N=124)</b>				
		Frequency	Percent	Valid Percent
Valid	Yes	10	8.1	8.1
	No	66	53.2	53.2
	Not Sure	48	38.7	38.7
	Total	124	100.0	100.0

In those organizations where a policy existed (38.7%) it is only enforced in 8.1% of those organizations. This raises serious doubts about the effectiveness of these policies. The other vital test is whether the policy is well-planned. If it is not well-planned, then the policy may not have identified the right information and resources to be secured or it may not have chosen the right mechanisms by which to secure those resources.

Information security policy may be enforced in several ways such as: technology-based enforcement, executive enforcement, audit-based enforcement and traditional management enforcement practices (Wylder 2012).

The risk assessment data in Table 5.20 shows that only 33.1% of all organizations have a risk assessment process. Given that 38.7% of all organizations have a security policy, at least 14% and possibly more, of those organizations do not have a risk assessment process. So, even where a security policy exists it may be protecting the wrong data or protecting it inappropriately. This low practice in risk assessment processes can increase risk and cause serious further information security problems for organizational assets.

**Table 5.20 Organization risk assessment process**

<b>Does your organization have a risk assessment process? (N=124)</b>				
		Frequency	Percent	Valid Percent
Valid	Yes	41	33.1	33.1
	No	83	66.9	66.9
	Total	124	100.0	100.0

This section has shown us that only 29% of surveyed organizations apply any InfoSec law and only 34.7% apply any InfoSec standards. However, an organization may still have effective InfoSec if it has policies in place which are well-planned and enforced. Unfortunately, only 38.7% of organizations surveyed had an InfoSec policy and it appears that the majority of these organizations do not enforce the policy. Finally, 66.9% of organizations surveyed do not have a risk assessment policy which is cornerstone of good InfoSec.

However, it is still possible to have adequate InfoSec practices without having formal policies or standards. Section 5.4 assesses the InfoSec practices in the organizations.

#### **5.4 Information assurance in the organization**

This section discusses information assurance procedures, tools and measures in the organizations including: managing users' accounts, having a data backup policy, having an incident reporting plan, vulnerability assessment, password practices, two factor authentications, firewalls, Internet use restrictions, software updates, anti-virus software, intrusion detection software, encryption, server room physical security, device

use restriction and employee training.

Table 5.21 indicated that 65.3% of the organizations had procedures and regulations for account creation and management, while 34.7% of the organizations did not. The number of organizations using account management far exceeds those with InfoSec policies, so this suggests that a significant proportion of organizations may have an ad hoc approach to InfoSec which may be quite effective. However, it is still alarming that 34.7% of organizations surveyed do not have account management at all.

**Table 5.21 Organization procedures and regulations for account creation and management**

<b>Do you have procedures and regulations in creating and managing users' accounts? (N=124)</b>				
		Frequency	Percent	Valid Percent
Valid	Yes	81	65.3	65.3
	No	43	34.7	34.7
	Total	124	100.0	100.0

Table 5.22 shows that 63.7% of organizations had a data backup and recovery policy. However, 36.3% of participants indicate that their organizations did not. This can be a serious risk factor because data backup acts as an insurance plan for organizations. It is very important because files may accidentally be deleted, mission-critical data can become corrupt and natural disasters can occur. With a solid backup and recovery plan, organizations can recover from any of these threats.

**Table 5.22 Organization data backup and recovery policy**

<b>Does your organization have a data backup and recovery policy? (N=124)</b>				
		Frequency	Percent	Valid Percent
Valid	Yes	79	63.7	63.7
	No	45	36.3	36.3
	Total	124	100.0	100.0

Table 5.23 indicated that only 31.5% of organizations did have a security incident reporting plan. The much lower percentage who have a reporting plan compared to those who have a data backup plan suggests a focus on prevention rather than reporting or contingency. The risks posed by either deliberate or accidental human actions (such as user error in IT processes, fraud and theft) should be covered by a specific department handling information security matters. Moreover, establishment of a



mechanism for reporting security incidents and inferred weaknesses in the existing system is necessary for a stronger sense of security among organizational stakeholders (Furnell et al. 2008).

**Table 5.23 Organization security incident reporting plan**

<b>Does your organization have a security incident reporting plan? (N=124)</b>				
		Frequency	Percent	Valid Percent
Valid	Yes	39	31.5	31.5
	No	85	68.5	68.5
	Total	124	100.0	100.0

#### 5.4.1 Information assurance tool/measures in the organization

Table 5.24 indicates that most vulnerability assessments performed in organizations have fared poorly (29%) or very poorly (20.2%). 14.5% of the organizations reported good vulnerability assessments and only 6.5% assessed them as very good.

**Table 5.24 Vulnerability assessment in organizations**

<b>How effective do you think Vulnerability Assessment performed in your organization (6=very good; 5=good;4=neutral;3=poor;2=very poor;1=not exist) (N=124)</b>				
		Frequency	Percent	Valid Percent
Valid	Not Exist	14	11.3	11.3
	Very Poor	25	20.2	20.2
	Poor	36	29.0	29.0
	Neutral	23	18.5	18.5
	Good	18	14.5	14.5
	Very Good	8	6.5	6.5
	Total	124	100.0	100.0

A previous question showed that only 33% of organizations had a risk assessment policy. Table 5.24 shows that 21% of all organizations had an “acceptable” (i.e. good or very good) vulnerability assessment. This means that at least 37% of the organizations with risk assessment policies still have unacceptable vulnerability practices.

Vulnerability assessments are an important aspect of information security since they enable systems administrators to determine, monitor and manage activities designed to address system vulnerabilities. The most common vulnerability assessment services

include: vulnerability scanning, vulnerability assessment and penetration testing, and application assessment (Kizza 2005). The histogram for Table 2.24, shown in Figure 5.1, indicates that vulnerability assessments performed in the respondent organizations have tended to generate lower ratings.



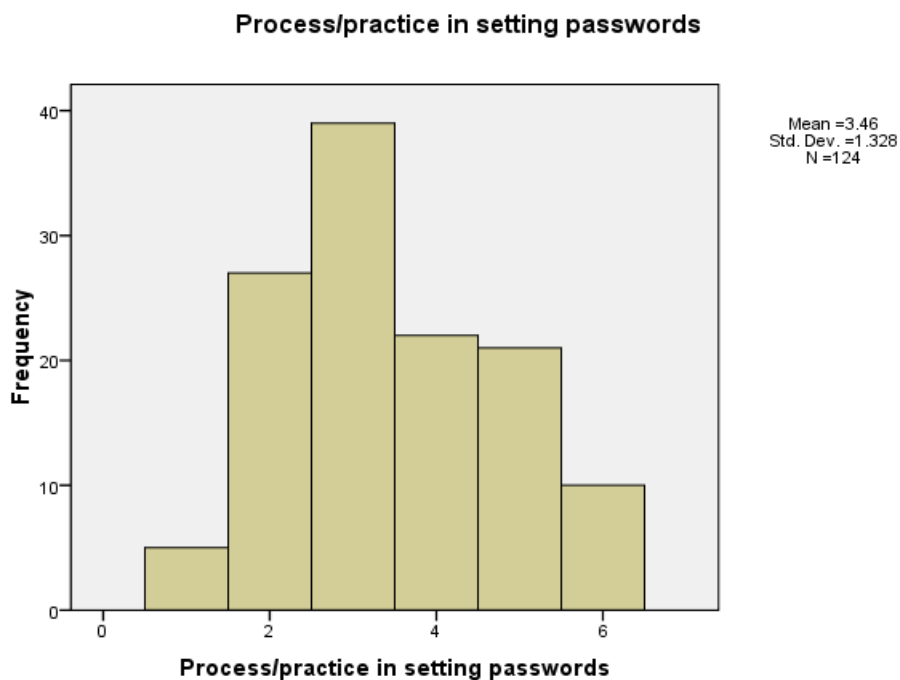
**Figure 5.1 Vulnerability assessment in organizations frequency histogram**

Data from Table 2.25 reveals that 31.5% of the organizations had poor security measures with respect to setting passwords. Another 21.8% of the organizations had very poor procedures in setting passwords. Only 8.1% of the organizations had very good and 16.9% had good password security processes. 17.7% chose to stay neutral regarding the issue and 4% of the respondents reported that password setting was not practiced in their organization. It may be observed from the framing of the item that it was the practice, not the policy, that was being evaluated.

**Table 5.25 Organization password practice**

How secure is your organization process/practice in setting passwords? (6=very good; 5=good;4=neutral;3=poor;2=very poor;1=not exist) (N=124)				
		Frequency	Percent	Valid Percent
Valid	Not Exist	5	4.0	4.0
	Very Poor	27	21.8	21.8
	Poor	39	31.5	31.5
	Neutral	22	17.7	17.7
	Good	21	16.9	16.9
	Very Good	10	8.1	8.1
	Total	124	100.0	100.0

As posited in Qureshi et al. (2009), “password mechanisms and their users form a socio-technical system, whose effectiveness relies strongly on users’ willingness to make the extra effort that security conscious behaviour requires”. Figure 5.2 shows the histogram for Table 5.25. It suggests that security regarding the setting of passwords in the respective organizations generally tends to produce lower ratings.



**Figure 5.2 Organization password practice frequency histogram**

As shown in Table 5.26, 66.1% of organizations had not implemented two-factor authentication such as smart cards, biometric or one-time passwords, with the remaining

one-third already having implemented two-factor authentication. Two-factor authentication has the lowest practice so far; perhaps because it is a relatively sophisticated practice, so it's not surprising that it's lower. The pairing of two basic authentication approaches is very well established among many organizations (Furnell et al. 2008). The results of this survey indicate that two-factor authentication implementation in the respective organizations is low.

**Table 5.26 Implementation of two-factor authentication in organizations**

<b>Does your organization implement two-factor authentication in your organization (i.e. smart-card, biometric, one-time password...etc ) (N=124)</b>				
		Frequency	Percent	Valid Percent
Valid	Yes	42	33.9	33.9
	No	82	66.1	66.1
	Total	124	100.0	100.0

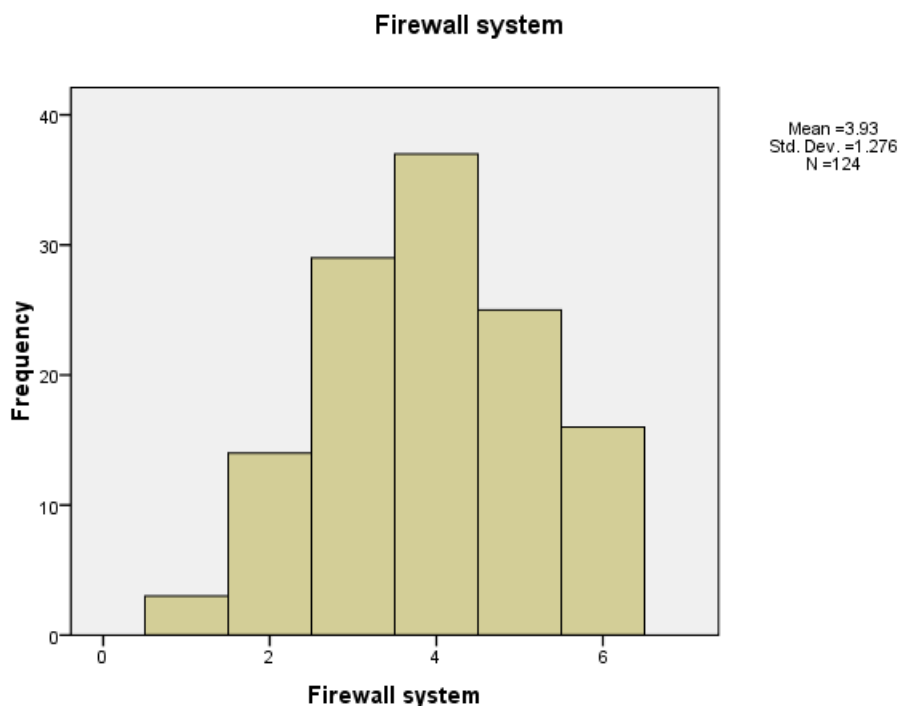
Firewalls are one of the most crucial elements in information security. Table 5.27 revealed that 29.8% of the respondents stood on neutral ground with respect to the security of the firewall systems installed in their organizations. 33.1% of the organizations reported that their firewall systems were good or very good, while 34.7% of the organizations had poor or very poor firewall systems. 2.4% of organizations did not have security firewall systems at all. Firewall scores 33.1% on adequate (good and very good) and that's the highest score for a practice so far; perhaps because it does not rely on users behaving themselves.

**Table 5.27 Organization firewall systems**

<b>How secure is your organization Firewall system to protect against undesired access to organization servers from outside the organization? (6=very good; 5=good;4=neutral;3=poor;2=very poor;1=not exist) (N=124)</b>				
		Frequency	Percent	Valid Percent
Valid	Not Exist	3	2.4	2.4
	Very Poor	14	11.3	11.3
	Poor	29	23.4	23.4
	Neutral	37	29.8	29.8
	Good	25	20.2	20.2
	Very Good	16	12.9	12.9
	Total	124	100.0	100.0

The secret to the success of firewalls is the formulation and implementation of filtering rules that protect the system from unauthorized access (Alshaer & Hamed 2004). The

histogram for Table 5.27, shown in Figure 5.3, indicates that firewall systems in the respective organizations were almost normally distributed. However, taking away the neutral ratings from the picture clearly directs the distribution to the lower end of the ratings since the lowest three ratings (not existent to poor) have a cumulative percentage of 37.1%, whereas the combined percentage of the two highest ratings (good and very good) is 33.1%.



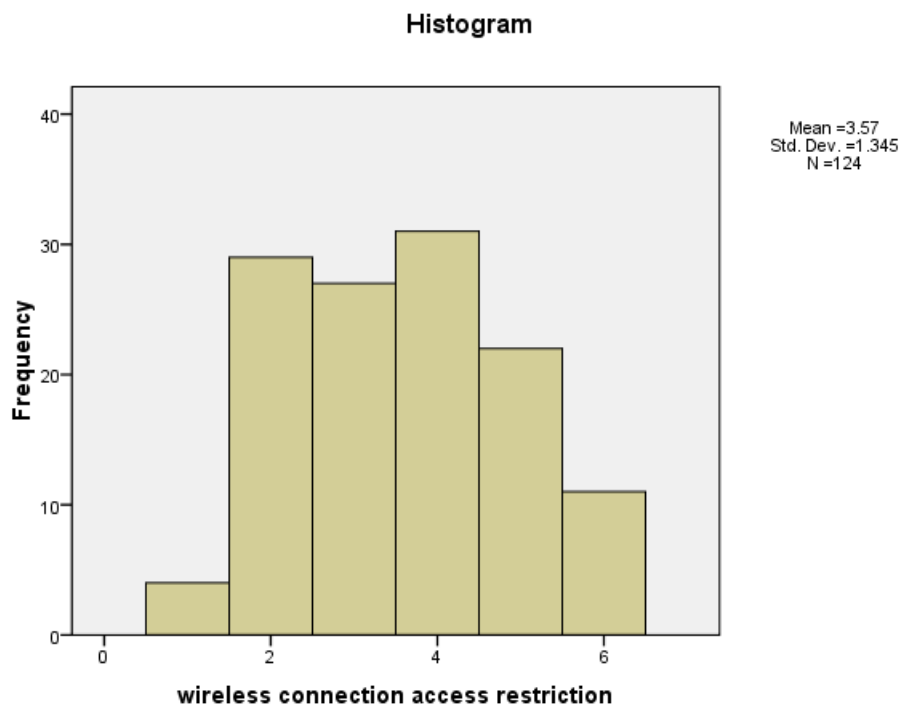
**Figure 5.3 Organization firewall systems frequency histogram**

Table 5.28 indicates that 45.2% of the organizational wireless access restrictions received poor (21.8%) or very poor (23.4%) ratings from their organizational representatives, whereas 26.6% of the organizations reported strict or very strict wireless access restrictions. 25% indicated neutrality on the issue and 3.2% of organizations reported no existing Internet access restrictions.

**Table 5.28 Organization wireless connection restrictions**

If your organization has wireless connection, how strict are the access rules that only its employees can use this wireless network? (6=very strict; 5=strict;4=neutral;3=poor restriction;2=very poor restriction;1=not exist) (N=124)				
		Frequency	Percent	Valid Percent
Valid	Not Exist	4	3.2	3.2
	Very Poor	29	23.4	23.4
	Poor	27	21.8	21.8
	Neutral	31	25.0	25.0
	Strict	22	17.7	17.7
	Very Strict	11	8.9	8.9
Total		124	100.0	100.0

Figure 5.4 shows the histogram for Table 5.28. It suggests that information security measures regarding Internet access controls in more organizations are relatively strict.



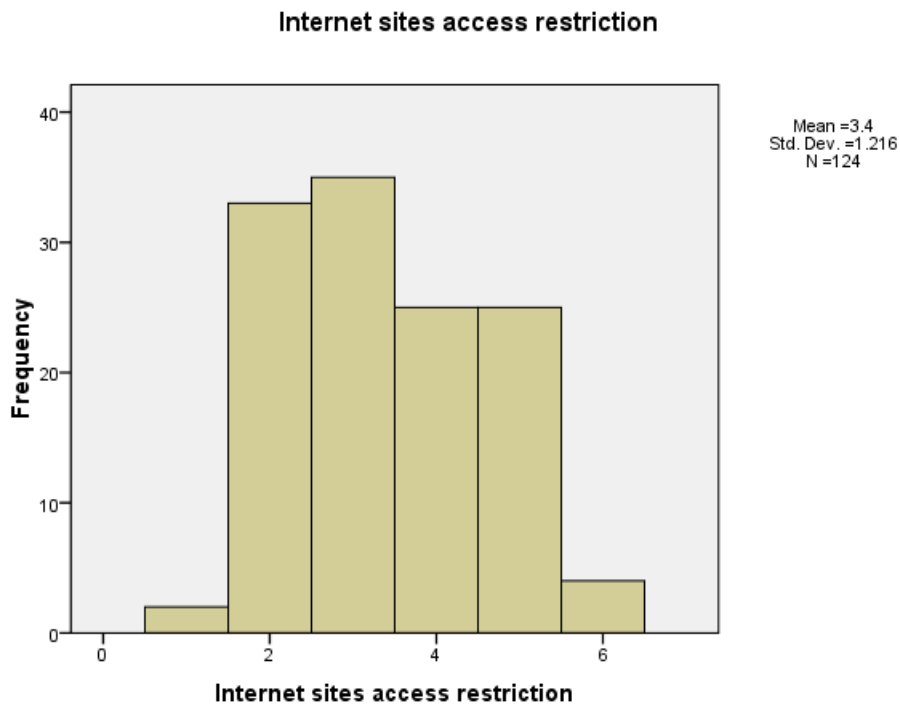
**Figure 5.4 Organization Internet access restrictions frequency histogram**

Table 5.29 revealed that 54.8% of organizational policies on restricting access to specific websites received poor (28.2%) and very poor (26.6%) ratings. 20.2% of the respondents took the neutral position on the issue. 23.4% reported that they had strict or very strict measures to restrict access to specific websites.

**Table 5.29 Organization policies on restricting access to specific websites**

How restrictive is your organization with access to specific Internet sites? (6=very strict; 5=strict;4=neutral;3=poor restriction;2=very poor restriction;1=not exist) (N=124)				
		Frequency	Percent	Valid Percent
Valid	Not Exist	2	1.6	1.6
	Very Poor	33	26.6	26.6
	Poor	35	28.2	28.2
	Neutral	25	20.2	20.2
	Strict	25	20.2	20.2
	Very Strict	4	3.2	3.2
	Total	124	100.0	100.0

Restriction policies on access to specific websites usually utilize a database containing websites that are prohibited from being accessed within the organization (Li & Li 2011). Internet access control methods, such as content filtering and blocking, serve as a protective barrier that prevents access to inappropriate and harmful content (Li & Li 2011). The histogram for Table 5.29, shown in Figure 5.5, indicates that restriction policies on access to specific websites in the respective organizations were generally given low ratings.



**Figure 5.5 Organization policies on restricting access to specific websites frequency histogram**

Table 5.30 shows that 46% of the organizations updated their operating systems and software on an annual basis. It is interesting to note that 33.9% of the organizations had never updated their operating systems and software. The rest of the organizations updated their operating systems and software packages on a quarterly (8.1%), monthly (5.6%), weekly (3.2%) or daily (3.2%) basis.

**Table 5.30 Operation systems and software updates in organizations**

<b>Does your organization keep operating systems and or software packages updated with most recent software/update releases? (N=124)</b>				
		Frequency	Percent	Valid Percent
Valid	Daily	4	3.2	3.2
	Weekly	4	3.2	3.2
	Monthly	7	5.6	5.6
	Quarterly	10	8.1	8.1
	Annually	57	46.0	46.0
	Never	42	33.9	33.9
	Total	124	100.0	100.0

Operating systems and software applications provide update patches on a regular basis. While some updates are provided for improved functionality, other updates are security-related, making it crucial to keep track of updates and install them as soon as they become available (Thompson & Thompson 2006). Given that only 12% of organizations update monthly or more frequently 88% of organizations have operating systems and software packages that are significantly out of data and may pose massive risks. This is the worst practice seen so far.

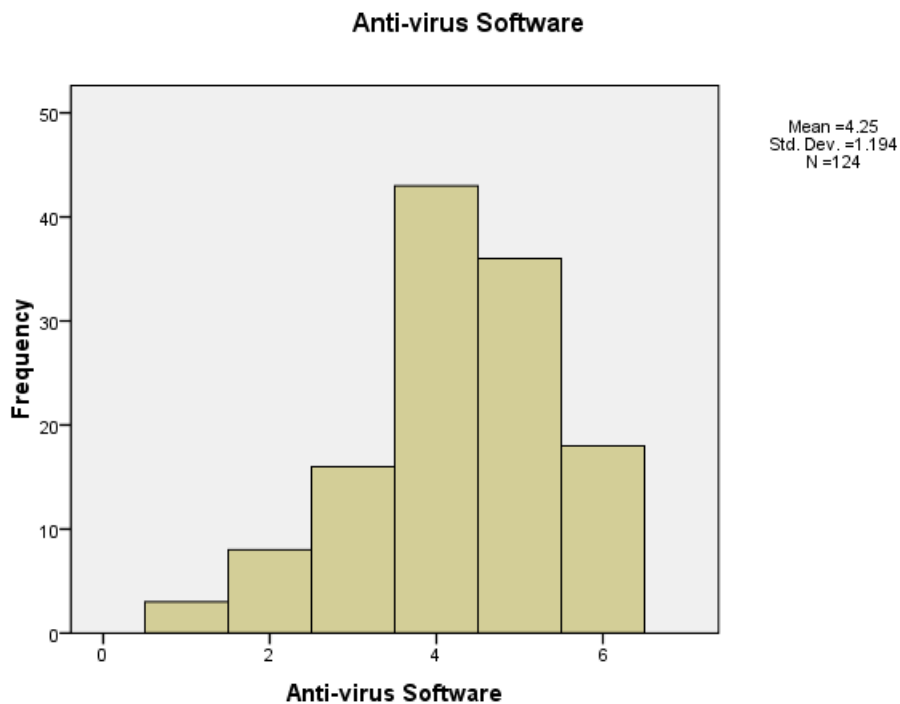
Table 5.31 reveals that the strength of the anti-virus software used by organizations was rated as good or very good by 43.5% of respondents. 34.7% of the organizations adopted a neutral stance on this issue. On the other hand, 19.4% of organizations indicated poor or very poor ratings for the strength of their anti-virus software. The score of 43.5% good or very good is the best score for practice so far. Why is that? Our study of ISA showed that many Saudis are aware of viruses, so perhaps employees too are aware.



**Table 5.31 Strength of anti-virus software in organizations**

How strong is your organization anti-virus software? (6=very good; 5=good;4=neutral;3=poor;2=very poor;1=not exist) (N=124)				
		Frequency	Percent	Valid Percent
Valid	Not Exist	3	2.4	2.4
	Very Poor	8	6.5	6.5
	Poor	16	12.9	12.9
	Neutral	43	34.7	34.7
	Good	36	29.0	29.0
	Very Good	18	14.5	14.5
	Total	124	100.0	100.0

Anti-virus software is a crucial element of information security because it serves as a solid line of defense capable of detecting and removing viruses before they cause significant harm to the system and the data stored in it (Ferguson 2005). The histogram for Table 5.31 is shown in Figure 5.6. It indicates that the strength of anti-virus software in the respective organizations was generally given high ratings.



**Figure 5.6 Strength of anti-virus software in organizations frequency histogram**

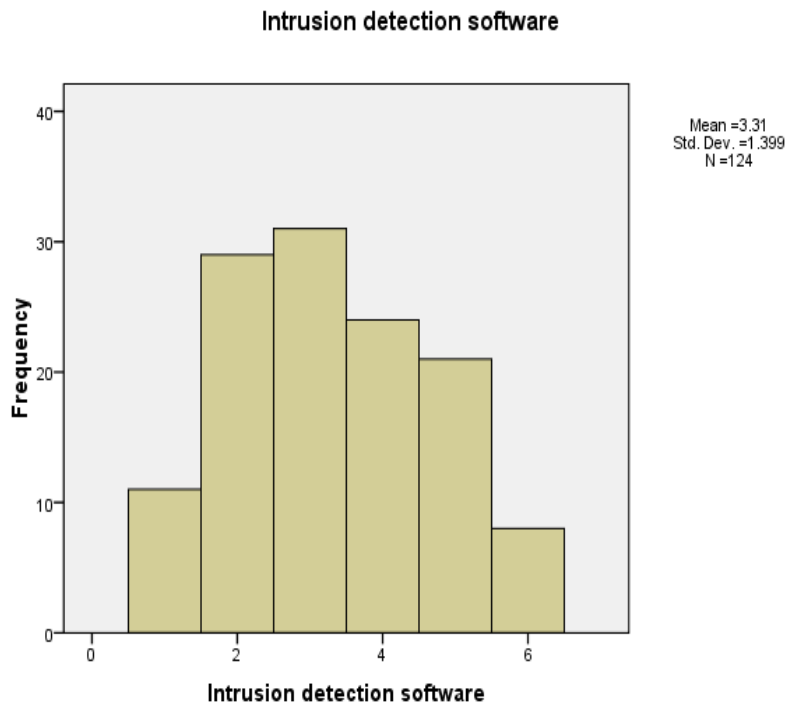
As depicted in Table 5.32, 48.4% of the organizations had poor or very poor intrusion detection systems. Moreover, 8.9% of the organizations did not even have intrusion

detection systems. It is possible that the 24 (19.4%) respondents who took the middle ground by responding neutral to this item did not consider their system to be effective but preferred not to project a negative image of their respective organizations. Only 23.4% of the organizations had good or very good intrusion detection systems installed. Why is this so low compared to virus protection? May be because of lower ISA, but IT staff should be aware.

**Table 5.32 Intrusion detection software in organizations**

How strong is your organization intrusion detection software? (6=very good; 5=good;4=neutral;3=poor;2=very poor;1=not exist) (N=124)				
		Frequency	Percent	Valid Percent
Valid	Not Exist	11	8.9	8.9
	Very Poor	29	23.4	23.4
	Poor	31	25.0	25.0
	Neutral	24	19.4	19.4
	Good	21	16.9	16.9
	Very Good	8	6.5	6.5
Total		124	100.0	100.0

Intrusion detection systems harmonize with protective mechanisms such as firewalls in enhancing information system security. Intrusion detection provides more knowledge about intrusions that happened or are currently happening so that the organization can better prepare for future information security threats and risks (Ning & Sushil 2004). Figure 5.7 shows the histogram for Table 5.32. It suggests that only a relatively few organizations have effective intrusion detection systems in place.



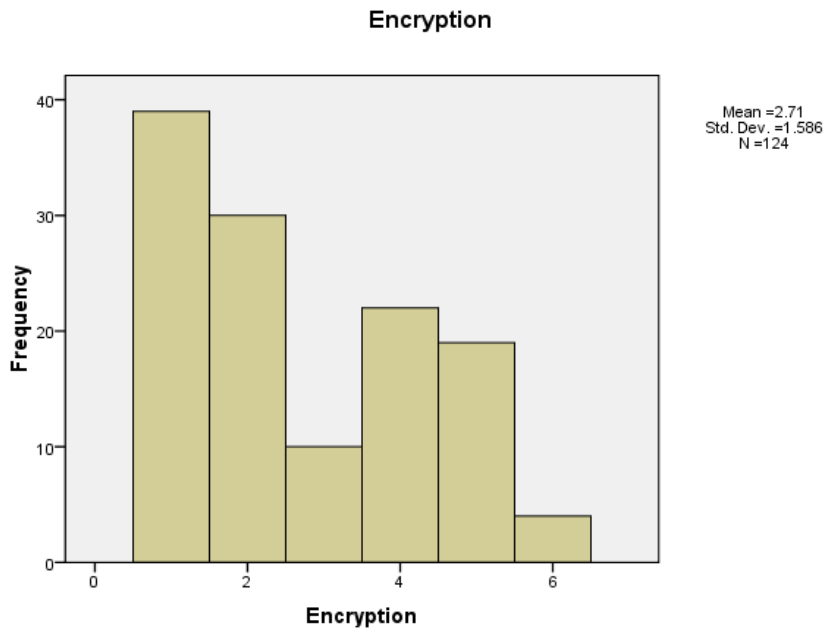
**Figure 5.7 Intrusion detection software in organizations frequency histogram**

As shown in Table 5.33, 31.5% of the organizations did not utilize encryption technology to protect their data. For organizations that used encryption technologies, 32.3% indicated poor (8.1%) to very poor (24.2%) effectiveness of the data encryption technologies currently being used. The rest of the respondents reported good (15.3%), and very good (3.2%) ratings, together with 17.7% of those who took a neutral position indicating that their encryption technology is neither good nor poor. 18.5% scored adequate (good or very good), one of lowest scores for practices. Why? How common a threat is data theft from unencrypted data storages? Maybe it is not seen as a “real” threat?

**Table 5.33 Data encryption systems in organizations**

How effective is your organization encryption for its important data? (6=very good; 5=good;4=neutral;3=poor;2=very poor;1=not exist) (N=124)				
		Frequency	Percent	Valid Percent
Valid	Not Exist	39	31.5	31.5
	Very Poor	30	24.2	24.2
	Poor	10	8.1	8.1
	Neutral	22	17.7	17.7
	Good	19	15.3	15.3
	Very Good	4	3.2	3.2
	Total	124	100.0	100.0

Data encryption and decryption techniques have been extensively used by information security professionals to keep information secure through the “security through obscurity” principle (Stewart et al. 2011). The histogram for Table 5.33, shown in Figure 5.8, indicates that the encryption systems in the respective organizations were generally given very low ratings.



**Figure 5.8 Data encryption systems in organizations frequency histogram**

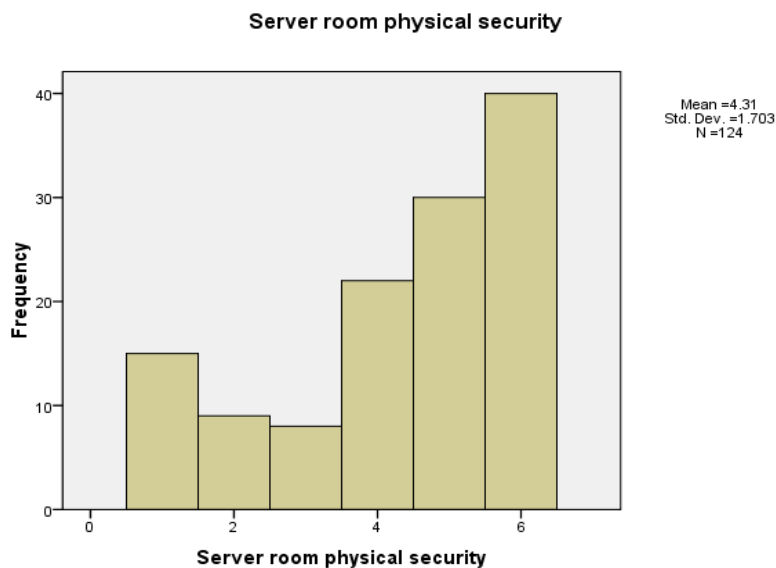
Table 5.34 shows that most of the organizations were convinced of the physical security capabilities of their server room, with the majority of respondents providing good (24.2%) or very good (32.3%) ratings. In contrast, some of the respondents reported poor (6.5%), and very poor (7.3%) ratings. Some respondents provided neutral

responses (17.7%). It is also noted that 15 organizations did not have physical security measures for their server room. 56.5% scored adequate (good and very good). Why? Physical security is relatively simple to achieve and deals with an obvious risk. Once set up there is little need for further updates.

**Table 5.34 Server room physical security in organizations**

How secure is your organization server room protected by physical security (i.e. PIN, Biometrics...etc)? (6=very good; 5=good;4=neutral;3=poor;2=very poor;1=not exist) (N=124)				
		Frequency	Percent	Valid Percent
Valid	Not Exist	15	12.1	12.1
	Very Poor	9	7.3	7.3
	Poor	8	6.5	6.5
	Neutral	22	17.7	17.7
	Good	30	24.2	24.2
	Very Good	40	32.3	32.3
	Total	124	100.0	100.0

The physical security of server rooms is crucial in maintaining information security. Important aspects include personnel access, storage, cooling, emergency power, humidity and fire protection, to name a few (Hintzbergen et al. 2010). Figure 2.9 shows the histogram for Table 5.34. It suggests that the majority of the organizations' server rooms had adequate physical security.



**Figure 5.9 Server room physical security in organizations frequency histogram**

17.7% scored adequate (good and very good). One of the poorest. Are we starting to see a trend? It's harder to control end users? But the question is actually about restrictions imposed by the organization. So our real question is why are not organizations more strict? Perhaps it's because so few vulnerability assessments means organizations not aware. Perhaps tech guys can not create procedures for staff generally.

Table 5.35 indicates that 60.5% of the organizations received poor (25%) and very poor (35.5%) ratings in terms of restricting the use of devices such as CD/DVD drives and USB memory drives. The rest of the respondents provided neutral (18.5%), strict (13.7%), and very strict (4%) ratings. However, four (3.2%) organizations reported that their organization had no policy restricting the use of input devices. 17.7% scored adequate (good and very good). One of the poorest. Are we starting to see a trend? It's harder to control end users? But the question is actually about restrictions imposed by the organization. So our real question is why are not organizations more strict? Perhaps it's because so few vulnerability assessments means organizations not aware. Perhaps tech guys can not create procedures for staff generally.

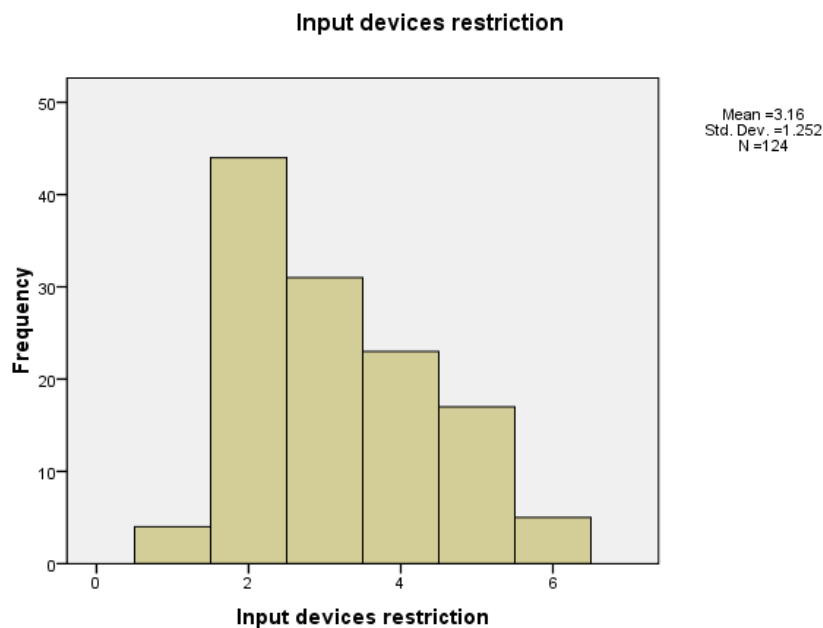
**Table 5.35 Restrictions on the use of input devices in organizations**

How restrictive is your organization with employees from using input devices such as CD/DVD drives and USB memory? (6=very strict; 5=strict;4=neutral;3=poor restriction;2=very poor restriction;1=not exist) (N=124)				
		Frequency	Percent	Valid Percent
Valid	Not Exist	4	3.2	3.2
	Very Poor	44	35.5	35.5
	Poor	31	25.0	25.0
	Neutral	23	18.5	18.5
	Strict	17	13.7	13.7
	Very Strict	5	4.0	4.0
	Total	124	100.0	100.0

Input devices such as USB drives are known to be used as carriers of Trojan horses and malware, which can compromise the security of a computer system. Disgruntled employees and persons engaged in espionage may also use these devices to copy and steal confidential data (Ciampa 2010). Restricting the use of such devices is therefore critical for information security. 17.7% scored adequate (good and very good). One of the poorest. Are we starting to see a trend? It's harder to control end users? But the question is actually about restrictions imposed by the organization. So our real question is why are not organizations more strict? Perhaps it's because so few vulnerability

assessments means organizations not aware. Perhaps tech guys can not create procedures for staff generally.

Table 5.35 shown in Figure 5.10, indicates that most of the organizations did not generally impose restriction on the use of removable input devices such as CD/DVD drives and flash drives.



**Figure 5.10 Restrictions on the use of input devices in organizations frequency histogram**

Table 5.36 indicated that the majority of organizations (70.2%) had not offered special information security training to employees while 29.8% had. This result indicates that the respondent organizations had a very low level of training. The lack of training may be the reason for low practices in some previous questions. Adequate information security training for all employees is required as per information security standards. Common training areas include information security awareness, asset classification and control, responding to security-related events, web access and messaging, user access control and responsibilities, legal compliance, and business continuity awareness and procedures (Calder 2006).

**Table 5.36 Information security training offered to employees in organizations**

<b>Does your organization offer special information security training to employees? (N=124)</b>				
		Frequency	Percent	Valid Percent
Valid	Yes	37	29.8	29.8
	No	87	70.2	70.2
	Total	124	100.0	100.0

As reflected in the data in Table 5.37, 44.4% of respondents from the participating organizations did not have plans to acquire information security certification. The second largest group of respondents (32.3%) intended to pursue a certification in information security but were unable to specify a time frame for this. 14.5% planned to acquire certification within the next 12 months and 8.1% intended to obtain their certification within the next 3 years. One person (0.8%) indicated his/her intention to do so within the next 10 years. There are now a growing number of educational programs focused on information security (Prabha 2004) which mirrors the importance of obtaining certifications in the field, particularly for those who are employed in IT-related positions. Employability and professional development of individuals working in the IT field can be enhanced by improving their competency through certifications (Echaore-McDavid 2008).

**Table 5.37 IT department staff distribution according to intent to obtain information security certification**

<b>Are you planning to acquire certification in InfoSec? (N=124)</b>				
		Frequency	Percent	Valid Percent
Valid	Yes, within the next 12 months	18	14.5	14.5
	Yes, within the next 3 years	10	8.1	8.1
	Yes, within the next 10 years	1	0.8	0.8
	Yes, but I'm not sure when	40	32.3	32.3
	No	55	44.4	44.4
	Total	124	100.0	100.0

In this chapter so far, we learned that very few organizations apply laws and only a few organizations have InfoSec policies (across a range of activities). We saw that enforcement was poor and risk assessment policies were rare. However, it is possible that ad hoc practices were still effective. Section 5.4 has shown that in almost every type of security practice the performance was inadequate. The performance, however, was not uniformly bad i.e. some practices were applied much worse than others. Those



practices that were mediocre were:

- Password practice.
- Wireless connection restrictions.
- Strength of anti-virus software.
- Server room physical security.

Those practices that were really poor were:

- Vulnerability assessments.
- Two-factor authentication.
- Firewall systems.
- Internet access restrictions.
- Operating systems and software updates.
- Intrusion detection software.
- Data encryption systems.
- Input devices use restrictions

#### **5.4.2 Information security risks in organizations**

This section discusses the incidence of information security risks such as attacks, vandalism and social threats.

Table 5.38 shows that 56.5% of organizations had experienced computer downtime caused by a computer virus infecting their systems. 11.3% of the respondent organizations' networks had never been brought down by a virus. 32.3% of the respondents were unsure whether their organization had been affected. One example of a virus attack causing serious downtime involves an email virus attached to an innocent-looking email. Once the attachment is opened, the virus will begin replicating itself, spreading to other computers in the network and clogging up servers with spam mail generated by the virus (Smith 2012).

**Table 5.38 Computer downtime due to viruses in organizations**

<b>Have your organization's information systems ever been down due to computer viruses? (N=124)</b>				
		Frequency	Percent	Valid Percent
Valid	Yes	70	56.5	56.5
	No	14	11.3	11.3
	Not Sure	40	32.3	32.3
	Total	124	100.0	100.0

Table 5.39 shows that 61.8% of organizations were unsure whether their website had been attacked by hackers. 20.6% of respondents indicated no reports of hacker attack on their organization's website. In contrast, 17.6% of the organizations reported their website being attacked by hackers. Hacking of organizational websites has a variety of motivations ranging from bragging rights to political causes. Examples of organizations that have reported hacking attacks include New York Times, Yahoo! and CNN (Camp & Lewis 2004).

**Table 5.39 Incidence of hacker attack on organization website**

<b>Has your organization's website ever been subjected to hacker attack? (N=124)</b>				
		Frequency	Percent	Actual Percent
Valid	Yes	18	14.5	17.6
	No	21	16.9	20.6
	Not Sure	63	50.8	61.8
	Do Not Have a Web Site	22	17.7	102
	Total	124	100.0	

Table 5.40 shows that majority of the organizations (74.2%) were unsure whether their information systems had been attacked by hackers. Meanwhile, 17.7% of the respondents reported no attacks from hackers. On the other hand, 8.1% indicated experience of a hacker attack. Although hacking had beneficial origins, individuals who have resorted to breaking into secured systems with the aim of causing damage has given hacking a negative image. Hacking was originally intended to be used as a means to discover vulnerabilities in the system with the aim of improving it. Today, expert hackers are known to be able to break into a system, steal information and cover up their tracks in the span of just 20 minutes (EC- Council 2010).

**Table 5.40 Incidence of hacker attack on organization's information systems**

<b>Have your organization's information systems been subjected to hacker attacks? (N=124)</b>				
		Frequency	Percent	Valid Percent
Valid	Yes	10	8.1	8.1
	No	22	17.7	17.7
	Not Sure	92	74.2	74.2
	Total	124	100.0	100.0

Table 5.41 revealed that most of the organizations had encountered internal employee vandalism (51.6%), theft of customer data (37.9%) and stolen computers or laptops (30.6%). Other security-related incidents included: denial of service attack (16.1%), website vandalism (10.5%) and unspecified incidents (1.6%). Only 6.5% of organizations reported that no security risks had been encountered. It was also observed that 34.7% of organizations expressed uncertainty regarding the nature of the security risk encountered.

Organizations face both internal and external security threats, each capable of causing significant damage to an organization. Examples of security threats include: website hacking, password stealing, computer viruses, unauthorized remote access, spam e-mail, pharming, phishing, spyware, malware, innate web vulnerabilities and online fraud (Kendrick 2010).

**Table 5.41 Other information security risks faced in organizations**

<b>Which of the following other computer security risks has your organization ever been exposed to? (please choose all that apply) (N=124)</b>		
	<b>Response Percent</b>	<b>Response Count</b>
Denial of service attack	16.1%	20
Internal employee vandalism	51.6%	64
Theft of customer/citizen data	37.9%	47
Stolen Computers/ laptops	30.6%	38
Website Vandalism	10.5%	13
No Risks	6.5%	8
Not Sure	34.7%	43
Other	1.6%	2
<b>Total</b>		<b>124</b>

It is likely that the incidence for viruses is reasonably accurate because the symptoms

are usually identifiable and anti-virus software can confirm infection. Attacks on websites are also detectable but only if website is monitored, so a much higher level of uncertainty exists. It is quite probable that the actual incidence is higher than reported. Attacks on information systems will go undetected if data is only copied. Attacks which result in damage may be misdiagnosed as bugs, so the unsure rating is so high and the real incidence of attack may be much higher than reported.

Another significant result is that the level of uncertainty indicates that these events are not being monitored.

#### 5.4.2.1 *Culture threat*

This section discusses some other risks that can be introduced as a cultural threat such as illegal tribal connections for information disclosure or issues pertaining Saudi women ID.

Table 5.42 shows that the majority of respondents (83.9%) believed that tribal societies pose a risk in terms of information security and privacy, with 55.2% expressing agreement and 28.7% showing strong agreement. On the other hand, 14.2% indicated disagreement and 1.9% showed strong disagreement with this statement. Meanwhile, 15.3% of respondents opted not to respond since they believe the question is not applicable to them. Tribalism in Saudi Arabia is known to permeate social, economic and political aspects of society, even in modern times. Hence, the question of loyalty between the organization and an individual's tribal affiliation needs to be seriously considered (Champion 2003).

**Table 5.42 Information security and privacy risks involving tribal societies in Saudi Arabia**

<b>Saudi Arabia has tribe societies, those societies can be a risk factor for information security and privacy especially with abuse or publishing incidents, do you think this risk is effective (N=124)</b>				
		Frequency	Percent	Actual Percent
Valid	Strongly Disagree	2	1.6	1.9
	Disagree	15	12.1	14.2
	Agree	58	46.8	55.2
	Strongly Agree	30	24.2	28.7
	N/A	19	15.3	
Total		124	100.0	105

Table 5.43 revealed that the majority of respondents (93.6%) expressed their agreement

(46.3%) and strong agreement (47.3%) that people can illegally acquire information by the use of tribal connections. Only 5.5% of the respondents showed disagreement and 0.9% expressed strong disagreement with this concept. In modern day Saudi Arabia, tribalism based on authority, stability, social rituals and commitment have heightened the status of tribal connections as a risk factor for information security issues. This stems from the tendency of employees to respect authority and strictly follow what the tribe tells them to do. Hence, the loyalty of an employee to an organization becomes questionable (Ali 2009).

**Table 5.43 Information security risks in terms of illegal acquisition of information utilizing tribal connections**

<b>Tribe society's people can get some information illegally using their tribe's connections (N=124)</b>				
		Frequency	Percent	Actual Percent
Valid	Strongly Disagree	1	0.8	0.9
	Disagree	6	4.8	5.5
	Agree	51	41.1	46.3
	Strongly Agree	52	41.9	47.3
	N/A	14	11.3	
	Total	124	100.0	110

Table 5.44 shows that majority of respondents (90%) indicated their agreement (43.6%) and strong agreement (46.4%) that the practice of hiring unqualified relatives in the organization occurs. Only 8.2% of the respondents showed disagreement and 1.8% expressed strong disagreement that this happens. In Saudi Arabian society, the concept of loyalty is very much evident, and it diminishes as one's relationship goes farther from the family. Hence, it can be said that loyalty has different levels and loyalty is strongest within the family, followed by in the clan, tribe and nation. While it may be frowned upon in the West, the practice of hiring relatives in the organization regardless of qualification is a common business practice in Saudi Arabia (Bowen 2008).

**Table 5.44 Practice of hiring unqualified relatives**

<b>In tribe society, people sometimes use their authority to employee their relative if they do not have related qualifications for the job (N=124)</b>				
		Frequency	Percent	Actual Percent
Valid	Strongly Disagree	2	1.6	1.8
	Disagree	9	7.3	8.2
	Agree	48	38.7	43.6
	Strongly Agree	51	41.1	46.4
	N/A	14	11.3	
	Total	124	100.0	110

Table 5.45 reveals that 71.7% of respondents' believed that there was an information security risk associated with women wearing veils (49.1% agreement, 22.6% strong agreement). On the other hand, some respondents showed disagreement (19.8%) and strong disagreement (8.5%) with this causing information security risk. The wearing of veils by women in Saudi Arabia has its roots in Islamic faith, requiring women to cover themselves with a face veil with the exception of the eyes and hands (Bowen 2008).

**Table 5.45 Information security risk in relation to women wearing veils**

<b>In Saudi Arabia women wear the veil which hide women identity and that can make it very hard to track their incidents for information, do you think this risk is affective (N=124)</b>				
		Frequency	Percent	Actual Percent
Valid	Strongly Disagree	9	7.3	8.5
	Disagree	21	16.9	19.8
	Agree	52	41.9	49.1
	Strongly Agree	24	19.4	22.6
	N/A	18	14.5	
	Total	124	100.0	106

Table 5.46 showed that most of the respondents either agreed (47.6%) agreed or strongly agreed (27.6%) that there were possible risks created by not having a picture on ID cards issued to women in Saudi Arabia. However, some respondents expressed their disagreement (18.1%) and strong disagreement (6.7%). Traditionally, women are not issued with ID cards and typically women are only listed as dependents on their father's or husband's ID card. However, the government has now started issuing ID cards to women. To qualify, a woman must be at least 18 years old and have written consent from her guardian. If employed, a letter from her employer is also required (The Saudi Ministry of Interior 2012). However, some women who are listed on their guradian's card do not have photo ID. The ID card issued features a picture of the cardholder to

deter forgeries and fraud (BBC 2001).

**Table 5.46 Information security risk in relation to lack of picture on identification cards used by Saudi Arabian women**

<b>Women in Saudi Arabia can use the other women ID because there is no matched picture which may cause serious problem (N=124)</b>				
		Frequency	Percent	Actual Percent
Valid	Strongly Disagree	7	5.6	6.7
	Disagree	19	15.3	18.1
	Agree	50	40.3	47.6
	Strongly Agree	29	23.4	27.6
	N/A	19	15.3	
	Total	124	100.0	105

Table 5.47 shows that the majority of respondents agreed (61.8%) or strongly agreed (27.3%) that, in some Saudi Arabian tribal cultures, people refuse to allow women to be issued ID cards with pictures. On the other hand, 10% of the respondents showed disagreement and 0.9% showed strong disagreement. Despite the government's move to issue ID cards to women, conservative citizens argue that the issuance of ID cards with picture violates veil and social customs (BBC 2001).

**Table 5.47 Refusing permission to issue picture identification cards to women in Saudi Arabia**

<b>In some of Saudi Arabia tribe's culture, people refused to give permission for their women to have ID with picture (N=124)</b>				
		Frequency	Percent	Actual Percent
Valid	Strongly Disagree	1	0.8	0.9
	Disagree	11	8.9	10.0
	Agree	68	54.8	61.8
	Strongly Agree	30	24.2	27.3
	N/A	14	11.3	
	Total	124	100.0	110

This section has shown us that survey respondents believed that Saudi culture has a high impact in some issues which could be marked as information security threats. It showed high scores of illegal tribal connections for information discloser and for using authority to employee non-qualified people. Also, the section has shown a high score regarding the weaknesses of women's ID cards. This sort of risk is unusual and may be not exist in many countries such as western countries; however the results have shown that in Saudi Arabia culture it does.

To address some of the information security practice problems that have been identified, we need to find the best mechanisms that can be used to improve the information security practices in the organization. Section 5.5 indicates some of questions that related to information security standards and policies implementation challenges and the most efficient methods that can be used to enhance the information security practices in organizations.

### **5.5 Promotion preferences**

From the data presented so far, there is a clear need to increase the level of information security practice. Increasing the level of practices among organizations can reduce the risks and increase the efficiency of information security systems. This final section relates to the challenges that could affect information security standards and policy implementation in an organization and the mechanisms by which such practices and awareness could be raised.

Table 5.48 shows that the respondents considered the challenges to the application of information security standards in the following order: shortage of qualified information security personnel (91.1%); hard to understand standards written in a language other than Arabic (47.6%); difficulty in applying international standards (43.5%); and insufficient budget (32.3%). However, 5.6% of respondents expressed uncertainty about the key challenge for their organization. Two respondents provided responses other than those mentioned above. The implementation of information security standards in the organization is restricted by challenges of human, organizational and technical natures (Werlinger et al. 2007).

**Table 5.48 Challenges of applying information security standards in organizations**

<b>What do you think are the challenges of applying information security standards in your organization? (Please tick the below options, whichever is applicable) (N=124)</b>		
	<b>Response Percent</b>	<b>Response Count</b>
Do not have the budget to do so	32.3%	40
Standards in non-Arabic are hard to understand	47.6%	59
Shortage of qualified people in information security	91.1%	113
International standards are difficult to apply in general	43.5%	54
Not sure	5.6%	7
Other	1.6%	2
<b>Total</b>		<b>124</b>



Table 5.49 reveals that the majority of the respondents (79%) indicated that high fees are the top hindrance faced when acquiring information security certifications. In addition, the respondents had issues concerning the following: unclear career roadmap (63.7%); lack of guidance in career progression (57.3%); insufficient study time (55.6%); lack of information regarding certification (19.4%); and insufficient exam guidance (12.1%). 20.4% of respondents provided other obstacles while 1.6% of respondents responded non-applicability. Despite such obstacles, a growing number of organizations are beginning to realize the value of information security. Budgets for additional training and certifications have been increasing in the past few years (Ayoub 2011).

**Table 5.49 Obstacles faced in acquiring certifications in information security**

<b>What are the obstacles you have faced/are facing in acquiring certifications in Information Security? (Please tick the below options, whichever is applicable) (N=124)</b>		
	<b>Response Percent</b>	<b>Response Count</b>
High fee amount	79.0%	98
Insufficient study time	55.6%	69
Insufficient exam guidance	12.1%	15
Unable to obtain information regarding certification	19.4%	24
Unclear career roadmap	63.7%	79
Lack of guidance on career progression	57.3%	71
N/A	1.6%	2
Other	2.4%	3
<b>Total</b>		<b>124</b>

Table 5.50 indicates that the majority of respondents would be encouraged to gain an information security certification if they had the opportunity for study leave (76.6%). Respondents also believed a certification fund as part of their contract (40.3%) or separately (19.4%), and payment of any exam fee with a bonded contract (9.7%) or without a contract (8.1%) would encourage them to gain further certification. Meanwhile, 1.6% suggested other benefits would motivate them and 6.5% replied non-applicability. The acquisition of additional information security certification has started to gain momentum since an individual possessing the required information security certifications is perceived as someone who has the knowledge, skills and abilities to protect the organization from information security threats (Ayoub 2011).

**Table 5.50 Benefits that would motivate respondents to acquire additional certification in information security**

<b>What kind of benefit from your organization would interest you to acquire additional certification in Information Security? (Please tick the below options, whichever is applicable) (N=124)</b>		
	<b>Response Percent</b>	<b>Response Count</b>
Certification Fund (Course/Training Fee & Exam Fee) without contract	19.4%	24
Certification Fund (Course/Training Fee & Exam Fee) with contract	40.3%	50
Exam Fee allocation without contract	8.1%	10
Exam Fee with bonded contract	9.7%	12
Study leave	76.6%	95
N/A	6.5%	8
Other	1.6%	2
		<b>124</b>

Table 5.51 shows the promotions that respondents believed would interest them in acquiring additional information security certification. The majority of respondents preferred an exam fee discount (79.8%). Respondents were also interested by product discounts (62.1%), networking events (56.5%) and IT security conference benefits (51.6%). 2.4% of respondents listed other promotions. A 2011 study revealed that information security managers preferred hiring professionals with information security certifications due to better competence, regulatory requirements and quality of work (Ayoub 2011).

**Table 5.51 Promotions that would motivate respondents to acquire additional certification in information security**

<b>What kind of promotions would interest you to acquire additional certification in Information Security? (Please tick the below options, whichever is applicable) (N=124)</b>		
	<b>Response Percent</b>	<b>Response Count</b>
Exam fee discount	79.8%	99
IT Security Conference benefits	51.6%	64
Networking event benefits	56.5%	70
Product discount benefits	62.1%	77
Other	2.4%	3
<b>Total</b>		<b>124</b>

## 5.6 Chi-Square Relationship Tests

Chi-square test was conducted to check the significance relationship between the nature of organizations and some InfoSec practices. A copy of the chi-square test tables is presented in Appendix F. Table 5.52 shows the statistically significant difference between:

**Table 5.52 Nature of organizations vs InfoSec practices Chi-Square test**

InfoSec Practices	Nature of Organization	InfoSec Practices	Nature of Organization
Information security law	0.787	Vulnerability assessment	0.174
Information security standards	0.354	Password setting	0.000
Information security policy	0.115	Two-factor authentication	0.659
Information security policy enforcement	0.229	Firewall security	0.039
Risk assessment process	0.148	Wireless access restriction	0.022
Accounts management	0.590	Internet access restriction	0.089
Data backup	0.745	Anti-virus strength	0.001
Security incidents reporting	0.223	Instruction detection strength	0.096
Software update	0.486	Encrypt technique	0.174
Information security training	0.089	Server room physical security	0.067
		Input devices restriction	0.250

1. A statistically significant relationship exists between the nature of the organization and password setting, p-value  $0.000 < 0.05$ . The proportion of organizations that have good and very good levels of password setting in the government sector is 18.6%. The proportion in the private sector is 37.2% and for non-profit organizations it is 16.6%. All sectors have poor password setting practice.
2. A statistically significant relationship exists between the nature of the organization and firewall security, p-value  $0.039 < 0.05$ . The proportion of organizations that have good and very good levels of firewall security in the government sector is 30.6%, while the proportion of the private sector is 39.9% and for non-profit organizations it is 16.6%. All sectors have poor firewall security.
3. A statistically significant relationship exists between the nature of the organization and wireless access restriction, p-value  $0.022 < 0.05$ . The proportion of organizations that have good and very good levels of wireless access restrictions in the

government sector is 20%; the private sector reports 37.2% and the non-profit organization reports 33.3%. All sectors have poor wireless access restriction.

4. A statistically significant relationship exists between the nature of the organization and anti-virus strength, p-value  $0.001 < 0.05$ . The proportion of organizations that have good and very good anti-virus is 42.6% in the government sector, 48.8% in the private sector and 16.6% for the non-profit organizations. All sectors have reasonably poor anti-virus systems.

The results discussed above were unexpected. Given that all organizations should have an awareness of these issues, all practices with less than 50% response/awareness were mentioned above.

In addition, chi-square test was conducted to check the significance relationship between the organization sector and some InfoSec practices. A copy of the chi-square test tables is presented in Appendix F. Table 5.53 shows statistically significant differences between:

**Table 5.53 Organization sectors vs InfoSec practices Chi-Square test**

<b>InfoSec Practices</b>	<b>Organization Sector</b>	<b>InfoSec Practices</b>	<b>Organization Sector</b>
Information security law	0.003	Password setting	0.003
Information security standards	0.014	Two-factor authentication	0.000
Information security policy	0.007	Firewall security	0.002
Information security policy enforcement	0.113	Wireless access restriction	0.000
Risk assessment process	0.000	Internet access restriction	0.042
Accounts management	0.083	Anti-virus strength	0.003
Data backup	0.007	Intrusion detection strength	0.036
Security incidents reporting	0.000	Encrypt technique	0.010
Software update	0.020	Server room physical security	0.025
Information security training	0.000	Input devices restriction	0.052
Vulnerability assessment	0.011		

1. A statistically significant relationship exists between organization sector and the

application of any data protection or information security law,  $p\text{-value } 0.003 < 0.05$ . The proportion of organizations that do not have data protection or information security law is extremely low (under 50%) for most sectors except banking and finance, and information and communication sectors (over 72%).

2. A statistically significant relationship exists between organization sector and the application of information security standards,  $p\text{-value } 0.014 < 0.05$ . The proportion of organizations that do not have information security standards is extremely low (under 50%) for most sectors except bank and finance, information and communication and foreign affair sectors (over 90%).
3. A statistically significant relationship exists between organization sector and the application of information security policy,  $p\text{-value } 0.007 < 0.05$ . The proportion of organizations that do not have an information security policy is extremely low (under 50%) for most sectors except bank and finance, information and communication and foreign affair sectors (over 83%).
4. A statistically significant relationship exists between organization sector and risk assessment process,  $p\text{-value } 0.000 < 0.05$ . The proportion of organizations that do not have a risk assessment process is extremely low (under 50%) for most sectors except bank and finance, information and communication and foreign affair sectors (over 83%).
5. A statistically significant relationship exists between organization sector and data backup,  $p\text{-value } 0.007 < 0.05$ . The proportion of organizations that complete data backup is high in some sectors and slightly low in others. Banking and finance, information and communication, health services, transportation, foreign affairs, labour, tourism and media sectors have over 75% while other sectors are under 66%.
6. A statistically significant relationship exists between organization sector and security incident reporting,  $p\text{-value } 0.000 < 0.05$ . The proportion of organizations that do have a policy about reporting information security incidents is extremely low among most sectors (under 50%) except the bank and finance, information and communication and foreign affair sectors, each of which commonly have incident reporting policies (over 83%).
7. A statistically significant relationship exists between organization sector and

software update, p-value  $0.020 < 0.05$ . Many organizational sectors indicated a high level (over 50%) of respondents who never complete software updates. This was not the case in the bank and finance, information and communication, health services, food and agriculture, transportation, water, foreign affair, tourism and media sectors.

8. A statistically significant relationship exists between organization sector and information security training, p-value  $0.000 < 0.05$ . The organization sectors that do training for their employees are bank and finance, information and communication and foreign affair sectors (over 83%) while the other sector have a low training percentage (under 49%).
9. A statistically significant relationship exists between organization sector and vulnerability assessment, p-value  $0.011 < 0.05$ . The proportion of organization sectors that have good and very good vulnerability assessments is low. All sectors except two have less than 51% good practice. These other two sectors, the bank and finance and information and communication sectors, recorded over 81% of good practices.
10. A statistically significant relationship exists between organization sector and password setting, p-value  $0.003 < 0.05$ . The proportion of organization sectors that has good and very good password setting practices is low. All sectors have less than 50% of good practice except two sectors, bank and finance and information and communication, which have over 80% of good practices.
11. A significant relationship exists between organization sector and two-factor authentication, p-value  $0.000 < 0.05$ . Bank and finance, information and communication, foreign affair and media sectors use two-factor authentication (over 79%), while other sectors have less than 50% of organizations using a two-factor authentication technique.
12. A statistically significant relationship exists between organization sector and firewall security, p-value  $0.002 < 0.05$ . The proportion of organization sectors that have good and very good firewall security is low. All sectors have less than 50% of good practice, except media (60%), and bank and the finance, information and communication, foreign affair and tourism sectors which have over 75% of good practices.

13. A statistically significant relationship exists between organization sector and wireless access restriction,  $p\text{-value } 0.000 < 0.05$ . The proportion of organization sectors that have good and very good wireless access restriction is low. All sectors have less than 50% of good practice except information and communication sector (66%), bank and finance and foreign affairs sectors, which have over 81% of good practices.
14. A statistically significant relationship exists between organization sector and Internet access restriction,  $p\text{-value } 0.042 < 0.05$ . The proportion of organization sectors that have good and very good Internet access restriction practices is low. All except three sectors have less than 50% of good practice; the exceptions of banking and finance, information and communication and foreign affairs have over 80% good practice.
15. A statistically significant relationship exists between organization sector and anti-virus strength,  $p\text{-value } 0.003 < 0.05$ . The proportion of organization sectors that have good and very good strength anti-virus systems is low. All sectors have less than 51% of good practice except the media sector (with 60%) and three other sectors of bank and finance, information and communication and foreign affairs (all over 90%).
16. A statistically significant relationship exists between organization sector and intrusion detection strength,  $p\text{-value } 0.036 < 0.05$ . The proportion of organization sectors that have good and very good intrusion detection systems is low. All sectors have less than 50% of respondents with good systems except in three sectors, bank and finance, information and communication and foreign affairs, each of which have over 81% of good intrusion detection system.
17. A statistically significant relationship exists between organization sector and the use of encryption technique,  $p\text{-value } 0.010 < 0.05$ . The proportion of organization sectors that have good and very good encryption technique systems is low. All sectors have less than 50% of respondent organizations with good systems, except three sectors, bank and finance, information and communication and foreign affairs, in which over 66% reported good encryption technique systems.
18. A statistically significant relationship exists between organization sector and server

room physical security, p-value  $0.025 < 0.05$ . The proportion of organization sectors that have good and very good server room physical security is low. All sectors reported less than 50% of respondents having good systems except three sectors, bank and finance, information and communication and foreign affair, each of which reported over 80% as having good server room physical security.

19. A statistically significant relationship exists between organization sector and input devices restriction, p-value  $0.052 < 0.05$ . The proportion of organization sectors that have good and very good input device restrictions is low. All sectors have less than 51% of good practice except two sectors, bank and finance and foreign affairs, where over 63% reported good input device restrictions.

It was unexpected that the majority of organizations in the majority of sectors had low InfoSec practices. The sectors that were consistently the exception to this were bank and finance, information and communication, and foreign affairs. Each of these three sectors reported good or very good InfoSec practices in most organizations. It is possible that these three sectors had better InfoSec practices than others because they have very sensitive information, have experience with information threats and have well-educated employees. While it was expected that InfoSec practices across all sectors would be at least 50%, the practices in all other sectors practices were found to occur in less than 50% of organizations.

Chi-square tests were conducted to determine the significance of the relationship between organization size and InfoSec practices. Detailed analysis supporting the chi-square test tables shown below is presented in Appendix F. Table 5.54 shows that there is a statistically significant difference between:



**Table 5.54 Organization size vs InfoSec practices Chi-Square test**

<b>InfoSec Practices</b>	<b>Organization Size</b>	<b>InfoSec Practices</b>	<b>Organization Size</b>
Information security law	0.072	Password setting	0.003
Information security standards	0.000	Two-factor authentication	0.000
Information security policy	0.000	Firewall security	0.000
Information security policy enforcement	0.000	Wireless access restriction	0.000
Risk assessment process	0.000	Internet access restriction	0.072
Accounts management	0.011	Anti-virus strength	0.000
Data backup	0.000	Instruction detection strength	0.001
Security incidents reporting	0.000	Encrypt technique	0.017
Software update	0.004	Server room physical security	0.014
Information security training	0.000	Input devices restriction	0.017
Vulnerability assessment	0.000		

1. A statistically significant relationship exists between organization size and the application of any information security standards, p-value  $0.000 < 0.05$ . When considered by organization size, results indicate that less than 36% of all participants' organizations apply any information security standards; the exception is very large organizations (more than 1000 employees), of which 59% use information security standards.
2. A statistically significant relationship exists between organization size and the application of any information security policy, p-value  $0.000 < 0.05$ . When considered by organization size, results indicate that less than 37% of all participants' organizations apply any information security policy; the exception is very large organizations (more than 1000 employees), of which 68% use an information security policy.
3. A statistically significant relationship exists between organization size and information security policy enforcement, p-value  $0.000 < 0.05$ . When considered by organization size, results indicate that information security policy enforcement policy ranges from 47% to 76%.

4. A statistically significant relationship exists between organization size and risk assessment process,  $p\text{-value } 0.000 < 0.05$ . When considered by organization size, results indicate that less than 36.3% of all participants' organizations use a risk assessment process; the exception is very large organizations (more than 1000 employees), of which 63.6% have a risk assessment process.
5. A statistically significant relationship exists between organization size and account management,  $p\text{-value } 0.011 < 0.05$ . When considered by organization size, results indicate that less than 59% use account management; exceptions are large (500-100 employees) and very large organizations (more than 1000 employees) which reported over 81% using account management.
6. A statistically significant relationship exists between organization size and data backup,  $p\text{-value } 0.000 < 0.05$ . When considered by organization size, results indicate that less than 58% use data backup; exceptions are large (500-100 employees) and very large organizations (more than 1000 employees) which reported over 82% using data backup.
7. A statistically significant relationship exists between organization size and incident reporting,  $p\text{-value } 0.000 < 0.05$ . When considered by organization size, results indicate that less than 37% have an incident reporting system; the exception is very large organizations (more than 1000 employees) which reported over 61% using incident reporting.
8. A statistically significant relationship exists between organization size and software update,  $p\text{-value } 0.004 < 0.05$ . When considered by organization size, results indicate that the proportion of participants' organizations that never do software updates is high across medium and small organizations (48% - 53%), while very large organizations (more than 1000 employees) reported that 19% never respond to software updates, indicating that 81% of very large organizations do software updates at least annually.
9. A statistically significant relationship exists between organization size and information security training,  $p\text{-value } 0.000 < 0.05$ . When considered by organization size, results indicate that the proportion of participants' organizations that provide training for employees is 56% for large and 45% for very large organizations, while

less than 19% of other organizations provided training.

10. A statistically significant relationship exists between organization size and vulnerability assessment,  $p\text{-value } 0.000 < 0.05$ . 43% of very large organizations reported good or very good vulnerability assessments, while other organizations reported less than 28%.
11. A statistically significant relationship exists between organization size and password setting,  $p\text{-value } 0.003 < 0.05$ . 47.7% of very large organizations have good and very good password setting practices while other organizations reported less than 37%.
12. A statistically significant relationship exists between organization size and two-factor authentication,  $p\text{-value } 0.000 < 0.05$ . 61.3% of very large organizations implement two-factor authentication while less than 37% of other organization sizes use it.
13. A statistically significant relationship exists between organization size and firewall security,  $p\text{-value } 0.000 < 0.05$ . 61.3% of very large organizations have good or very good firewall security practices while other organizations have less than 46%.
14. A statistically significant relationship exists between organization size and wireless access restriction,  $p\text{-value } 0.000 < 0.05$ . Only 52.2% of very large organizations have good or very good wireless access restrictions; other organizations reported less than 18.2%.
15. A statistically significant relationship exists between organization size and anti-virus strength,  $p\text{-value } 0.000 < 0.05$ . 90.9% of large organizations and 68.1% of very large organizations have good or very good anti-virus systems; less than 24.1% of other organizations reported this.
16. A statistically significant relationship exists between organization size and intrusion detection strength,  $p\text{-value } 0.001 < 0.05$ . All respondents' organizations have a low level of intrusion detection systems. Only 47.7% of very large organizations reported good or very good intrusion detection; other organizations have less than 36.3%.
17. A statistically significant relationship exists between organization size and the use of encryption techniques,  $p\text{-value } 0.017 < 0.05$ . All respondents' organizations have a

very low level of encryption technique usage. Only 36% of very large organizations reported good or very good encryption techniques, while less than 10% of other organizations had at least good intrusion detection.

18. A statistically significant relationship exists between organization size and server room physical security,  $p\text{-value } 0.014 < 0.05$ . 81.8% of large organizations and 77.2% of very large organizations have good or very good server room physical security; less than 49% of other sized organizations have this.

19. A statistically significant relationship exists between organization size and input device restrictions,  $p\text{-value } 0.017 < 0.05$ . All respondents' organizations have low input device restrictions. Only 36% of very large organizations have good or very good input device restrictions; other sized organizations reported having this in less than 18.2% of cases.

When considered by organization size, the majority of organization sizes reported low InfoSec practices across organizations. Exceptions were very large and large organization, and only in some practices. This was unexpected. This indicates a low implementation of InfoSec practices even with large organizations. Lack of training and low information security budgets may be a reason for such poor practices.

## **5.7 Conclusion**

A total of 124 respondents from a range of organizations were involved in the present study. The majority of organizations were public sector organizations from the education sector employing over 1000 employees and in operation for more than three decades. The majority of the organizations had IT departments and IT budget. However, the majority of IT departments do not have a specific budget for information security.

29% organizations surveyed applied data protection laws. The majority of the respondents did not feel comfortable with existing data protection laws or believe that the laws were comprehensive, appropriate or powerful. In relation to the issue of information security standards, the majority of the organizations (65.3%) said they did not apply any information security standards and this majority is undecided as to whether to apply information security standards in the future. Of the organizations who adhered to information security standards, 29.8% felt their information was somehow

secured, despite the majority of these organizations (54.8%) not having anyone responsible for ensuring compliance with the standards. 61.3% of the organizations did not have an information security policy in place. The majority of the organizations (66.9%) did not have a risk assessment process or a security incident reporting plan.

Considering information assurance issues, most of the organizations (65.3%) had procedures and regulations for account creation and management and (63.7%) for data backup and recovery. For information assurance tool or measures, performed badly in vulnerability assessments (60.5% across very poor, poor or not existent), and had unsatisfactory security measures with respect to password setting (57.3% across very poor, poor or not-existent). The majority of the organizations (66.1%) did not implement two-factor authentication; 48.4% had very poor, poor or not-existent Internet access restrictions; 56.4% had very poor, poor or non-existent organizational policies on restricting access to specific websites, and 79.9% of respondents' organizations updated their operating systems and software yearly or never. 57.3% had very poor, poor or no intrusion detection systems; 63.8% did not utilize encryption technology to protect their data; 63.7% had very poor, poor or no restrictions on the use of removable computer devices, and 70.2% did not offer special information security training to employees. However, the majority of the organizations (62.9%) had neutral, good or very good firewall systems; 78.2% had neutral, good or very good anti-virus software, and 74.2% of respondent's organizations had physically secure server room capabilities.

For information security risk issues, the majority of organizations (56.5%) experienced computer downtime caused by a computer virus infecting the system and had encountered internal employee vandalism (51.6%). The majority of the respondents (74.2%) were unsure whether their websites or information systems had been attacked by hackers. The majority of respondents (71%) also believed that tribal societies pose a risk in terms of information security and privacy and that tribal connections influence the illegal acquisition of information (83%). The majority of respondents (79.8%) believed that the practice of hiring unqualified relatives was prevalent and that there are information security risks related to women wearing veils and not having picture ID cards (61.3%). An overwhelming, the majority of the respondents (79%) agreed and strongly agreed on the issue of refusing permission to issue ID cards with pictures to

women.

Finally as to incentive preferences, the main challenges perceived by the respondents in applying information security standards were shortages of qualified people in information security (91.1%), standards that were not written in Arabic were hard to understand (47.6%) and international standards were difficult to apply in general (43.5%). The main obstacles preventing the respondents' acquisition of information security certification were high fee amount (79%), unclear career roadmap (63.7%), lack of guidance on career progression (57.3%) and insufficient study time (55.6%). Thus, majority of the respondents believed that a study leave benefit (76.6%) and examination fee discounts (79.8%) would enhance interest in obtaining information security certifications.

The results of this study have shown that a problem exists within the IT practices of many organizations in Saudi Arabia. The next chapter of this research will provide suggested solutions for the existing weaknesses and recommendations to increase information security awareness and practices among the public and organizations in Saudi Arabia.

## ***Chapter 6 Summarised Findings Directly Related to Model***

The previous chapters have identified that information security awareness and practice in Saudi Arabia are extremely low. Thus, the purpose of this chapter is to discuss the findings about information security awareness and practices among the public and in organizations in Saudi Arabia and to present recommendations for improvements in both information security awareness and related practices. The next section of this chapter provides appropriate solutions for the existing weaknesses and recommendations to increase the information security awareness and practices among the public and organizations in Saudi Arabia.

### ***6.1 Research contributions and recommendations***

Based on the findings of this study, information security and systems in Saudi Arabia require strong infrastructure and practices to reduce the current risks and to prevent further information threats. To address these problems, Saudi Arabia needs to acknowledge the significant impact of culture practice on information systems. This section provides some suggested solutions that may assist in building and providing greater protection for information systems in Saudi Arabia. A new model of Information Security Cultural Adaptation Process (InfoSec CAP) will be introduced. This model proposes an information security infrastructure and efficient solutions that include culturally relevant components.

#### ***6.1.1 The Proposed InfoSec CAP Model***

The InfoSec CAP model will assist to draw appropriate relationships between all the involved elements. This will allow the achievement of the research objective of proposing guidelines to address these weaknesses and their causes by providing appropriate solutions. This information security model does not replace the many sources of security program best practice. It does, however, provide a view of information security programs that is highly relevant and appropriate for countries that have a weak infrastructure and culture complexities that impact on information security.

A critical piece of the model that differentiates it from many others is the importance it places on organizational culture. Creating an intentional security culture is a primary

objective for the model. Some countries with a high culture like Saudi Arabia need thorough consideration of the culture aspect in the model phases to ensure the establishment of appropriateness and to provide maximum benefits of the model. For example, women in Saudi Arabia wear a veil which can restrict facial identification and they may not have picture ID. In this case, the cultural impact should be well studied by educational, cultural and IT specialists. This allows the design and implementation of appropriate solutions that can lead to best practice without clashing with Saudi culture.

The new InfoSec CAP model has been designed based on the findings of the research results. It will help embed the identified concepts in information security practice globally.

#### *6.1.1.1 Structure of InfoSec CAP model*

Waterfall model finds its application in mega enterprises that have converted their operations onto information based digital technology networks. The name is assigned based on the water fall like structure with different phases in downward direction to one another. Toyota Motors is one of the examples of the world class companies that have had its history of using waterfall model for software applications and data handling.

One of the basic features and functions attributed to this model include the large scaled domain of this model. It ensures each activity and each sub component of the major project is covered under the basic guidelines set forth in the waterfall model (Saleh 2009).

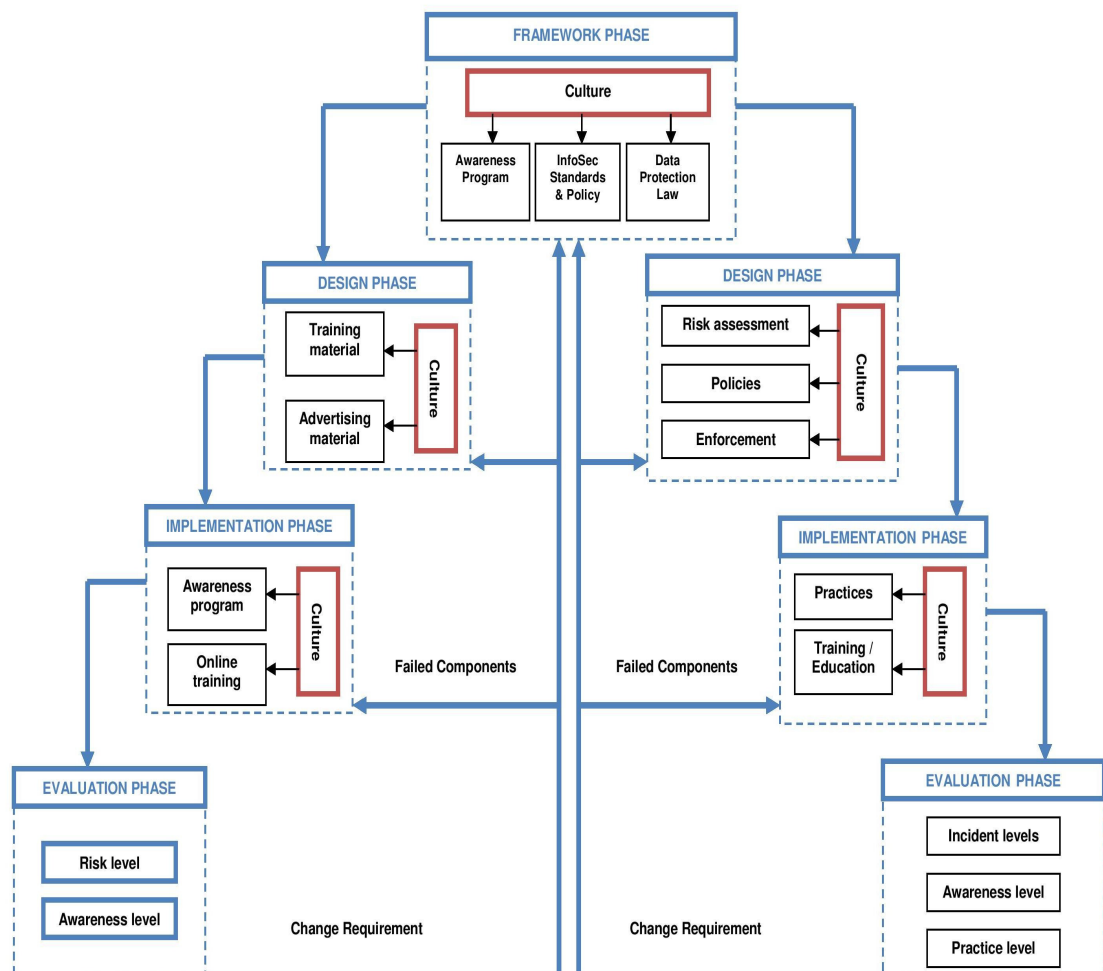
Flexibility of operations is another added function and feature attributed to this particular model. It is also believed to be relatively flexible in working and handling towards the administrative management. Time allotment for each function and activity based on the different activities within the project.

Coherence is ensured and repetition avoiding is another advantage of waterfall model. This feature is reflected in the pattern in which the different stages are aligned and with activity starting from top and leading on to the last stage. Other advantages of this model include its broader applicability to the field of manufacturing and construction as a whole.



Petersen et al. have assessed the validity of this theory with regard to the scale of organization. They have through their research and findings revealed and established that this model is efficiently suited to the large scale organizations.

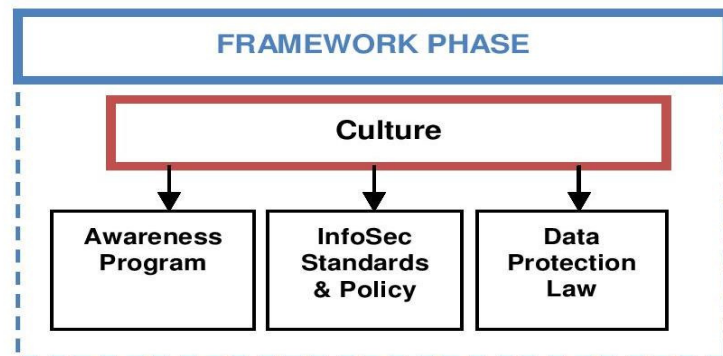
The model consists of two main parts. The first part has been designed for ISA among the public and the second part for InfoSec among organizations. As illustrated in Figure 6.1, the model is best viewed as a flexible, four-phase, waterfall-shaped structure linked together by dynamic interconnections. All aspects of each part in the model interact with each other. If any one part of the model is changed, not addressed or managed inappropriately, the equilibrium of the model is potentially at risk. The four phases of the model are framework, design, implementation and evaluation.



**Figure 6.1 InfoSec CAP Model for Cultural Adaptation Process**

#### 6.1.1.1.1 Framework Phase

The Framework Phase in the model consists of four main aspects which are culture that directly linked to data protection law, InfoSec standards & policy and awareness program. This phase has been designed to be used for the general public and organizations. Figure 6.2 shows the structure of the Framework Phase.



**Figure 6.2 Framework Phase Structure**

Some view information security solely as a technical discipline. While IT provides tools useful for protecting information, technology alone is not the solution. To protect information, organizations need to introduce data protection laws, information security policies and standards, procedures and awareness guidelines programs. This guidance establishes the direction for the information security program and expectations as to how information is to be used, shared, transmitted and destroyed. In many organizations, technology strategies, policies and processes are developed without consideration of the effectiveness of culture impacts. Information security programs that fail to consider how humans react to and use technology often do not deliver intended benefits. Information security programs need to take into account how the organization and its people, processes and technologies interact, and how organizational governance, culture, human factors and architectures support or hinder the ability of the organization to protect information and to manage risk.

While information security law and standards are important, the results showed an absence of data protection law in many organizations (71%). However, the majority of the respondents did not feel comfortable with data protection laws and did not believe

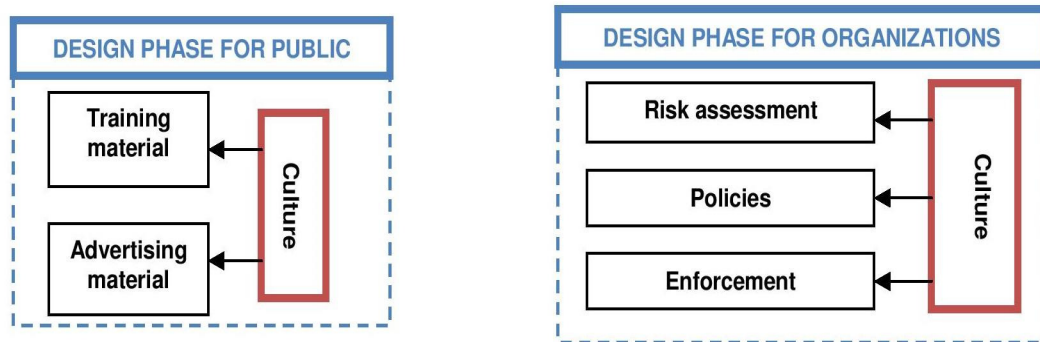
that the laws were comprehensive, appropriate or powerful. In addition, the majority of the organizations in the research findings (65.3%) did not apply any information security standards. Information security awareness among the general public was poor and showed shortages of information security awareness and physical security tools such as password practices, defence software, data backup or security incidents reports. From the results, it clear that Saudi society is missing some important foundations for information security like data protection law and information security standards and policy and awareness programs.

Currently, there exist some international data protection law and standards, however, some of them may not work well, especially when law and culture is different. To overcome these weaknesses, introducing appropriate data protection law and information security standards that are closely aligned to Saudi's culture and law is the best idea. To execute this phase, organizations such as the Ministries of Justice, Education, Interior and Communication and Information Technology Commission must be involved. They are responsible for establishing data protection law and information security standard that reflect Saudi culture. It is important that specific cultural directions be included, such as tribal impact.

This Framework Phase of the model is linked to the next phase which is the Design Phase. The outcomes of the Framework Phase will be used for the Design Phase. The Framework Phase uses feedback from the Implementation Phase and the Evaluation Phase to determine changes and improvements. The next section will present the second phase in the model which is Design Phase.

#### 6.1.1.1.2 Design Phase

The Design Phase in the model consists of two main parts. The first part has been designed for ISA among the general public and it has three main aspects: culture which is directly linked to training and advertising materials. The second part has been designed for InfoSec in organizations and it has four main aspects which are culture that directly linked to risk assessment, policies and enforcement. Figure 6.3 shows the structure of the Design Phase.



**Figure 6.3 Design Phase**

The research findings indicated that ISA among the general public is low, particularly in regard to practices such as password setting, backup and information threats awareness. To solve these weaknesses, culturally specific ISA programs should be designed and implemented. For examples, women in Saudi Arabia do not have as many options of training that are accessible by women in western counties. 75% of 412 respondents indicated that a web portal would be the most effective means of increasing their awareness. So, designing appropriate training and advertising materials to be accessed through the web portal will contribute to achieving the benefit of increased awareness and practice.

In addition, the research findings indicated that InfoSec policies in organizations are also low. It indicates that most of the organizations (61.3%) did not have an information security policy in place. Only 8.1% of those organizations, who had an InfoSec policy actually enforced it. 66.9% of respondent organizations did not have a risk assessment policy which is cornerstone of good InfoSec.

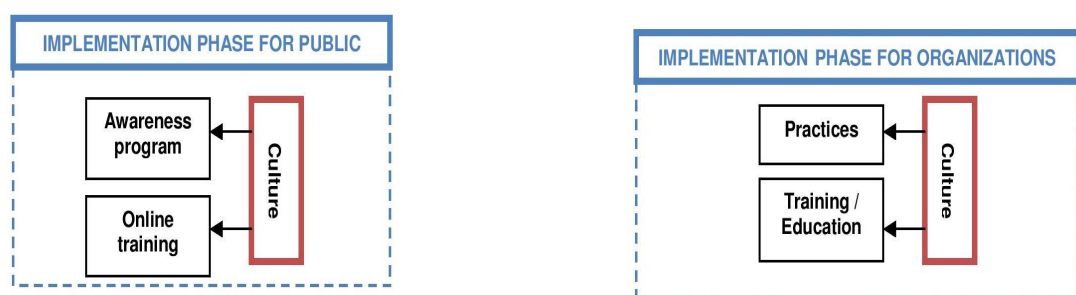
This survey uncovered some new perspectives on information security risks which were related to culture in Saudi Arabia. The majority of respondents (71%) believed that tribal societies pose a risk in terms of information security and privacy and that tribal connections influence the illegal acquisition of information (83%). Furthermore, the majority of respondents (79.8%) believed that the practice of hiring unqualified relatives was prevalent. This poses a significant risk if these unqualified family members have important roles in InfoSec in an organization. The study identified that there are

information security risks related to women wearing veils and not having picture ID cards (61.3%). In addition to this, some respondents did not want women to have a picture ID card. The majority of the respondents (79%) agreed and strongly agreed on the issue of refusing permission to issue ID cards with pictures to women. The outcome of these identified InfoSec cultural factors indicates that well-planned training and advertising materials for the general public, and risk assessment, policies and enforcement for InfoSec for organizations must be aligned with cultural expectations.

The Design Phase suggests a strong link between all four aspects to have maximum benefit. The outcomes of Design Phase can be used in the next phase. The Design Phase uses feedback from the Evaluation Phase to determine changes and improvements. The next section will present the last phase in the model which is Implementation Phase.

#### 6.1.1.1.3 Implementation Phase

In this phase all the implemented solutions will be introduced and executed. It consists of two main parts. The first part has been designed for ISA among the general public and it has three main aspects: culture, which is directly linked to an awareness program, and the online training. The second part has been designed for InfoSec in organizations and it has three main aspects: culture, which is directly linked to practices, and training/education. Figure 6.4 shows the structure of the Implementation phase.



**Figure 6.4 Implementation Phase**

In this phase, physical and procedural security should be used as a defence from threats. To protect information, people and organizations have to set up strong defences to protect their information assets. Physical and procedural security, such as vulnerability

assessments, password mechanisms, firewalls, anti-virus, anti-spy, anti-spam, software updates, intrusion detection and encryption can provide ongoing protection.

While physical and procedural security (including assurance tools or measures) are very important (Oliva 2004; Stallings & Brown 2008), the research findings indicated extremely low physical and procedural security practice among the general public and organizations in Saudi Arabia. The results have shown that the physical security practice among the general public is low. This includes techniques such as password strength, sharing of passwords, use of anti-threats software, software updates and data backup.

In addition, the findings indicated that physical and procedural security practices among Saudi Arabian organizations are also low. For example, 66.1% of Saudi respondent organizations did not implement two-factor authentication; 60.5% performed poorly on vulnerability assessments; 57.3% were rated poorly with respect to password security measures; 48.4% had poor Internet access restrictions; 56.4% had poor organizational policies for restricting access to specific websites; 79.9% rarely updated their operating systems and software; 57.3% had ineffective intrusion detection systems; 63.8% did not utilize encryption technology to protect their data, and 63.7% did not have effective restrictions on the use of removable computer devices. The majority of the organizations (33.1%) rated their firewall systems as good or very good, 43.5% had neutral, good or very good anti-virus software, and 56.5% of respondents' organizations had physically secure server room capabilities.

Countries with culture impact like Saudi Arabia require full consideration of their culture on their information security to develop an appropriate information security system with full benefits and protection. Designing and implementing appropriate tools and practices that do not create any conflict with the Saudi culture and privacy requirements is essential. An example of this is providing alternative techniques that can support the identification of women. Smart access cards and finger print readers are two such techniques. These solutions combine the privacy aspects of Saudi culture and the benefits of information security tools and practice.

However, physical and procedural security alone is not enough; to have maximum

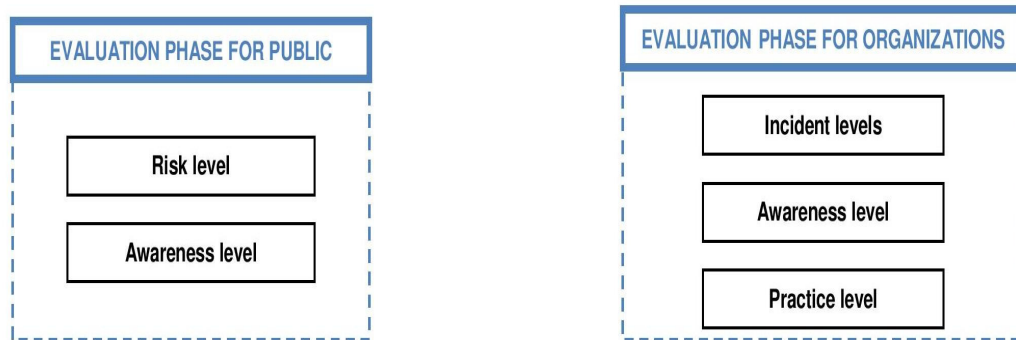
protection, all system users require education and ongoing training because information threats arise quickly. The research findings in Chapters 4 and 5 indicated that ISA among public and organizations is low. Also, the research result indicated that 70.2% of the respective organizations in this study did not offer special information security training to employees. IT department staff believe that a shortage of qualified people in information security and difficulty in applying international standards because the standards in non-Arabic are hard to understand, are obstacles to applying information security standards in their organizations.

To solve these weaknesses; providing good training and education about information security issues that suits the culture to raises the awareness level is also required. Governments and organizational management should provide all required awareness and training via the best available mechanism to increase information security awareness and practice among the general public and within organizations. The research findings indicated that online training is likely to be able to address the limitations imposed by the Saudi culture among the general public. In organizations, IT staff believes that ongoing training is important and seek to improve their knowledge by some suggested methods such as providing courses with career roadmap, study leave or course fee discounts.

The outcomes of Implementation Phase can be tested and evaluated in the next phase. The Implementation Phase uses feedback from the Evaluation Phase to determine changes and improvements. The next section will present the last phase in the model which is Evaluation Phase.

#### 6.1.1.1.4 Evaluation Phase

The Evaluation Phase in this model consists of two parts. The first part has been designed for ISA among general public and it has two main aspects which are evaluation for risk and awareness levels. The second part has been designed for InfoSec in organizations and it has three main aspects which are evaluation of incidents, awareness and practices levels. Figure 6.5 shows the evaluation phase structure.



**Figure 6.5 Evaluation Phase**

To achieve the objectives of this model, every outcome from these aspects is important. The evaluation tools are the tools required to measure the level of three aspects such as physical security software, information security incidents reports or data transmission monitoring software. Ongoing monitoring by a team of IT experts, educational specialists and legislation experts is essential to evaluate the outcomes that have been measured by evaluation tools. The needs of this integrated system are to control the risks either from global information risks or from cultural impact; to evaluate the information security awareness level among the general public and to evaluate the information security practice in the organizations.

Failed components are considered and ongoing feedback is provided for other phases to assist in reducing future failures and ensuring the quality of program outcomes. The model provides flexibility to make all the required changes which can then be applied in the Design and Implementation Phases, thereby reducing the errors and maximising the benefits of this program.

## **6.2 Conclusion**

This study has clearly indicated that information security in Saudi Arabia faces some serious risks from a range of threat types. It has been determined that these risks are at least partially due to low awareness of information security among the public and low information security practices in organizations. There is a need to reduce the risks faced and provide good strategies for further protection from threats quickly. This study has



proposed the InfoSec CAP model as a process to inform a culturally appropriate response to this challenge. Numerous cultural factors impacting on information security in Saudi Arabia have been considered and addressed. The use of the model will help to establish a strong information security practice and to provide a further information protection.

## **Chapter 7 Conclusion**

### **7.1 Introduction**

This research set out to determine information security awareness and practices in Saudi Arabia. The primary method adopted was online surveys, used to collect the data, and SPSS for analysis. The findings from the analysis were used to frame an understanding of the information security level in Saudi Arabia and to design an appropriate information security structure which takes into account cultural impact. This chapter highlights the overall scope of the research and also presents the significance of the research, findings limitations, and future research directions.

### **7.2 Research Scope**

#### **7.2.1 Links to Earlier Findings**

As the research indicated in earlier chapters, Saudi Arabia has been reported as one of the top countries that are suffering from several types of risks such as attacks (Kaspersky Lab 2011) or spam (Symantec Lab 2011). To find out the reasons behind this, this study was conducted to find out the problem sources. No previous large studies have been conducted and published in this field in Saudi Arabia, perhaps because of either the shortages of qualified people; the high censorship levels; or low awareness of the importance of this matter.

The research has used survey questions which were selected from an instrument developed by the Cyber Security Organization in Malaysia, in consultation with KPMG. The focus of the Cyber Security Organization instrument was very similar to the focus of this research investigation of ISA within the general public. While the Cyber Security Organization questions were developed in Malaysia, they were deemed to be the most appropriate for use in this research due to the similarities of Islamic culture and the absence of other related existing studies and instruments internationally. Due to cultural constraints, it would ordinarily be difficult to gather data from female respondents in Saudi Arabia, however, the use of an online survey helped to collect the data successfully.

Also, the research has used two conducted studies for comparison purposes to determine the ISA and InfoSec levels in Saudi Arabia.

Based on the established understanding of the problems, it was essential to provide a proposed set of guidelines for providing appropriate solutions to address these weaknesses. A new InfoSec CAP model has been introduced to suggest a comprehensive solution for ISA and InfoSec practices.

### ***7.3 Significance of the research***

Threats to InfoSec are a global problem. If one country, or a group of countries, is prone to threats, this weakens InfoSec for everyone. This research has identified a group of high risk countries and suggested that they may be at increased risk due to cultural reasons like their being highly-censored. This study is the first comprehensive study of InfoSec in a highly-censored country. It is the first simultaneous study of both ISA in the public and InfoSec practices in organization.

This study has shown that the high incidence of attacks is almost certainly due to low ISA and poor practices among the general public and to low skill levels and poor practices in organizations. This trend is very likely true in other highly-censored and distinctive culture countries.

It has also demonstrated that cultural practices, such as sharing information with family or wearing a veil, can have negative impact on InfoSec practices. In doing so, it has brought the question of culture, and its impact on InfoSec, into the spotlight.

Finally, this research has proposed a process that could be used in distinctive culture countries to significantly reduce the likelihood of attack and hence increase global InfoSec.

### ***7.4 Limitations of the findings***

The reader should take note of several limitations of this research. As noted in Section 1.6, the lack of the academic literature about information security awareness practices in the Middle East, and especially in Saudi Arabia, was one of the main obstacles. However, the researcher has addressed this problem by using international sources to

achieve the research objectives. Second, the data collection took longer than anticipated to achieved a sufficient response rate for both surveys. The reasons for slow response may be that Saudis are not familiar with surveys or Saudi culture plays a role for response rate for surveys. Also, some Saudi Arabian government organizations that are responsible for censorship were not supportive, resisting providing details about information security in Saudi Arabia with the justification that they were ‘government secrets’.

These findings can be applied in countries that have a similar cultural and legislative framework; however, given the significance of cultural aspects, they are not completely generalizable.

### **7.5 Future research**

Given that this research examines ISA among the general public and InfoSec among organizations in Saudi Arabia, it informs significant areas for future research.

- One of the outcomes of this research is providing feedback and suggestions to the Saudi government and private sector organizations. The findings identified weakness that should be considered and addressed to manage current information risks and to inform the establishment of improved protections from the further threat.
- Replicate the study in other highly-censored and distinctive culture countries to validate findings.
- Conduct one or more longitudinal studies in highly-censored and distinctive culture countries.
- The longitudinal studies could be done to test the InfoSec CAP model. For example, five more highly-censored and distinctive culture countries could be studied. By deploying the InfoSec CAP model in three of them, the performance of these countries could be compared to the performance of the three countries without the model.

## **7.6 Conclusion**

This thesis set out to examine ISA and InfoSec practices in Saudi Arabia and to explore the reasons for the current information risks there. The results indicate that Saudi Arabia has low information security awareness across the general public when compared with other countries. Saudi Arabian organizations also revealed a low level of practice, which may explain the current risks being faced. The vision of this research was to provide a tool that would protect and enhance the information security awareness and practice in Saudi Arabia in the short and long terms. This was provided in the InfoSec cultural adaptation process.

## References

- Abuayen, K. 2006, *Women in Islam*, Dar Majdalawi Pub., Amman, Jordan (Arabic Text).
- Abu-Musa, A. 2007, 'Exploring Information Technology Governance( ITG) in Developing Countries: AN Empirical Study, Saudia Arabia', *The International Journal of Digital Accounting Research*.
- Action Fraud. 2011, accessed 4 August 2011, <http://actionfraud.org.uk/what-is-fraud>
- Afyouni, H. 2006, *Database Security and Auditing: Protecting Data Integrity and Accessibility*, Thomson Course, Canada.
- Albosaily, A. and Rinker-Morris, D. 2012, *Data protection update 5 – Data protection in the Kingdom of Saudi Arabia*, accessed 20 August 2012, <http://www.clydeco.com/knowledge/articles/data-protection-update-5-data-protection-in-the-kingdom-of-saudi-arabia>>
- Albarrak, A. 2014, INTEGRATION OF HOSPITAL SYSTEMS INTO MEDICAL EDUCATION: A BLENDED LEARNING APPROACH, Riyadh: Department of Health Informatics, College of Medicine, King Saud University.
- Albrik, H. 1995, *Encyclopedia of Muslim women*, Dar Almedad Ltd., Saudi Arabia (Arabic Text).
- Aldosari, S. 2009, *Aldawaser Tripe: historical studies*, Dar Manar Alhuda, Riyadh (Arabic Text).
- Alfozan, M. 2008, *Muslim Women Loyalty and her Social Role*, Books World Ltd., Saudi Arabia (Arabic Text).
- Alhagil, H. 2001, *Treasure lineage and Arts Complex*, Saudi National House, Riyadh (Arabic Text).

- Alhajiri, E. 2004, *Internet History in Saudi Arabia*, Saudi Arabia (Arabic Text).
- Ali, A. 2009, *Business and management environment in Saudi Arabia*, NY: Taylor and Francis, New York.
- Alminshaw, M. 2003, *Internet Crimes in Saudi Society*, Naif Arab University for Security Sciences, Riyadh (Arabic Text).
- Alnatheer, M. & Nelson, K. 2009, *Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context*, Melbourne: Australian Information Security Management Conference.
- Alothimin, A. 2009, *History of Saudi Arabia*, Obekan Ltd., Riyadh (Arabic Text).
- Al-Owain M., Al-Zaidan H. & Al-Hassnan Z. 2012, 'Map of autosomal recessive genetic disorders in Saudi Arabia: Concepts and future directions', *Am J Med Genet Part A* 158A: 2629–2640.
- Alqahtani, M. 2006, *Girls in Spider Net*, Dar Twaiq Ltd., Riyadh (Arabic Text).
- Alshaer, E. & Hamed, H. 2004, 'Modelling and Management of Firewall Policies', *IEEE Transactions on Network and Service Management*, vol.1, no.1, pp.2-10.
- Alvesson, M. & Deetz, S. 2000, *Doing Critical Management Research*, Sage Publications, London.
- Armistead, L. 2007, *Information Warfare: Separating Hype from Reality*. s.l.:Potomac Books Inc.
- Ateeq, A. 2012, 'Type of Security Threats and It's Prevention', *International Journal of Computer Technology and Applications*, vol.3, no.2, pp.750-752.
- Ayoub, R. 2011, *The 2011 (ISC) 2 global information security workforce study*, CA: Frost & Sullivan, Mountain View.
- Bandi, F. & Russell, J. 2004, Full-information transaction costs, *Proceedings of the*

*Conference on Analysis of high-frequency data and market microstructure*,  
Taipei.

Banisar, D. 2011, accessed 19 October 2012,  
<https://www.privacyinternational.org/search/content/data%20protection%20map>

Bargiela-Chiappini, F. 2009, *The Handbook of Business Discourse*. s.l.:Edinburgh  
University Press.

Bashir, K. 2006, *Muslim Women World*, Dar ALMamoun, Jordan (Arabic Text).

BBC, 2001. *Saudi women get identity cards*, accessed 6 March 2011,  
[http://news.bbc.co.uk/2/hi/middle\\_east/1702342.stm](http://news.bbc.co.uk/2/hi/middle_east/1702342.stm)

Bisson, J. & Saint-Germain, R. 2005, 'The BS 7799 / ISO 17799 Standard For a Better  
Approach to Information Security', *Callio Technologies*, pp.1-19.

Blaikie, N. 2003, *Analyzing Quantitative Data*, SAGE Publications Ltd., London.

Borns, R. 1996, 'The Internet: Privacy, Censorship, The First Amendment, and  
Transnational Communications; What's At Stake?', *IEEE Xplore*, pp.1337-1341.

Boujettif, M. & Wang, Y. 2007. *Constructivist Approach To Information Security  
Awareness In The Middle East* Mohammed Boujettif, Liverpool: Dept. CS,  
University of Liverpool.

Bowen, W. 2008, *The History of Saudi Arabia*, Greenwood Publishing Group,  
Incorporated.

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

Brotby, W. 2009, *Information Security Management Metrics*, Taylor & Francis Group,  
United States of America.

Brown, B. 2009, *Help Prevent Computer Theft*, Palmerston North, New Zealand.



- Bullen, J. 2000, 'A Critical Assessment of the Key Elements of Successful Project Management', *Working Paper for the Business Information Technology*, pp.79-89.
- Burke, R. 1999, 'Project Management Planning and Control', *West Sussex*, pp.202-230.
- Bygrave, L. 2002, *Data Protection Law, Approaching its Rationale, Logic, and Limits.*, GBR: Wolters Kluwer Law and Business, London.
- Byrd, T. & Turner, D. 2000, 'Measuring the Flexibility of Information Technology Infrastructure: Exploratory Analysis of a Construct. *Journal of Management Information Systems*, vol.17, no.1, pp.167-208.
- Caelli, W., Longley, D. & Shain, M. 1989, 'Information Security for Managers: Annual Information Security Survey', *Stockton Press*, pp.56-82.
- Calder, A. 2006, 'Information security training'. In J. Reuvid, (ed), *The secure online business handbook: A practical guide to risk management and business continuity*, PA: Kogan Page, Philadelphia.
- Calder, A. 2008, *ISO27001 / ISO27002: A Pocket Guide*, IT Governance Publication, United Kingdom.
- Camp, L. & Lewis, S. 2004, *Economics of information security*, MA: Kluwer Academic, Norwell.
- Carol, F., Orit, H., Lenore, B. & Dias, M. 2006, 'Culture and Environment as Determinants of Women's Participation in Computing: Revealing the "women-CS fit"'. *Proceedings of the 37th SIGCSE Technical Symposium on Computer science education*, Houston, Texas.
- Cassell, C., & Symon, G. 1994. 'Qualitative research in work contexts'. In C. Cassell & G. Symon (Eds.), *Qualitative methods in organizational research* (pp. 1-13). Thousand Oaks, CA: Sage Publications.
- Chambers, A. & Rand, G. 2010, *Operational Auditing Handbook: Auditing Business and IT Processes, Second Edition*, GBR: John Wiley & Sons, West Sussex.

- Champion, D. 2003, *The Paradoxical Kingdom: Saudi Arabia and the Momentum of Reform*, GBR: C. Hurst & Co, London.
- Chen, Kinshuk, Wang, 2005, “ Cyber Schooling Framework: Improving Mobility and Situated Learning”: Fifth IEEE International Conference on Advanced Learning Technologies; Taiwan.
- Ciampa, M. 2010, *Security Awareness: Applying Practical Security in Your World*, Course Technology, Boston.
- CITC. 2011, Reports and Studies, accessed 18 July 2011, <http://www.citc.gov.sa/arabic/Reportsandstudies/Reports/Documents/IT%20006%20A%20-%20IT%20Report%202010.pdf>
- CITC. 2012, CITC Roles and Responsibilities, accessed 24 May 2012, <http://www.citc.gov.sa/English/AboutUs/AreasOfwork/Pages/default.aspx>
- Coyne, C. & Leeson, P. 2004, 'Who Protects Cyberspace? Global Prosperity Initiative Working Paper', *Mercatus Center, George Mason University*, vol.37, pp.44-73.
- Crescenzo, G., Rubin, A., Parno, B., Kuo, C. & Perrig, A. 2006, *Financial Cryptography and Data Security*, Springer Berlin Heidelberg, Germany.
- Creswell, J. 2002, *Educational Research: Planning, Conducting and Evaluating Quantitative and Qualitative Research*, Pearson Education Ltd., London.
- Creswell, J. 2003, *Research Design: Qualitative, Quantitative, and Mixed Method Approaches*, Sage Publications, California.
- CSI Computer Crime and Security Survey. 2011, accessed 23 May 2012, <http://reports.informationweek.com/abstract/21/7377/security/research-2010-2011-csi-survey.html>
- David, R. & Brierley, J. 1988, *Major Legal Systems in the World Today*, The Legal Classic Library, Birmingham.
- Deibert, R., Palfrey, J., Rohozinski, R. & Zittrain, J. (Eds) 2008, *Access Denied: The*

*Practice Policy of Global Internet Filtering*, The MIT Press, London.

Detmar, W., Karen, D. & Carole, E. 2003, 'Transfer of information technology to the Arab world: a Test of Cultural Influence Modeling', *Advanced Topics in Global Information Management*. IGI Publishing.

Dorfman, M. 1998, *Introduction to Risk Management and Insurance*, Prentice Hall, New Jersey.

Easttom, C. 2006, *Computer Security Fundamental*, Pearson Prentice Hall, United States of America.

EC-Council, 2010, *Ethical hacking and countermeasures: Linux, Macintosh, and Mobile Systems*, NY: Cengage Learning, Clifton Park.

Echaore-McDavid, S. 2008, *Career opportunities in science*, 2nd ed, NY: Ferguson / Infobase, New York.

Edwards, L. 2010, 'Content Filtering and the New Censorship', *IEEE Computer Society*, pp.317-322.

Erbschloe, M. 2003, *Guide To Disaster Recovery*, Course Technology, Canada.

Farid, S., Roya, G., Dolores, A. & Hig, N. 2009, 'The impact of information and communication technology (ICT), education and regulation on economic freedom in Islamic Middle Eastern countries', *Inf. Manage.*, vol.46, no.8, pp.426-433.

Ferguson, B. 2005, *Network+ fast pass*, CA: SYBEX, Alameda.

Ferrari, E. & Thuraisingham, B. 2006, *Web and Information Security*, IRM Press, United States of America.

Finne, T. 1997, 'A Conceptual Framework for Information Security Management', *Computers and Security*, vol.16, no.6, pp.469-479.

Fisk, M. 2002, 'Causes & Remedies for Social Acceptance of Network Insecurity, Contribution to the "Workshop on Economics and Information Security',

University of California: Berkeley, pp.106-127.

Fugini, M. & Bellettini, C. 2004, *Information Security Policies and Actions in Modern Integrated System*, Idea Group, United States of America.

Furnell, S., Katsikas, S., Lopez, J. & Patel, A. (eds) 2008, *Securing information and Communication Systems: Principles, Technologies, and Applications*, Norwood, MA: Artech House.

Geer, D., Bace, R., Gutmann, P., Metzger, P., Pfleeger, C., Quarterman, J. & Schneier, B. 2003, 'CyberInsecurity: The Cost of Monopoly: How the Dominance of Microsoft's Products Poses a Risk to Security', *Computer & Communications Industry Association*, pp.48-68.

Geric, S. & Hutinski, Z. 2007, 'Information System Security Threats Classifications', *Journal of Information & Organizational Science*, vol.31, no.11.

Glenn, H. 2007, *Legal Traditions of the world*, Oxford University Press, New York.

Green, J. & Karolidies, N. 2005, *Encyclopedia of Censorship*, Facts On File, New York.

Greenwood, P. & Nikulin, M. 1996, *A Guide to Chi-Squared Testing*, John Wiley & Sons, Canada.

Hamade, S. 2008, 'Internet Filtering and Censorship', *IEEE Computer Society*, pp.1081-1086.

Hancock, D. & Algozzine, B. 2006, *Doing Case Study Research*, Teachers College Press, New York.

Hannabuss, S. & Allard, M. 2001, 'Issues of censorship', *Library Review*, vol.50, no.2, pp.81-89.

Harvey, F. & Lausanne 1997, *National cultural differences in theory and practice: Evaluating Hofstede's national cultural framework*, s.l.: MCB UP Ltd.

- Hintzbergen, J., Hintzbergen, K., Smulders, A. & Baars, H. 2010, *Foundations of IT security: Based on ISO 27001/27002*, GBR: Van Haren, Norfolk.
- Hofstede G 2009, 'National and organisational culture: Arab world', accessed 9 February 2010, <http://geert-hofstede.com/arab-world-egiqkwlblysa.html>
- Holmes, O. 2009, *Common Law*, Harvard University Press, Cambridge.
- Hoo, K. 2000, 'How Much is Enough? A Risk Management Approach to Computer Security', *Working Paper: Center for International and Security Studies*, pp.138-152.
- HSBC 2010, *The Report: Saudi Arabia*, s.l.: Oxford Business Group.
- Huang, N., Huang, T.,Keh, H. & Shaw, R. 2011, 'Information Security Awareness on-line materials design with knowledge maps', *International Journal of Distance Education Technologies*, vol.9, p.41.
- Hussain, J. 2004, *Islam: Its law and society*, The Federation Press, Sydney.
- ICT Regulation Toolkit Organization. 2010, accessed 3 April 2010, <http://www.ictregulationtoolkit.org/6.3>
- Johnson, B. & Christensen, L. 2004, *Educational Research: Quantitative, Qualitative and Mixed Approaches*, Pearson Education, United States of America.
- Johnson, R. 2011, *Security policies and implementation issues*, MA: Jones & Bartlett Learning, Sudbury.
- Jones, A. & Ashenden, D. 2005, *Risk Management for Computer Security*, Elsevier Butterworth-Heinemann, United Kingdom.
- Jones, M. & Alony, I. 2007. *The cultural impact of information systems –through the eyes of Hofstede – a critical journey*, s.l.: University of Wollongong.
- Jones, T. 2011, *Desert Kingdom: How Oil and Water Forged Modern Saudi Arabia*, Harvard College, United States of America.

- KACST- King Abdulaziz City for Science and Technology 2010, accessed 17 March 2009, <http://www.kacst.edu.sa/en/Pages/default.aspx>
- Kaspersky Lab. 2010, accessed 29 February 2010, [http://www.securelist.com/en/analysis/204792101/Kaspersky\\_Security\\_Bulletin\\_2009\\_Statistics\\_2009](http://www.securelist.com/en/analysis/204792101/Kaspersky_Security_Bulletin_2009_Statistics_2009)
- Kaspersky Lab. 2011, accessed 14 May 2011 [http://www.securelist.com/en/analysis/204792162/Kaspersky\\_Security\\_Bulletin\\_2010\\_Statistics\\_2010](http://www.securelist.com/en/analysis/204792162/Kaspersky_Security_Bulletin_2010_Statistics_2010)
- Kealey, D. & Protheroe, D. 1996, 'The effectiveness of cross-cultural training for expatriates: An assessment of the literature on the issue', *International Journal of Intercultural Relations*, vol.20, no.2, pp.141-165.
- Kendrick, R. 2010, *Cyber risks for business professionals: A management guide*, GBR: IT Governance, Cambridgeshire.
- Kenning, M. 2001, "Security Management Standard - ISO 17799/BS 7799", *BT Technology Journal*, vol.19, no.3, pp.132-132.
- Khaild, M. 2003, *Internet in Saudi Arabia: Distribution and Use*, Obekan Ltd., Riyadh (Arabic Text).
- Kizza, J. 2005, *Computer network security*, NY: Springer, New York.
- Kizza, J. 2005, *Computer Network Security*, Springer Science Business Media, United States of America.
- Kliem, R. 1999, 'Managing and Controlling Risk', *Year 2000 Practitioner*, vol.2, no.1, p14.
- Knapp, K. Marshall, T., Rainer, K. & Ford, N. 2006, 'Information security: management's effect on culture and policy', *Information Management & Computer Security*, vol.14, no.1, pp.24-36.
- Kruger, H., Drvein, L. & Steyn, T. 2010, 'A vocabulary test to assess information security awareness', *Information Management & Computer Security*, vol.18,

no.5, pp.316-327.

Lanza, R. 2000, 'Does Your Project Risk Management System Do the Job?', *Information Strategy: The Executive's Journal*, pp.6-12.

Lawton, R 2002, 'Balance Your Balanced Scorecard', *Quality Progress*, vol.35, n. 3, pp. 66-71.

Li, X. & Li, J. 2011, *Quality-based content delivery over the Internet*, NY: Springer, New York.

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

Maconachy, W., Schou, C. & Ragsdale, D. 2001. *A Model for Information Assurance: An Integrated Approach*, West Point: Workshop on Information Assurance and Security IEEE.

Mantel, S., Jr., Meredith, J., Shafer, S. & Sutton M. 2001, *Project Management in Practice*, John Wiley & Sons, New Jersey.

McLean, J. 2000 *Security Models and Information Flow*, Washington, D.C: Center for High Assurance Computer Systems.

Merkow, M. & Breithaupt, J. 2006, *Information Security: Principles and Practices*, Pearson Education Ltd., New Jersey.

Microsoft Solutions for Security and Compliance 2006, *The Security Risk Management Guide*, pp.56-78.

Mikusch, R. 2006, 'Prevent Theft of Your Computer', *Beyond Numbers*, Issue no.451, p.26.

Ministry of Communication and Information Technology, 2009, Electronic Crimes Law, accessed date 10/01/2009, <http://www.mcit.gov.sa/arabic/regulations/criminallaws/>

Moaddel, M. 2006, 'The Saudi public speaks: religion, gender, and politics',

*International Journal of Middle East Studies*, vol.38, pp.79-108.

Murphy, J. 2012, Governance and risk management within the context of information security. In: H. F. Tipton and M. K. Nozaki, (eds). *Information security management handbook*, vol.1, 6th ed., FL: CRC / Taylor and Francis, Boca Raton.

Myers, M. & Tan, F. 1997, 'Beyond models of national culture in information systems research' *Journal of Global Information Management*, vol.10, no.1, pp. 24-32.

National Security Agency 2000, *National Information Systems Security Glossary*, NSTISSI 4009 Fort Meade, MD.

NetWitness. 2010, accessed 23 December 2010, <http://www.netwitness.com/resources/pressreleases/feb182010.aspx>

Nichols, A. 2002, 'A Perspective on Threat in the Risk Analysis Process', pp.67-78.

Ning, P. & Sushil, J. 2004, Intrusion detection techniques. In: H. Bidgoli, ed. *The Internet encyclopedia*, vol.2, Hoboken: John Wiley and Sons, pp.355-367.

O'Harrow, R. & Cha, A. 2003, 'Internet Worm Unearths New Holes: Attack Reveals Flaws in How Critical Systems Are Connected', *Washington Post*, <http://www.washingtonpost.com/ac2/wp-dyn/A57550-2003Jan28>.

OECD International Futures Programme 2004, *The Security Economy*, OECD, Paris, pp.34-42.

Oliva, L. 2004, *Information Technology Security Advice from Experts*, Idea Group, United States of America.

Peace, A. 2003, 'Balancing free speech and censorship: academia's response to the Internet', *Communications of the ACM*, vol.46, no.11, pp.104-109.

Peltier, T. 2004, *Information Security Policies and Procedures*, CRC Press, United States of America.

Pittman, R. 2012, Organization culture awareness will cultivate your information



- security program. In: H. F. Tipton and M. K. Nozaki, eds. *Information security management handbook*, Vol.1. 6th ed. Boca Raton, FL: CRC / Taylor and Francis.
- Poulsen, K. 2003, 'Security Focus news article: "Slammer worm crashed Ohio nuke plant network', Security Focus, <http://www.securityfocus.com/news/6767>.
- Prabha, A. 2004, *Information security training*, Malaysia, Kuala Lumpur.
- Purser, S. 2004, *A practical guide to managing information security*, MA: Artech, Norwood.
- Qureshi, A., Younus, A. & Khan, A. 2009, 'Philosophical Survey of Passwords', *International Journal of Computer Science Issues*, vol.2, pp.8-12.
- Raval, V. & Fichadia, A. 2007, *Risks, Controls, and Security: Concepts and Applications*, John & Sons, Inc., United States of America.
- Refat, H. 1998, *Islam and Women Rights*, Dar Alhasad Pub., Syria (Arabic Text).
- Saint-Germain, R. 2005, 'Information Security Management Best Practice Based on ISO/IEC 17799', *The Information Management Journal*, vol.July/August, pp.60-66.
- SANS. 2010, accessed 22 July 2011, <http://www.sans.org/security-resources/policies/>
- Saleh, K. 2009, *Software Engineering*, s.l.:J. Ross Publishing.
- Schönthaler, F., Vossen, G. & Oberweis, A. 2012, *Business Processes for Business Communities: Modeling Languages, Methods, Tools*. s.l.:Springer Science & Business Media.
- Shaluf, I. 2007, 'An Overview on disaster', *Disaster Prevention and Management*, vol.16, no.5, pp.687-703.
- Shaluf, I. 2007, 'Disaster Types', *Disaster Prevention and Management*, vol.16, no.5, pp.704-717.

- Shaw, R., Chen, C., Harris, A. & Huang, H. 2008, 'The impact of information richness on information security awareness training effectiveness', *Computers and Education*, vol.52, no.1, pp.92-100.
- Sherwood, J. 2000, 'Opening up the Enterprise', *Computers & Security*, vol.19, no.8, pp.710-719.
- Siponen, M. 2000, 'A conceptual foundation for organizational: information security awareness', *Information Management & Computer Security*, vol.8, no.1, pp.31-41.
- Siponen, M., Pahnla, S. & Mahmood, A. 2007, Employees' adherence to information security policies: An empirical study. In H. Venter, M. Eloff, L. Labuschagne, J. Eloff, and R. von Solms, eds. *New approaches for security, privacy, and trust in complex environments*. New York, NY: International Federation for Information Processing.
- Slay, J. & Koronios, A. 2006, *Information Technology Security & Risk Management*, John Wiley & Sons Australia Ltd, Australia.
- Smith, P. 1999, 'Managing Risk as Product Development Schedules Shrink', *Research & Technology Management*, pp.25-32.
- Smith, R. 2012, *Elementary information security*, MA: Jones & Bartlett, Burlington.
- Solomon, M. & Chapple, M. 2005, *Information Security Illuminated*, Jones and Bartlett, United States of America.
- Stamp, M. 2006, *Information Security Principles and Practice*, John Wiley & sons Inc., Canada.
- Stanton, J., Guzman, I., and Caldera, C. 2003, *Examining the linkage between organizational commitment and information security*, Proceedings of IEEE Systems, Man, and Cybernetics Conference. Washington. D.C.
- Stanton, J., Stam, K., Mastrangelo, P. & Jolton, J. 2006, Behavioral information security: An overview, results, and research agenda. In: P. Zhang and D. Galletta, eds. *Human-computer interaction and management information*

- systems: Foundations*. Armonk, NY: M. E. Sharpe, pp.262-279.
- Stallings, W. & Brown, L. 2008, *Computer Security Principles and Practice*, Pearson Education, United States of America
- Stewart, J., Tittel, E. & Chapple, M. 2011, *CISSP Certified Information Systems Security Professional Study Guide, 5th edition*, IN: Wiley, Indianapolis.
- Straub, D., Goodman, S. & Baskerville, R. 2008, *Information Security Policy, Processes, and Practices*, M.E Sharpe, United states of America.
- Stulz, R. 2003, *Risk Management & Derivatives*, Mason, Ohio: Thomson South-Western.
- Symantec Lab. 2011, accessed 19 March 2012, [http://www.symantec.com/about/news/release/article.jsp?prid=20110927\\_01](http://www.symantec.com/about/news/release/article.jsp?prid=20110927_01)
- Talib, S., Clarke, N. & Furnell, S. 2010, 'An Analysis of Information Security Awareness within Home and Work Environments', *IEEE Computer Society*, pp.196-203.
- Tashakkori, A. & Teddie, C. 1998, *Mixed Methodology: compaing qualitative and quantitative Approaches*, Sega Publications, United States of America.
- The Saudi Ministry of Interior 2012. 2012, accessed 19 November 2012, [http://www.moi.gov.sa/wps/portal/civilaffairs!/ut/p/b1/04\\_SjzS1NLc0tTS1sNCP0I\\_KSyzLTE8syczPS8wB8aPM4t39woKN3T2MDd39nFwMPAMtnU0s\\_IMN3EMM9YNT8\\_RzoxwVAVLYUeM/](http://www.moi.gov.sa/wps/portal/civilaffairs!/ut/p/b1/04_SjzS1NLc0tTS1sNCP0I_KSyzLTE8syczPS8wB8aPM4t39woKN3T2MDd39nFwMPAMtnU0s_IMN3EMM9YNT8_RzoxwVAVLYUeM/)
- Thompson, R. & Thompson, B. 2006, *Repairing and upgrading your PC.*, CA: O'Reilly Media, Sebastopol.
- Thuraisingham, B. 2005, *Database and Applications Security*, Auerbach Publications, United States of America.
- Torres, J., Sarriegi, J., Santos, J. & Serrano, N. 2006, Managing information systems security: Critical success factors and indicators to measure effectiveness. In: S.

- K> Katsikas, J. Lopez, M. Backes, S. Gritzalis, and B. Preneel, eds. *Information Security: 9th International Conference, ISC 2006 Proceedings*. pp.530-546. Berlin, DEU: Springer.
- Trend Micro Smart Protection Network, 2010, accessed 28 March 2011, [http://...u/cloud-content/us/pdfs/security-intelligence/reports/rpt\\_threat-trends-2010\\_year-of-the-toolkit.pdf](http://...u/cloud-content/us/pdfs/security-intelligence/reports/rpt_threat-trends-2010_year-of-the-toolkit.pdf)
- Turban, E., Wetherbe, J. & McLean, E. 1996, *Information Security Technology for Management: Improving Quality and Productivity*, United States of America.
- United States Government Accountability Office 2007, *Information security: Sustained management commitment and oversight are vital to resolving long-standing weaknesses at the Department of Veteran Affairs*. Darby, PA: Diane.
- Vacca, J. 2009, *Computer and information security handbook*, Burlington, MA: Morgan Kaufmann.
- Wang, L. & Yi, J. 2009 'China's civil law since reform and opening up in 1978', *Social Sciences in China*, vol.30, no.1, pp.83-99.
- Weirich, D. & Sasse, M. 2001, Pretty good persuasion: A first step towards effective password security in the real world. In: V. Raskin, S. J. Greenwald, B. Timmerman, Darrell M. Kienzle. eds., NSPW (National Security Paradigms Workshop) *Proceedings of the 2001 workshop on new security paradigms*, Cloudcroft, New Mexico 10-13 September 2001. New York: Association for Computing Machinery (ACM).
- Willett, K. 2008. *Information Assurance Architecture*. s.l.:CRC Press.
- Werlinger, R., Hawkey, K. & Beznosov, K. 2007, *Human, Organizational and Technological Challenges of Implementing IT Security in Organizations*. <http://lersse-dl.ece.ubc.ca/record/153/files/153.pdf>.
- Whitman, M. & Mattord, H. 2008, *Management of Information Security*, Thomson

Course Technology, Canada.

Whitman, M. & Mattord, H. 2012, *Principles of information technology*, MA: Cengage Learning, Boston.

Wilson, P. & Douglas, G. 1994, *Saudi Arabia: the coming storm*, M. E. Sharpe, New York.

Wright, C. 2008, *The IT regulatory and standards compliance handbook: How to survive an information systems audit and assessments*, MA: Syngress, Burlington.

Wright, M. & Kakalik, J. 2007, *Information Security: Contemporary Cases*, Jones and Bartlett, United States of America.

Wylder, J. 2004, *Strategic Information Security*, CRC Press LLC, United States of America.

Wylder, J. 2012, Toward enforcing security policy: Encouraging personal accountability for corporate information security policy. In: H. F. Tipton and M. K. Nozaki, eds. *Information security management handbook*, Volume 1. 6th ed. Boca Raton, FL: CRC / Taylor and Francis.

Zakour, A. 2004, *CULTURAL DIFFERENCES AND INFORMATION TECHNOLOGY ACCEPTANCE*, Georgia: Proceedings of the 7th Annual Conference of the Southern Association for Information Systems.

## **Appendix A: Survey Questions for Public Awareness on Information Security in Saudi Arabia (English)**

### **1. Section A - General Background**

#### **1. What gender group do you belong to?**

- ☐ Male
- ☐ Female

#### **2. What age group do you belong to?**

- ☐ 18 - 22
- ☐ 23 - 27
- ☐ 28 - 32
- ☐ 33 - 42
- ☐ 43 - 59
- ☐ 60 and above

#### **3. What is your highest education level?**

- ☐ Doctoral Degree
- ☐ Master Degree
- ☐ Undergraduate Degree
- ☐ Diploma
- ☐ High School
- ☐ Intermediate School
- ☐ Primary School
- ☐ None

**4. Please select the appropriate type of organization that you are currently working for:**

- ☐ Government
- ☐ Private Sector
- ☐ Other (Please Specify)

**5. What is your currently working status?**

- ☐ Self employed (own business, etc.)
- ☐ Not Employed
- ☐ Student
- ☐ Other (Please Specify)

**6. Please select the appropriate type of industry that your organization belong to**

- ☐ Military Sector
- ☐ Banking & Finance
- ☐ Education
- ☐ Industry Services
- ☐ Trading & Contracting
- ☐ Information & Communication
- ☐ Health Services
- ☐ Food & Agriculture
- ☐ Transportation
- ☐ Energy
- ☐ Water
- ☐ Foreign Affairs Sector
- ☐ National Economy Sector

☐ Planning and Housing Sector

☐ Labour Sector

☐ Tourism

☐ Social Affairs Sector

☐ Justice Sector

☐ Islamic Affairs Sector

☐ Media Sector

☐ Other (Please Specify)

**7. Do you live in a rural or urban area?**

☐ Rural

☐ Urban

**8. Which city in Saudi Arabia do you currently live in?**

☐ Riyadh

☐ Makkah

☐ Jeddah

☐ Dammam

☐ Qasim

☐ Abha

☐ Arar

☐ Other (Please Specify)

**2. Section B1 - General Practices**

**9. Have you ever used internet?**

☐ Yes

☐ No Go to question 11



**10. For what purpose do you spend your time online? Please indicate the amount of time that spent per hour on each purpose per week?**

	0	1 to 6	7 to 12	13 to 18	19-24	25 & more
<input type="checkbox"/> Email	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Instant Messaging	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Shopping	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Blogging	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Social Networking	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Online transactions	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Online games	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> File downloading	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Video sharing	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Latest news	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Researching Information	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Other, please specify						

**11. What type of devices do you currently use? (Please tick the below options, whichever is applicable)**

- ☐ Desktop/ Laptop
- ☐ Mobile phone
- ☐ Smart phone/ PDA
- ☐ Portable video game console
- ☐ USB Flash Drive
- ☐ GPS

**12. Do you keep your mobile devices (PDAs, laptop, USB keys) in a secured place and do you practice precautions to keep it secured (i.e. use locking devices) when not used?**

- ☐ Yes, all the time
- ☐ Sometimes
- ☐ No
- ☐ I don't have such devices
- ☐ I do not know

**13. How secure do you think information is on your computer/mobile device? If it's secure please select the secure level (6=very good; 5=good;4=neutral;3=poor;2=very poor;1=not exist)**

- |                                 |                          |                          |                          |                          |                          |                          |
|---------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
|                                 | 1                        | 2                        | 3                        | 4                        | 5                        | 6                        |
| <input type="checkbox"/> Secure | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

**14. Do you have passwords for the following on your device(s)?**

- ☐ Login/ Switch On
- ☐ Screensaver
- ☐ Neither
- ☐ Other (Please Specify)

**15. How secure is your password? (Select more than one column if applicable)**

- |   |                          |                          |                          |                          |
|---|--------------------------|--------------------------|--------------------------|--------------------------|
|   | Small letters            | Capital letters          | Numbers                  | Special Characters       |
| <input type="checkbox"/> Less than 5 characters | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> 5 to 8 characters      | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> more than 8 characters | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

**16. How often do you change your password?**

- ☐ Daily
- ☐ Weekly

- ☐ Monthly
- ☐ Quarterly
- ☐ Annually
- ☐ Never

**17. Your password used to access your accounts data is known:**

- ☐ Only by you
- ☐ By a few colleagues
- ☐ By a system administrator
- ☐ By family members

**18. Have you heard of and are aware of the existence of the following threats?  
(Please tick whichever is applicable)**

- ☐ Virus or malware
- ☐ Phishing
- ☐ Spam emails
- ☐ Denials of Services
- ☐ Fraud and forgery
- ☐ Vulnerability probing
- ☐ Harassment or cyber bullying
- ☐ Cyber stalking
- ☐ System intrusion
- ☐ Identity theft

**19. What software do you currently use?**

- ☐ Antivirus
- ☐ Firewall
- ☐ Internet Security
- ☐ Anti-spam
- ☐ Anti-spy

**20. What is the type of used software and when did you last update it?**

	One day ago	Last month	3 months ago	6 months ago	Last year	Never
<input type="checkbox"/> Freeware	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Paid License	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**21. Do you use private web mail for professional purposes?**

- ☐ Never
- ☐ Sometimes
- ☐ Frequently
- ☐ Everyday

**22. How often do you back up your sensitive / critical data?**

- ☐ Never
- ☐ Sometimes
- ☐ Frequently
- ☐ Everyday

**23. How would you react if you receive a phone call or an email asking for information (i.e. mobile number, personal email address)?**

- ☐ I never answer
- ☐ I answer the questions
- ☐ I ask for details before answering
- ☐ I ask a colleague or a friend for advice
- ☐ I do not know

**24. Do you know if you can report security incidents (i.e. illegal content, inappropriate websites, spam, harassment, hack threat) and where you can report this?**

- ☐ No
- ☐ Yes

**25. Has your information been hacked or stolen from you're mobile/ computer and how many times if that happened?**

- ☐ Yes
- ☐ No
- ☐ Do not Know

## **Section B2 - Perception / Confidence Level**

**26. I feel privacy is important when online activities:**

- ☐ Strongly Disagree
- ☐ Disagree
- ☐ Agree
- ☐ Strongly Agree
- ☐ N/A

**27. Who do you think is responsible for the privacy of your digital information?**

- ☐ Myself
- ☐ The government
- ☐ The company I divulge my digital information to

## **Section C – Promotion Preferences**

**28. Have you ever been or use one of the following sources to learn about information security? (Please tick from the options below)**

- ☐ Exhibitions or seminars
- ☐ Courses
- ☐ Books
- ☐ Articles
- ☐ Internet Websites
- ☐ N/A

**29. Which communication do you think is effective in promoting awareness of information security for the public? Please tick the best THREE options below.**

- ☐ Newspapers
- ☐ Magazines
- ☐ Books
- ☐ Billboard/ Posters
- ☐ Web portals
- ☐ E-Books/ e-Magazines
- ☐ Web based games
- ☐ Exhibitions
- ☐ Seminars
- ☐ Talks
- ☐ Advertisements
- ☐ Cartoon series
- ☐ Educational Programs (i.e. Documentaries)
- ☐ Other (Please Specify)

## Appendix B: Survey Questions for Public Awareness on Information Security in Saudi Arabia (Arabic)

استبيان عن الوعي العام عن امن المعلومات في المملكة العربية السعودية

القسم الأول: معلومات عامة

1. الجنس:

☐ ذكر

☐ أنثى

2. ما الفئة العمرية التي تنتمي إليها؟

☐ 18 - 22

☐ 23 - 27

☐ 28 - 32

☐ 33 - 42

☐ 43 - 59

☐ 60 فما فوق

3. ما هو أعلى مستوى تعليمي حصلت عليه؟

☐ الدكتوراه

☐ الماجستير

☐ البكالوريوس الجامعي

☐ الدبلوم

☐ الثانوية

☐ المرحلة المتوسطة

☐ المرحلة الابتدائية

☐ لا احمل مؤهل دراسي

4. نوع المؤسسة التي تعمل بها حاليا :

- ☐ حكومية
- ☐ القطاع الخاص
- ☐ غير ذلك (الرجاء التوضيح)

5. ما هو وضعك الوظيفي الحالي إذا كنت لا تنتمي إلى المؤسستين السابقتين؟

- ☐ عمل خاص بك
- ☐ غير موظف
- ☐ طالب / طالبة
- ☐ غير ذلك (الرجاء التوضيح)

6. الرجاء اختيار النوع المناسب التي تنتمي إليه المؤسسة التي تعمل بها:

- ☐ القطاع العسكري
- ☐ البنوك والمصرفية المالية
- ☐ التعليم
- ☐ الصناعة
- ☐ التجارة والمقاولات
- ☐ المعلومات والاتصالات
- ☐ الصحة
- ☐ الأغذية والزراعة
- ☐ النقل والمواصلات
- ☐ الطاقة
- ☐ الكهرباء
- ☐ المياه
- ☐ وزارة الخارجية
- ☐ الاقتصاد الوطني
- ☐ التخطيط والإسكان
- ☐ وزارة العمل



- ☐ السياحة
- ☐ الشؤون الاجتماعية
- ☐ وزارة العدل
- ☐ الشؤون الإسلامية والأوقاف
- ☐ الإعلام
- ☐ غير ذلك (الرجاء التوضيح)

7. هل تعيش بمدينة أم في الأرياف ؟

- ☐ مدينة
- ☐ قرية (الريف)

8. ماهي المدينة التي تعيش بها حاليا في المملكة العربية السعودية؟

- ☐ الرياض
- ☐ مكة
- ☐ المدينة المنورة
- ☐ جدة
- ☐ الدمام
- ☐ القصيم
- ☐ أبها
- ☐ عرعر
- ☐ غير ذلك (الرجاء التوضيح)

القسم الثاني- الجزء الأول: الممارسات العامة

9. هل سبق وان استخدمت الانترنت ؟

- ☐ نعم
- ☐ لا      أذهب إلى السؤال رقم 11

10. لأي غرض كنت تقضي وقتك على الانترنت؟ الرجاء تحديد مقدار الوقت المستنفذ على كل غرض في الأسبوع؟

صفر 6-1 12-7 18-13 24-19 25+

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	البريد الالكتروني
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	التراسل الفوري (المحادثة)
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	التسوق
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	المنتديات
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	الشبكات الاجتماعية (كالفيس بوك وتويتر)
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	المعاملات الكترونية عبر الانترنت
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	الألعاب المباشرة على الانترنت
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	تحميل الملفات
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	المشاركات الفيديوية
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	الأخبار
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	البحث عن المعلومات
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	دورات مباشرة على الانترنت أو تعليم عن بعد
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	غير ذلك (الرجاء التوضيح)

11. ما هو نوع الأجهزة التي تستخدمها حالياً؟ (الرجاء اختيار وتحديد الأنواع)

- ☐ كمبيوتر مكتبي / محمول
- ☐ تلفون نقال
- ☐ الهاتف الذكي / المساعد الشخصي الرقمي
- ☐ أجهزة ألعاب الفيديو المحمولة
- ☐ وسائط تخزينية قابلة للإزالة
- ☐ نظام تحديد المواقع

12. هل تبقى أجهزة الجوال (أجهزة المساعد الرقمي الشخصي ، والكمبيوتر المحمول ، وسائط تخزينية قابلة للإزالة في مكان آمن وهل تضع احتياطاتك للحفاظ عليها أمانة (أي استخدام أقفال للأجهزة) عند عدم استخدامها؟

- ☐ نعم ، كل الوقت  
☐ أحيانا  
☐ لا  
☐ ليس لدي مثل هذه الأجهزة  
☐ لا أعرف

13. هل تعتقد أن المعلومات الموجودة على جهاز الكمبيوتر الخاص بك / جهاز الهاتف النقال آمنة؟ إذا كانت آمنة ، يرجى تحديد مستوى الأمان (6 = الأكثر ؛ 1 = لا يوجد)

- |                          |                          |                          |                          |                          |                          |                               |
|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|-------------------------------|
| 6                        | 5                        | 4                        | 3                        | 2                        | 1                        |                               |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | آمنة <input type="checkbox"/> |

14. هل لديك كلمة مرور على الأجهزة الخاصة بك؟

- ☐ الدخول والتشغيل  
☐ شاشة التوقف  
☐ لا

15. ما هي درجة الأمان لكلمة المرور الخاصة بك؟ الرجاء اختيار أكثر من عمود إن وجدت

- | رموز خاصة                | ارقام                    | أحرف صغيرة               | أحرف كبيرة               |  |
|--------------------------|--------------------------|--------------------------|--------------------------|--|
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> أقل من خمسة أحرف        |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> من خمسة إلى ثمانية أحرف |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> أكثر من ثمانية أحرف     |

16. تقوم بتغيير كلمة المرور الخاصة بك:

- ☐ يوميا  
☐ أسبوعيا  
☐ شهريا  
☐ فصليا  
☐ سنويا

☐ أبدا لا أقوم بتغييرها

**17. كلمة المرور المستخدمة للوصول إلى حساباتك معروفة من:**

☐ فقط من قبلك أنت

☐ قليل من أصدقائك

☐ مسئول النظام

☐ أفراد أسرته

**18. هل سبق لك وان سمعت أو كنت واعيا عن أي من التهديدات التالية؟ ( الرجاء اختيار وتحديد الأنواع)**

☐ الفيروسات والبرامج الخبيثة

☐ الخداع والتصيد

☐ رسائل البريد الإلكتروني المزعجة

☐ هجوم الحرمان من الخدمات

☐ الاحتيال والتزوير

☐ الثغرات وضعف التحقيق

☐ المضايقة والترهيب بواسطة الانترنت

☐ المطاردة والتتبع بواسطة الانترنت

☐ نظام التسلل

☐ سرقة الهوية

**19. أي من البرامج الحالية تستخدمها في أجهزتك:**

☐ مكافحة الفيروسات

☐ الجدار الناري

☐ امن الانترنت

☐ مكافحة التجسس

☐ مكافحة البريد المزعج

20. ما هو نوع البرامج المستخدمة؟ ومتى آخر تحديث لها؟

قبل يوم	قبل شهر	قبل ثلاثة أشهر	قبل ستة أشهر	قبل سنة	أبدا
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

21. هل تستخدم البريد الإلكتروني الخاص لأغراض مهنية؟

- ☐ أبدا
- ☐ أحيانا
- ☐ كثيرا
- ☐ يوميا

22. تقوم بعمل نسخ احتياطي لبياناتك المهمة:

- ☐ لا تقوم بذلك أبدا
- ☐ أحيانا
- ☐ كثيرا
- ☐ يوميا

23. كيف ستكون ردة فعلك إذا تلقيت مكالمة هاتفية أو رسالة بريد إلكتروني تطلب معلومات عن ( رقم الهاتف المتحرك ، بيانات البريد الإلكتروني الشخصي )

- ☐ لا أجيب
- ☐ أجيب عن الأسئلة
- ☐ أسأل عن التفاصيل قبل الإجابة
- ☐ أطلب الحصول على النصيحة من صديق أو زميل
- ☐ لا أعرف

24. هل تعرف إذا كنت تستطيع التبليغ عن الحوادث الأمنية (أي محتوى غير قانوني ، ومواقع الويب غير الملائمة ، والبريد المزعج والمضايقة والتهديد الإختراق) ، وإلى أين ترسل هذا التقرير؟

- ☐ لا
- ☐ نعم

25. هل سبق وأن اخترقت أو سرقت معلوماتك الشخصية من هاتفك المتحرك أو الكمبيوتر وكم مرة حصل ذلك إن وجد

☐ نعم

☐ لا

☐ ليس لدي فكرة أن كان ذلك قد حدث

### القسم الثاني- الجزء الثاني: الإدراك ومستوى الثقة

26. أشعر بأن الخصوصية مهمة عند القيام باستخدام الانترنت:

☐ لا أوافق بشدة

☐ لا أوافق

☐ أوافق

☐ أوافق بشدة

☐ غير متوفر

27. من هم المسؤولين برأيك عن خصوصية معلوماتك الرقمية؟

☐ أنا

☐ الحكومة

☐ الشركة التي أقوم بإرسال المعلومات من خلالها

### القسم الثالث: الدعم والمفاضلة

28. هل سبق لك استخدام واحدة من المصادر التالية لمعرفة المزيد عن أمن المعلومات؟ ( يرجى وضع علامة من بين الخيارات أدناه )

☐ المعارض أو الندوات

☐ الموضوع:

☐ الكتب

☐ مقالات

☐ مواقع الإنترنت

☐ غير متوفر

29. ما هي الطرق والوسائل الفعالة برأيك في تفعيل وتعزيز امن المعلومات لدى المستخدمين؟ ( الرجاء اختيار أفضل ثلاث وسائل)

- ☐ الصحف
- ☐ المجلات
- ☐ الكتب
- ☐ الملصقات التوعوية
- ☐ منتديات وبوابات الانترنت
- ☐ الكتب والمجلات الالكترونية
- ☐ الألعاب التوعوية
- ☐ المعارض
- ☐ الندوات
- ☐ المحادثات
- ☐ الإعلانات
- ☐ الرسوم المتحركة التعليمية
- ☐ البرامج التعليمية الوثائقية
- ☐ أخرى (الرجاء التوضيح)

## **Appendix C: Information Security and Risk Management Policies Survey for IT Department in Saudi Arabia (English)**

### **Section A: Organization Background**

#### **1. Nature of Organization:**

- ☐ Public sector / Government agency
- ☐ Private sector / Business
- ☐ Non-for-profit organization
- ☐ Other, please specify

#### **2. Organization's Sector:**

- ☐ Military Sector
- ☐ Banking & Finance
- ☐ Education
- ☐ Industry Services
- ☐ Trading & Contracting
- ☐ Information & Communication
- ☐ Health Services
- ☐ Food & Agriculture
- ☐ Transportation
- ☐ Energy
- ☐ Water
- ☐ Foreign Affairs Sector
- ☐ National Economy Sector
- ☐ Planning and Housing Sector
- ☐ Labour Sector



- ☐ Tourism
- ☐ Social Affairs Sector
- ☐ Justice Sector
- ☐ Islamic Affairs Sector
- ☐ Media Sector
- ☐ Other (Please Specify)

**3. Size of your organization:**

- ☐ 1 - 50 Employees
- ☐ 51 – 100 Employees
- ☐ 101 – 500 Employees
- ☐ 501 - 1000 Employees
- ☐ Above 1000 Employee

**4. Number of years of the organization:**

- ☐ Less than 1 year
- ☐ Between 11 to 20 years
- ☐ Between 1 to 5 years
- ☐ Between 21 to 30 years
- ☐ Between 6 to 10 years
- ☐ More than 30 years

**5. Does your organization have an IT department?**

- ☐ Yes
- ☐ No

**6. Does your organization have a specific IT budget?**

- ☐ Yes
- ☐ No
- ☐ Not Sure

**7. Does your organization have a specific Information Security budget?**

- ☐ Yes

☐ No

☐ Not Sure

**8. Is there at least one person in the organization who is knowledgeable about information security who tries to take care of information security matters?**

☐ Yes

☐ No

### **Section B1: Data Protection Laws in the Organization**

**9. Does your organization apply any data protection or information security Law?**

☐ Yes

☐ No

**10. I feel comfortable with this law:**

☐ Strongly Disagree

☐ Disagree

☐ Agree

☐ Strongly Agree

☐ N/A

**11. I feel comfortable about the quality of this law:**

☐ Strongly Disagree

☐ Disagree

☐ Agree

☐ Strongly Agree

☐ N/A

**12. I feel comfortable about the comprehensive and appropriate of this law:**

☐ Strongly Disagree

☐ Disagree

☐ Agree

☐ Strongly Agree

☐ N/A

**13. I feel comfortable about the power of this law:**

☐ Strongly Disagree

☐ Disagree

☐ Agree

☐ Strongly Agree

☐ N/A

## **Section B2: Organization's Information Security Standards**

**14. Does your organization apply any information security standards?**

☐ Yes

☐ No

**15. If not currently applied, does your organization plan to apply information security standards in the future?**

☐ Yes

☐ No

☐ Not Sure

**16. If your organization has already applied information security standards, do you feel more secure in your organization?**

☐ Yes

☐ No

☐ Somewhat

☐ N/A

**17. Is there someone in your organization who is responsible for ensuring that adopted standards are being adhered to:**

☐ Yes

☐ No

☐ Not Sure

### **Section B3: Information Security Policies in Organizations**

**18. Does your organization have an information security policy?**

☐ Yes

☐ No

**19. If there is an information security policy, does your organization enforce it?**

☐ Yes

☐ No

☐ Not Sure

**20. Does your organization have a risk assessment process?**

☐ Yes

☐ No

### **Section C1: Information Assurance in the Organization**

**21. Do you have procedures and regulations in creating and managing users' accounts?**

☐ Yes

☐ No

**22. Does your organization have a data backup and recovery policy?**

☐ Yes

☐ No

**23. Does your organization have a security incidents reporting plan?**

☐ Yes

☐ No

## Section C2: Information Assurance Tool/ Measures in the Organization

**24. How effective do you think Vulnerability Assessment performed in your organization (6=very good; 5=good;4= neutral;3=poor;2=very poor;1=not exist)**

	1	2	3	4	5	6
<input type="checkbox"/> Vulnerability Assessment	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**25. How secure is your organization process/practice in setting passwords?**

**(6=very good; 5=good;4= neutral;3=poor;2=very poor;1=not exist)**

	1	2	3	4	5	6
<input type="checkbox"/> Password setting	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**26. Does your organization implement two factor authentication in your organization (i.e. smart-card, biometric, one time password...etc )**

☐ Yes

☐ No

**27. How secure is your organization Firewall system to protect against undesired access to organization servers from outside the organization?**

**(6=very good; 5=good;4= neutral;3=poor;2=very poor;1=not exist)**

	1	2	3	4	5	6
<input type="checkbox"/> Firewall security	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**28. If your organization has wireless internet connection, how strict are the access rules that only its employees can use this wireless network?**

**(6=very strict; 5=strict;4=neutral;3=poor restriction;2=very poor restriction;1=not exist)**

	1	2	3	4	5	6
<input type="checkbox"/> Wireless Access Rule	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**29. How restrict is your organization with access to specific internet sites?**

**(6=very strict; 5=strict;4=neutral;3=poor restriction;2=very poor restriction;1=not exist)**

1	2	3	4	5	6
---	---	---	---	---	---

☐ Internet Access ☐ ☐ ☐ ☐ ☐ ☐

**30. Does your organization keep operating systems and or software packages updated with most recent software/update releases?**

- ☐ Daily  
☐ Weekly  
☐ Monthly  
☐ Quarterly  
☐ Annually  
☐ Never

**31. How strong is your organization anti-virus software?**

(6=very good; 5=good;4= neutral;3=poor;2=very poor;1=not exist)

	1	2	3	4	5	6
<input type="checkbox"/> Anti-virus software strength	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>						

**32. How strong is your organization intrusion detection software?**

(6=very good; 5=good;4= neutral;3=poor;2=very poor;1=not exist)

	1	2	3	4	5	6
<input type="checkbox"/> Intrusion detection software strength	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**33. How effective is your organization encryption for its important data?**

(6=very good; 5=good;4= neutral;3=poor;2=very poor;1=not exist)

	1	2	3	4	5	6
<input type="checkbox"/> Encrypt technique	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>						

**34. How secure is your organization server room protected by physical security (i.e. PIN, Biometrics...etc)?**

(6=very good; 5=good;4= neutral;3=poor;2=very poor;1=not exist)

	1	2	3	4	5	6

☐ Server room physical security    ☐    ☐    ☐    ☐    ☐    ☐

**35. How restricted is your organization with employees from using input devices such as CD/DVD drives and USB memory?**

(6=very strict; 5=strict;4=neutral;3=poor restriction;2=very poor restriction;1=not exist)

1                      2                      3                      4                      5                      6

☐ Input devices use                      ☐                      ☐                      ☐                      ☐                      ☐

**36. Does your organization offer special information security training to employees?**

☐ Yes

☐ No

**37. Are you planning to acquire certifications in Information Security?**

☐ Yes, within the next 12 months

☐ Yes, but I'm not sure when

☐ Yes, within the next 3 years

☐ No

☐ Yes, within the next 10 years

### **Section C3: Information Security risks in organizations**

**38. Have your organization's information systems ever been down due to computer viruses?**

☐ Yes

☐ No

☐ Not Sure

**39. Has your organization's web site ever been subjected to hacker attack?**

☐ Yes

☐ No

☐ Not Sure

☐ Do Not Have a Web Site

**40. Have your organization's information systems been subjected to hacker attacks?**

- ☐ Yes
- ☐ No
- ☐ Not Sure

**41. Which of the following other computer security risks has your organization ever been exposed to (please choose all that apply)**

- ☐ Denial of service attack
- ☐ Internal employee vandalism
- ☐ Theft of customer/citizen data
- ☐ Stolen Computers/ laptops
- ☐ Website Vandalism
- ☐ No Risks
- ☐ Not Sure
- ☐ Other, please specify

**42. Saudi Arabia has tribe societies, those societies can be a risk factor for information security and privacy especially with abuse or publishing incidents, do you think this risk is effective:**

- ☐ Strongly Disagree
- ☐ Disagree
- ☐ Agree
- ☐ Strongly Agree
- ☐ N/A

**43. Tribe society's people can get some information illegally using their tribe's connections**

- ☐ Strongly Disagree
- ☐ Disagree
- ☐ Agree



☐ Strongly Agree

☐ N/A

**44. In tribe society, people sometimes use their authority to employ their relative if they do not have related qualifications for the job:**

☐ Strongly Disagree

☐ Disagree

☐ Agree

☐ Strongly Agree

☐ N/A

**45. In Saudi Arabia women wear the veil which hide women identity and that can make it very hard to track their incidents for information, do you think this risk is affective:**

☐ Strongly Disagree

☐ Disagree

☐ Agree

☐ Strongly Agree

☐ N/A

**46. Women in Saudi Arabia can use the other women ID because there is no matched picture which may cause serious problem:**

☐ Strongly Disagree

☐ Disagree

☐ Agree

☐ Strongly Agree

☐ N/A

**47. In some of Saudi Arabia tribe's culture, people refused to give permission for their women to have ID with picture:**

☐ Strongly Disagree

☐ Disagree

☐ Agree

☐ Strongly Agree

☐ N/A

## **Section D: Preferences Promotions**

**48. What do you think are the challenges of applying information security standards in your organization? (Please tick the below options, whichever is applicable)**

☐ Do not have the budget to do so

☐ Standards in non-Arabic are hard to understand

☐ Shortage of qualified people in information security

☐ International standards are difficult to apply in general

☐ Not sure

☐ Other, please specify

--

**49. What are the obstacles you have faced/are facing in acquiring certifications in Information Security? (Please tick the below options, whichever is applicable)**

☐ High fee amount

☐ Unclear career roadmap

☐ Insufficient study time

☐ Lack of guidance on career progression

☐ Insufficient exam guidance

☐ Not applicable (N/A)

☐ Unable to obtain information regarding certification

☐ Other (Please Specify)

**50. What kind of benefit from your organization would interest you to acquire additional certification in Information Security? (Please tick the below options, whichever is applicable)**

☐ Certification Fund (Course/Training Fee & Exam Fee) without contract

☐ Certification Fund (Course/Training Fee & Exam Fee) with contract

☐ Exam Fee allocation without contract

☐ Exam Fee with bonded contract

- ☐ Study leave
- ☐ Not applicable (N/A)
- ☐ Other (Please Specify)

**51. What kind of promotions would interest you to acquire additional certification in Information Security? (Please tick the below options, whichever is applicable)**

- ☐ Exam fee discount
- ☐ IT Security Conference benefits
- ☐ Networking event benefits
- ☐ Product discount benefits
- ☐ Other (Please Specify)

## Appendix D: Information Security and Risk Management Policies Survey for IT Department in Saudi Arabia (Arabic)

استبيان خاص بسياسة والممارسة الخاصة بأمن المعلومات بأقسام تقنية المعلومات في المملكة العربية  
السعودية

القسم الأول – الجزء الأول: خلفية عامة عن المنظمة

### 1. طبيعة المنظمة:

- ☐ القطاع العام / وكالة حكومية
- ☐ القطاع الخاص / الأعمال
- ☐ منظمة غير هادفة للربح
- ☐ أخرى ، يرجى تحديدها

### 2. قطاع المنظمة:

☐ القطاع العسكري

☐ البنوك والمصرفية المالية

☐ التعليم

☐ الصناعة

☐ التجارة والمقاولات

☐ المعلومات والاتصالات

☐ الصحة

☐ الأغذية والزراعة

☐ النقل والمواصلات

☐ الطاقة

☐ الكهرباء

☐ المياه

☐ وزارة الخارجية

☐ الاقتصاد الوطني

☐ التخطيط والإسكان

☐ وزارة العمل

- ☐ السياحة
- ☐ الشؤون الاجتماعية
- ☐ وزارة العدل
- ☐ الشؤون الإسلامية والأوقاف
- ☐ الإعلام
- ☐ غير ذلك (الرجاء التوضيح)

**3. حجم المنظمة :**

- ☐ 1 - 50 موظف
- ☐ 51 - 100 موظف
- ☐ 101 - 500 موظف
- ☐ 501 - 1000 موظف
- ☐ أكثر من 1000 موظف

**4. عمر المنظمة (عدد سنوات المنظمة):**

- ☐ أقل من سنة
- ☐ ما بين 11 - 20 سنة
- ☐ ما بين 1 - 5 سنوات
- ☐ ما بين 21 - 30 سنة
- ☐ ما بين 6 - 10 سنوات
- ☐ أكثر من 30 سنة

**5. هل يوجد بمنظمتكم قسم خاص بتقنية المعلومات؟**

- ☐ نعم
- ☐ لا

**6. هل لدى منظمتكم ميزانية محددة لتقنية المعلومات؟**

- ☐ نعم
- ☐ لا
- ☐ غير متأكد

**7. هل لدى منظمتكم ميزانية محددة لأمن المعلومات؟**

- ☐ نعم
- ☐ لا
- ☐ غير متأكد

**8. هل يوجد بمنظمتكم ما لا يقل عن شخص واحد على دراية بأمن المعلومات للاهتمام بما يتعلق بأمن المعلومات؟**

- ☐ نعم

□ لا

القسم الثاني – الجزء الأول: قانون حماية البيانات في المنظمة

9. هل منظمتكم تطبق أي قانون خاص بحماية البيانات أو أمن المعلومات ؟

□ نعم

□ لا

10. أشعر بالارتياح مع هذا القانون:

□ لا أوافق تماما

□ لا أوافق

□ أوافق

□ أوافق تماما

□ غير متوفر (لا ينطبق)

11. أشعر بالارتياح حول جودة هذا القانون:

□ لا أوافق تماما

□ لا أوافق

□ أوافق

□ أوافق تماما

□ غير متوفر (لا ينطبق)

12. أشعر بالارتياح حول ملائمة وشمولية هذا القانون:

□ لا أوافق تماما

□ لا أوافق

□ أوافق

□ أوافق تماما

□ غير متوفر (لا ينطبق)

13. أشعر بالارتياح حول قوة هذا القانون:

□ لا أوافق تماما

□ لا أوافق

□ أوافق

- ☐ أوافق تماماً  
☐ غير متوفر (لا ينطبق)

القسم الثاني – الجزء الثاني : معايير أمن المعلومات في المنظمة

14. هل منظمتم تطبيق أية نوع من معايير أمن المعلومات؟

- ☐ نعم  
☐ لا

15. إذا لم تكن مطبقة حالياً، هل لدى منظمتم خطة لتطبيق معايير أمن المعلومات في المستقبل؟

- ☐ نعم  
☐ لا  
☐ غير متأكد

16. إذا كانت منظمتم قد قامت بالفعل بتطبيق معايير أمن المعلومات، هل تشعر أكثر أماناً في منظمتم؟

- ☐ نعم  
☐ لا  
☐ إلى حد ما  
☐ غير متوفر (لا ينطبق)

17. هل هناك شخص ما في منظمتم مسؤول عن ضمان الالتزام بالمعايير المعتمدة لأمن المعلومات:

- ☐ نعم  
☐ لا  
☐ غير متأكد

القسم الثاني – الجزء الثالث : سياسة أمن المعلومات في المنظمة

18. هل لدى منظمتم سياسة خاصة بأمن المعلومات؟

- ☐ نعم  
☐ لا

19. إذا كان هناك سياسة خاصة بأمن المعلومات، هل منظماتكم ساهمت في تطبيقها؟

☐ نعم

☐ لا

☐ غير متأكد

20. هل لدى منظماتكم عمليات و إجراءات لتقييم المخاطر؟

☐ نعم

☐ لا

القسم الثالث – الجزء الأول : أمن المعلومات في المنظمة

21. هل لديكم إجراءات وأنظمة خاصة بإنشاء وإدارة حسابات المستخدمين؟

☐ نعم

☐ لا

22. هل لدى منظماتكم آلية خاصة بالنسخ الاحتياطي للبيانات وسياسة الاسترداد؟

☐ نعم

☐ لا

23. هل لدى منظماتكم خطة خاصة بتقارير الحوادث الأمنية للمعلومات ؟

☐ نعم

☐ لا

القسم الثالث – الجزء الثاني: أدوات أمن المعلومات / والمقاييس في المنظمة

24. ما هو رأيك عن مدى فعالية وأداء تقييم الثغرات والضعف في منظماتكم (6 = جيد جدا ؛ 5 = جيد ، 4 =

مقبول (متعادل) ؛ 3 = ضعيف ؛ 2 = ضعيف جدا ؛ 1 = غير موجود)

6 5 4 3 2 1

☐ تقييم الضعف



25. ما مدى الأمان والممارسة في عمليات منظماتكم في وضع كلمات السر؟

(6 = جيد جدا ؛ 5 = جيد ، 4 = مقبول (متعادل) ؛ 3 = ضعيف ؛ 2 = ضعيف جدا ؛ 1 = غير موجود)

6 5 4 3 2 1

☐ إعداد كلمة المرور

26. هل منظماتكم تقوم بتنفيذ أكثر من عامل للتوثق (إتاحة الوصول) داخل المنظمة (على سبيل المثال: البطاقة

الذكية ، كلمة مرور الخ)

☐ نعم

☐ لا

27. ما مدى الأمان الخاص بنظام جدار الحماية بمنظماتكم وذلك لحمايته من الوصول الغير مسموح به من خارج

المنظمة لخدمات المنظمة ؟

(6 = جيد جدا ؛ 5 = جيد ، 4 = مقبول (متعادل) ؛ 3 = ضعيف ؛ 2 = ضعيف جدا ؛ 1 = غير موجود)

6 5 4 3 2 1

☐ جدار الحماية الأمني

28. إذا كان لدى منظماتكم خدمة انترنت لاسلكية ، هل يتم تطبيق قواعد وإجراءات صارمة تفيد بأن استخدام الشبكة

اللاسلكية مقصور على موظفيها فقط ؟

(6 = صارمة للغاية ؛ 5 = صارمة ؛ 4 = محايد ؛ 3 = ضعيفة ؛ 2 = ضعيفة جدا ؛ 1 = غير موجود)

6 5 4 3 2 1

☐ الوصول للشبكة اللاسلكية

29. ما مدى صرامة منظماتكم وتقيدها في تصفح مواقع إنترنت معينة؟

(6 = صارمة للغاية ؛ 5 = صارمة ؛ 4 = مقبولة ؛ 3 = ضعيف ؛ 2 = ضعيف جدا ؛ 1 = غير موجود)

6 5 4 3 2 1

☐ تصفح مواقع على شبكة الانترنت

30. هل منظمتكم تقوم بتحديث أنظمة التشغيل أو البرامج المستخدمة لمواكبة آخر البرامج المصدرة؟

☐ يومي

☐ أسبوعي

☐ الشهري

☐ ربع سنوي

☐ سنويا

☐ أبدا

31. ما مدى قوة برنامج مكافحة الفيروسات المستخدم في منظمتكم؟

(6 = قوي جدا ؛ 5 = قوي ؛ 4 = مقبول ؛ 3 = ضعيف ؛ 2 = ضعيف جدا ؛ 1 = غير موجود)

6 5 4 3 2 1

☐ مدى قوة برنامج مكافحة الفيروسات

32. ما مدى قوة البرنامج الخاص بكشف التسلل والاختراق في المنظمة؟

(6 = قوي جدا ؛ 5 = قوي ؛ 4 = محايد ؛ 3 = ضعيف ؛ 2 = ضعيف جدا ؛ 1 = غير موجود)

6 5 4 3 2 1

☐ مدى قوة برنامج الكشف عن الاختراق

33. ما مدى فعالية التشفير الخاص بالبيانات المهمة في المنظمة؟

(6 = جيد جدا ؛ 5 = جيد ، 4 = محايد ؛ 3 = ضعيف ؛ 2 = ضعيف جدا ؛ 1 = غير موجود)

6 5 4 3 2 1

☐ تقنية تشفير البيانات

34. ما مدى مستوى الأمان المادي لغرفة الخادم (السيرفر) (أي رقم التعريف الشخصي ، القياسات الحيوية... الخ)؟

(6 = جيد جدا ؛ 5 = جيد ، 4 = مقبول (متعادل) ؛ 3 = ضعيف ؛ 2 = ضعيف جدا ؛ 1 = غير موجود)

6 5 4 3 2 1

☐ الأمان لغرفة خادم

35. ما مدى صرامة وتقييد منظمكم مع الموظفين في استخدام أجهزة الإدخال مثل محركات الأقراص المضغوطة ووسائط التخزينية القابلة للإزالة في منظمكم؟

(6 = صارمة للغاية ؛ 5 = صارمة ؛ 4 = مقبولة ؛ 3 = ضعيفة ؛ 2 = ضعيف جدا ؛ 1 = غير موجود)

6 5 4 3 2 1

☐ استخدام أجهزة نقل البيانات

36. هل تقوم منظمكم بتقديم عروض تدريبية للموظفين حول امن المعلومات؟

☐ نعم

☐ لا

37. هل تخطط للحصول على شهادات في أمن المعلومات؟

☐ نعم ، خلال الأشهر ال 12 القادمة ☐ نعم ، ولكن لست متأكدا متى سأقوم بذلك

☐ نعم ، خلال ال 3 سنوات القادمة ☐ لا ، إذهب الى السؤال رقم 15

☐ نعم ، خلال ال 10 سنوات القادمة

### القسم الثالث – الجزء الثالث: مخاطر أمن معلومات في منظمكم

38. هل سبق لنظام المعلومات في منظمكم بأن توقف في أي وقت مضى بسبب فيروسات الكمبيوتر؟

☐ نعم

☐ لا

☐ غير متأكد

39. هل سبق وأن تعرض موقع المنظمة على شبكة الانترنت لهجوم المخترقين؟

☐ نعم

☐ لا

☐ غير متأكد

☐ ليس لدينا موقع انترنت

40. هل سبق وأن تعرض نظام المعلومات الخاصة بالمؤسسة لهجمات القرصنة والمخترقين؟

- ☐ نعم
- ☐ لا
- ☐ غير متأكد

41. أي من المخاطر الأمنية التالية قد تعرضت له منظمتكم (يرجى اختيار كل ما ينطبق)

- ☐ الهجوم والحرمان من الخدمة الهجوم (DoS)
- ☐ التخريب الداخلي من قبل الموظفين
- ☐ سرقة بيانات العملاء أو المواطنين
- ☐ سرقة الأجهزة الحواسيب المكتبية أو المحمولة
- ☐ تخريب موقع المنظمة
- ☐ لا يوجد مخاطر
- ☐ غير متأكد
- ☐ أخرى ، يرجى تحديدها

42. المملكة العربية السعودية تمتاز بأنها مجتمعات قبلية ، ويمكن لهذه المجتمعات أن تكون عامل خطر لأمن المعلومات والخصوصية لا سيما مع حوادث الاعتداء أو النشر ، هل تعتقد أن هذا الخطر فعال :

- ☐ لا أوافق تماماً
- ☐ لا أوافق
- ☐ أوافق
- ☐ أوافق تماماً
- ☐ غير متوفر (لا ينطبق)

43. الناس في المجتمعات القبلية أحياناً يستطيعون الحصول على بعض المعلومات بطرق غير رسمية بواسطة أقاربهم أو من تربطهم بهم قرابة أو قبيلة:

- ☐ لا أوافق تماماً
- ☐ لا أوافق
- ☐ أوافق
- ☐ أوافق تماماً

☐ غير متوفر (لا ينطبق)

44. في المجتمعات القبلية، الناس في بعض الأحيان يستخدمون سلطتهم لتوظيف أقاربهم حتى ولو أن كانوا ليس لديهم المؤهلات ذات العلاقة للحصول على الوظيفة:

☐ لا أوافق تماماً

☐ لا أوافق

☐ أوافق

☐ أوافق تماماً

☐ غير متوفر (لا ينطبق)

45. في المملكة العربية السعودية النساء تقوم بارتداء النقاب (الغطاء الكامل للوجه) الذي يخفي هوية المرأة وبالتالي يصبح من الصعب جداً تعقب الحوادث التي يتسببون بها على المعلومات على سبيل المثال سرقة أجهزة تحمل معلومات مهمة أو وصول لمعلومات بدون إذن وصلاحيّة ، هل تعتقد أن هذا الخطر فعال :

☐ لا أوافق تماماً

☐ لا أوافق

☐ أوافق

☐ أوافق تماماً

☐ غير متوفر (لا ينطبق)

46. يمكن للمرأة في المملكة العربية السعودية استخدام بطاقة غيرها من النساء لأنه لا يوجد صور المطابقة التي قد تسبب مشكلة خطيرة:

☐ أعارض تماماً

☐ لا أوافق

☐ أوافق

☐ أوافق تماماً

☐ غير موجود (لا ينطبق)

47. في بعض الثقافات القبلية في المملكة العربية السعودية ، الناس ترفض إعطاء الإذن لنسائهم أن يكون لديهم هوية تمتاز بوجود صورة مطابقة لحاملها:

☐ أعارض تماماً

☐ لا أوافق

- ☐ أوافق
- ☐ أوافق تماماً
- ☐ غير موجود (لا ينطبق)

#### الجزء الرابع: الدعم والمفاضلة

48. من وجهة نظرك ما هي التحديات التي تواجه تطبيق معايير أمن المعلومات في منظمته؟ (يرجى إختيار ما ينطبق)

- ☐ ليس لديك ميزانية للقيام بذلك
- ☐ المعايير في غير اللغة العربية يصعب فهمها
- ☐ نقص في وجود المؤهلين في أمن المعلومات
- ☐ المعايير الدولية يصعب تطبيقها في العام
- ☐ لست متأكدا
- ☐ أخرى ، يرجى تحديدها

49. ما هي العقبات التي واجهتك أو ستواجهها في الحصول على شهادات في أمن المعلومات؟ (يرجى إختيار ما ينطبق)

- ☐ الرسوم العالية
- ☐ عدم وجود توجه وخطه واضحة
- ☐ عدم وجود وقت كافى للدراسة
- ☐ ضعف التوجيه بشأن التقدم الوظيفي
- ☐ عدم وجود توجه كافى للامتحانات
- ☐ لا ينطبق
- ☐ عدم القدرة على الحصول على معلومات بشأن الشهادة
- ☐ أخرى (يرجى التحديد)

50. ما هو نوع الاستفادة التي تهتمك لتجعلك تسعى للحصول على شهادة إضافية في أمن المعلومات في منظمته؟ (يرجى إختيار ما ينطبق)

- ☐ المورد المالي للشهادة (دورة / رسوم تدريب وإمتحان) من دون تعاقد
- ☐ المورد المالي للشهادة (دورة / رسوم تدريب وإمتحان) مع تعاقد
- ☐ تخصيص رسوم الامتحان دون تعاقد
- ☐ رسوم الاختبار مع تعاقد مضمون

- ☐ إجازة دراسية
- ☐ لا ينطبق
- ☐ أخرى (يرجى التحديد)

51. ما هو نوع العرض الذي يشدك للحصول على شهادة إضافية في أمن المعلومات؟ (يرجى إختيار ما ينطبق)

- ☐ خصم رسوم الاختبار
- ☐ فوائد مؤتمرات أمن تقنية المعلومات
- ☐ فوائد ناتجة عن الاجتماع بالمختصين وتكوين العلاقات
- ☐ فوائد خصم على المنتجات
- ☐ أخرى (يرجى التحديد)

## Appendix E: ISA Chi-Square Relationships Tests

### Gender \* ISA awareness and practices

Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Gender * Devices in secured place	462	100.0%	0	.0%	462	100.0%
Gender * Password Change	353	76.4%	109	23.6%	462	100.0%
Gender * Do you use private web mail for professional purposes?	462	100.0%	0	.0%	462	100.0%
Gender * React for Information	462	100.0%	0	.0%	462	100.0%
Gender * Data Backup	462	100.0%	0	.0%	462	100.0%
Gender * Information incidents report	462	100.0%	0	.0%	462	100.0%

### Gender \* Devices in secured place

		Devices in secured place					Total
		Yes, all the time	Sometimes	No	I don't have such devices	I do not know	
Gender	Male	52	59	45	2	6	164
	Female	82	140	60	5	11	298
Total		134	199	105	7	17	462



Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	6.245 <sup>a</sup>	4	.182
Likelihood Ratio	6.261	4	.180
Linear-by-Linear Association	.052	1	.820
N of Valid Cases	462		

a. 2 cells (20.0%) have expected count less than 5. The minimum expected count is 2.48.

## Gender \* Password Change

		Password Change						Total
		Daily	Weekly	Monthly	Quarterly	Annually	Never	
Gender	Male	4	5	14	14	15	85	137
	Female	4	3	15	20	27	147	216
Total		8	8	29	34	42	232	353

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	4.117 <sup>a</sup>	5	.533
Likelihood Ratio	4.023	5	.546
Linear-by-Linear Association	3.171	1	.075
N of Valid Cases	353		

a. 4 cells (33.3%) have expected count less than 5. The minimum expected count is 3.10.

## Gender \* Do you use private web mail for professional purposes?

		Do you use private web mail for professional purposes?				Total
		Never	Sometimes	Frequently	Everyday	
Gender	Male	34	77	44	9	164
	Female	115	138	36	9	298
Total		149	215	80	18	462

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	25.413 <sup>a</sup>	3	.000
Likelihood Ratio	25.427	3	.000
Linear-by-Linear Association	23.016	1	.000
N of Valid Cases	462		

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 6.39.

## Gender \* React for Information

		React for Information					Total
		I never answer	I answer the questions	I ask for details before answering	I ask a colleague or a friend for advice	I do not know	
Gender	Male	86	40	38	0	0	164
	Female	231	10	50	6	1	298
Total		317	50	88	6	1	462

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	59.064 <sup>a</sup>	4	.000
Likelihood Ratio	60.046	4	.000
Linear-by-Linear Association	10.057	1	.002
N of Valid Cases	462		

a. 4 cells (40.0%) have expected count less than 5. The minimum expected count is .35.

## Gender \* Data Backup

		Data Backup				Total
		Never	Sometimes	Frequently	Everyday	
Gender	Male	74	57	26	7	164
	Female	129	120	44	5	298
Total		203	177	70	12	462

**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	3.736 <sup>a</sup>	3	.291
Likelihood Ratio	3.598	3	.308
Linear-by-Linear Association	.325	1	.569
N of Valid Cases	462		

a. 1 cells (12.5%) have expected count less than 5. The minimum expected count is 4.26.

## Gender \* Information incidents report

		Information incidents report		Total
		No	Yes	
Gender	Male	128	36	164
	Female	244	54	298
Total		372	90	462

**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	.989 <sup>a</sup>	1	.320		
Continuity Correction <sup>b</sup>	.760	1	.383		
Likelihood Ratio	.977	1	.323		
Fisher's Exact Test				.328	.191
Linear-by-Linear Association	.987	1	.320		
N of Valid Cases	462				

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 31.95.

b. Computed only for a 2x2 table

**Case Processing Summary**

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Age * Devices in secured place	462	100.0%	0	.0%	462	100.0%
Age * Password Change	353	76.4%	109	23.6%	462	100.0%
Age * Do you use private web mail for professional purposes?	462	100.0%	0	.0%	462	100.0%
Age * React for Information	462	100.0%	0	.0%	462	100.0%
Age * Data Backup	462	100.0%	0	.0%	462	100.0%
Age * Information incidents report	462	100.0%	0	.0%	462	100.0%

**Age \* Devices in secured place**

		Devices in secured place					Total
		Yes, all the time	Sometimes	No	I don't have such devices	I do not know	
Age	18-22	14	30	13	3	5	65
	23-27	36	58	23	0	3	120
	28-32	40	55	37	2	3	137
	33-42	28	43	25	2	5	103
	43-59	16	11	7	0	1	35
	60-100	0	2	0	0	0	2
Total		134	199	105	7	17	462

**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	23.135 <sup>a</sup>	20	.282
Likelihood Ratio	23.905	20	.247
Linear-by-Linear Association	1.229	1	.268
N of Valid Cases	462		

a. 14 cells (46.7%) have expected count less than 5. The minimum expected count is .03.

### Age \* Password Change

		Password Change						Total
		Daily	Weekly	Monthly	Quarterly	Annually	Never	
Age	18-22	1	2	3	3	6	32	47
	23-27	1	1	7	8	12	63	92
	28-32	5	2	6	8	11	69	101
	33-42	0	1	8	9	8	52	78
	43-59	1	2	5	5	5	15	33
	60-100	0	0	0	1	0	1	2
Total		8	8	29	34	42	232	353

### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	21.887 <sup>a</sup>	25	.642
Likelihood Ratio	20.941	25	.696
Linear-by-Linear Association	2.794	1	.095
N of Valid Cases	353		

a. 21 cells (58.3%) have expected count less than 5. The minimum expected count is .05.

### Age \* Do you use private web mail for professional purposes?

		Do you use private web mail for professional purposes?				Total
		Never	Sometimes	Frequently	Everyday	
Age	18-22	21	33	10	1	65
	23-27	30	66	21	3	120
	28-32	52	53	24	8	137
	33-42	36	43	19	5	103
	43-59	9	19	6	1	35
	60-100	1	1	0	0	2
Total		149	215	80	18	462

**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	12.949 <sup>a</sup>	15	.606
Likelihood Ratio	13.646	15	.553
Linear-by-Linear Association	.038	1	.846
N of Valid Cases	462		

a. 8 cells (33.3%) have expected count less than 5. The minimum expected count is .08.

## Age \* React for Information

		React for Information					Total
		I never answer	I answer the questions	I ask for details before answering	I ask a colleague or a friend for advice	I do not know	
Age	18-22	48	4	11	2	0	65
	23-27	79	9	29	2	1	120
	28-32	100	16	20	1	0	137
	33-42	68	17	17	1	0	103
	43-59	21	4	10	0	0	35
	60-100	1	0	1	0	0	2
Total		317	50	88	6	1	462

**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	19.001 <sup>a</sup>	20	.522
Likelihood Ratio	18.619	20	.547
Linear-by-Linear Association	.056	1	.812
N of Valid Cases	462		

a. 16 cells (53.3%) have expected count less than 5. The minimum expected count is .00.

## Age \* Data Backup

		Data Backup				Total
		Never	Sometimes	Frequently	Everyday	
Age	18-22	34	22	8	1	65
	23-27	46	57	15	2	120
	28-32	61	51	21	4	137
	33-42	49	35	17	2	103
	43-59	13	10	9	3	35
	60-100	0	2	0	0	2
Total		203	177	70	12	462

## Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	19.522 <sup>a</sup>	15	.191
Likelihood Ratio	17.961	15	.265
Linear-by-Linear Association	2.906	1	.088
N of Valid Cases	462		

a. 9 cells (37.5%) have expected count less than 5. The minimum expected count is .05.

## Age \* Information incidents report

		Information incidents report		Total
		No	Yes	
Age	18-22	49	16	65
	23-27	93	27	120
	28-32	114	23	137
	33-42	90	13	103
	43-59	24	11	35
	60-100	2	0	2
Total		372	90	462

**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	9.182 <sup>a</sup>	5	.102
Likelihood Ratio	9.468	5	.092
Linear-by-Linear Association	1.044	1	.307
N of Valid Cases	462		

a. 2 cells (16.7%) have expected count less than 5. The minimum expected count is .39.

## Education \* ISA awareness and practices

**Case Processing Summary**

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Education * Devices in secured place	462	100.0%	0	.0%	462	100.0%
Education * Password Change	353	76.4%	109	23.6%	462	100.0%
Education * Do you use private web mail for professional purposes?	462	100.0%	0	.0%	462	100.0%
Education * React for Information	462	100.0%	0	.0%	462	100.0%
Education * Data Backup	462	100.0%	0	.0%	462	100.0%
Education * Information incidents report	462	100.0%	0	.0%	462	100.0%



## Education \* Devices in secured place

		Devices in secured place					Total
		Yes, all the time	Sometimes	No	I don't have such devices	I do not know	
Education	Doctoral Degree	4	2	1	1	0	8
	Master Degree	14	13	2	0	0	29
	Undergraduate Degree	60	116	52	4	6	238
	Diploma	17	18	18	0	3	56
	High School	34	44	25	1	7	111
	Intermediate School	5	6	6	1	1	19
	None	0	0	1	0	0	1
Total		134	199	105	7	17	462

### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	35.633 <sup>a</sup>	24	.060
Likelihood Ratio	33.388	24	.096
Linear-by-Linear Association	5.257	1	.022
N of Valid Cases	462		

a. 20 cells (57.1%) have expected count less than 5. The minimum expected count is .02.

## Education \* Password Change

		Password Change						Total
		Daily	Weekly	Monthly	Quarterly	Annually	Never	
Education	Doctoral Degree	0	1	0	2	1	4	8
	Master Degree	2	0	3	6	5	9	25
	Undergraduate Degree	3	4	11	14	26	123	181
	Diploma	2	0	7	7	2	23	41
	High School	1	2	5	5	7	64	84
	Intermediate School	0	1	3	0	1	8	13
	None	0	0	0	0	0	1	1
Total		8	8	29	34	42	232	353

### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	47.201 <sup>a</sup>	30	.024
Likelihood Ratio	43.776	30	.050
Linear-by-Linear Association	1.865	1	.172
N of Valid Cases	353		

a. 30 cells (71.4%) have expected count less than 5. The minimum expected count is .02.

## Education \* Do you use private web mail for professional purposes?

		Do you use private web mail for professional purposes?				Total
		Never	Sometimes	Frequently	Everyday	
Education	Doctoral Degree	2	4	1	1	8
	Master Degree	6	10	8	5	29
	Undergraduate Degree	77	115	41	5	238
	Diploma	16	26	12	2	56
	High School	43	50	14	4	111
	Intermediate School	5	9	4	1	19
	None	0	1	0	0	1
Total		149	215	80	18	462

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	26.387 <sup>a</sup>	18	.091
Likelihood Ratio	20.522	18	.304
Linear-by-Linear Association	2.767	1	.096
N of Valid Cases	462		

a. 13 cells (46.4%) have expected count less than 5. The minimum expected count is .04.

## Education \* React for Information

		React for Information					Total
		I never answer	I answer the questions	I ask for details before answering	I ask a colleague or a friend for advice	I do not know	
Education	Doctoral Degree	4	1	3	0	0	8
	Master Degree	19	2	8	0	0	29
	Undergraduate Degree	172	18	46	2	0	238
	Diploma	32	9	13	1	1	56
	High School	78	14	17	2	0	111
	Intermediate School	12	5	1	1	0	19
	None	0	1	0	0	0	1
Total		317	50	88	6	1	462

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	35.586 <sup>a</sup>	24	.060
Likelihood Ratio	27.618	24	.276
Linear-by-Linear Association	.069	1	.793
N of Valid Cases	462		

a. 22 cells (62.9%) have expected count less than 5. The minimum expected count is .00.

## Education \* Data Backup

		Data Backup				Total
		Never	Sometimes	Frequently	Everyday	
Education	Doctoral Degree	1	2	4	1	8
	Master Degree	9	11	8	1	29
	Undergraduate Degree	106	93	33	6	238
	Diploma	24	21	9	2	56
	High School	52	43	15	1	111
	Intermediate School	10	7	1	1	19
	None	1	0	0	0	1
Total		203	177	70	12	462

### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	21.328 <sup>a</sup>	18	.263
Likelihood Ratio	18.786	18	.405
Linear-by-Linear Association	6.432	1	.011
N of Valid Cases	462		

a. 14 cells (50.0%) have expected count less than 5. The minimum expected count is .03.

## Education \* Information incidents report

		Information incidents report		Total
		No	Yes	
Education	Doctoral Degree	5	3	8
	Master Degree	19	10	29
	Undergraduate Degree	197	41	238
	Diploma	41	15	56
	High School	93	18	111
	Intermediate School	16	3	19
	None	1	0	1
Total		372	90	462

**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	9.654 <sup>a</sup>	6	.140
Likelihood Ratio	8.928	6	.178
Linear-by-Linear Association	2.029	1	.154
N of Valid Cases	462		

a. 4 cells (28.6%) have expected count less than 5. The minimum expected count is .19.

## Organization Type \* ISA awareness and practices

**Case Processing Summary**

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Organization Type * Devices in secured place	462	100.0%	0	.0%	462	100.0%
Organization Type * Password Change	353	76.4%	109	23.6%	462	100.0%
Organization Type * Do you use private web mail for professional purposes?	462	100.0%	0	.0%	462	100.0%
Organization Type * React for Information	462	100.0%	0	.0%	462	100.0%
Organization Type * Data Backup	462	100.0%	0	.0%	462	100.0%
Organization Type * Information incidents report	462	100.0%	0	.0%	462	100.0%

## Organization Type \* Devices in secured place

		Devices in secured place					Total
		Yes, all the time	Sometimes	No	I don't have such devices	I do not know	
Organization Type	Government	57	82	35	3	6	183
	Private Sector	16	27	26	0	4	73
	Other	61	90	44	4	7	206
Total		134	199	105	7	17	462

### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	11.043 <sup>a</sup>	8	.199
Likelihood Ratio	11.458	8	.177
Linear-by-Linear Association	.192	1	.661
N of Valid Cases	462		

a. 4 cells (26.7%) have expected count less than 5. The minimum expected count is 1.11.

## Organization Type \* Password Change

		Password Change						Total
		Daily	Weekly	Monthly	Quarterly	Annually	Never	
Organization Type	Government	5	3	11	19	23	88	149
	Private Sector	1	2	8	6	5	35	57
	Other	2	3	10	9	14	109	147
Total		8	8	29	34	42	232	353

### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	13.596 <sup>a</sup>	10	.192
Likelihood Ratio	13.227	10	.211
Linear-by-Linear Association	4.376	1	.036
N of Valid Cases	353		

a. 7 cells (38.9%) have expected count less than 5. The minimum expected count is 1.29.

## Organization Type \* Do you use private web mail for professional purposes?

		Do you use private web mail for professional purposes?				Total
		Never	Sometimes	Frequently	Everyday	
Organization Type	Government	41	102	32	8	183
	Private Sector	15	25	29	4	73
	Other	93	88	19	6	206
Total		149	215	80	18	462

### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	55.619 <sup>a</sup>	6	.000
Likelihood Ratio	51.499	6	.000
Linear-by-Linear Association	18.057	1	.000
N of Valid Cases	462		

a. 1 cells (8.3%) have expected count less than 5. The minimum expected count is 2.84.

## Organization Type \* React for Information

		React for Information					Total
		I never answer	I answer the questions	I ask for details before answering	I ask a colleague or a friend for advice	I do not know	
Organization Type	Government	118	23	40	2	0	183
	Private Sector	37	21	13	1	1	73
	Other	162	6	35	3	0	206
Total		317	50	88	6	1	462

### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	47.745 <sup>a</sup>	8	.000
Likelihood Ratio	44.352	8	.000
Linear-by-Linear Association	4.634	1	.031
N of Valid Cases	462		

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	47.745 <sup>a</sup>	8	.000
Likelihood Ratio	44.352	8	.000
Linear-by-Linear Association	4.634	1	.031
N of Valid Cases	462		

a. 6 cells (40.0%) have expected count less than 5. The minimum expected count is .16.

## Organization Type \* Data Backup

		Data Backup				Total
		Never	Sometimes	Frequently	Everyday	
Organization Type	Government	62	80	34	7	183
	Private Sector	41	18	11	3	73
	Other	100	79	25	2	206
Total		203	177	70	12	462

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	19.098 <sup>a</sup>	6	.004
Likelihood Ratio	20.111	6	.003
Linear-by-Linear Association	10.706	1	.001
N of Valid Cases	462		

a. 2 cells (16.7%) have expected count less than 5. The minimum expected count is 1.90.

## Organization Type \* Information incidents report

		Information incidents report		Total
		No	Yes	
Organization Type	Government	139	44	183
	Private Sector	60	13	73
	Other	173	33	206
Total		372	90	462



Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	4.133 <sup>a</sup>	2	.127
Likelihood Ratio	4.086	2	.130
Linear-by-Linear Association	3.931	1	.047
N of Valid Cases	462		

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 14.22.

## Living Area \* ISA awareness and practices

Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Living area * Devices in secured place	462	100.0%	0	.0%	462	100.0%
Living area * Password Change	353	76.4%	109	23.6%	462	100.0%
Living area * Do you use private web mail for professional purposes?	462	100.0%	0	.0%	462	100.0%
Living area * React for Information	462	100.0%	0	.0%	462	100.0%
Living area * Data Backup	462	100.0%	0	.0%	462	100.0%
Living area * Information incidents report	462	100.0%	0	.0%	462	100.0%

## Living area \* Devices in secured place

	Devices in secured place					Total
	Yes, all the time	Sometimes	No	I don't have such devices	I do not know	
Living area Urban	125	182	97	6	15	425
Rural	9	17	8	1	2	37

		Devices in secured place					Total
		Yes, all the time	Sometimes	No	I don't have such devices	I do not know	
Living area	Urban	125	182	97	6	15	425
	Rural	9	17	8	1	2	37
Total		134	199	105	7	17	462

**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	1.102 <sup>a</sup>	4	.894
Likelihood Ratio	1.015	4	.908
Linear-by-Linear Association	.550	1	.458
N of Valid Cases	462		

a. 2 cells (20.0%) have expected count less than 5. The minimum expected count is .56.

## Living area \* Password Change

		Password Change						Total
		Daily	Weekly	Monthly	Quarterly	Annually	Never	
Living area	Urban	8	8	28	31	37	214	326
	Rural	0	0	1	3	5	18	27
Total		8	8	29	34	42	232	353

**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	3.197 <sup>a</sup>	5	.670
Likelihood Ratio	4.444	5	.487
Linear-by-Linear Association	1.086	1	.297
N of Valid Cases	353		

a. 5 cells (41.7%) have expected count less than 5. The minimum expected count is .61.

## Living area \* Do you use private web mail for professional purposes?

		Do you use private web mail for professional purposes?				Total
		Never	Sometimes	Frequently	Everyday	
Living area	Urban	135	198	74	18	425
	Rural	14	17	6	0	37
Total		149	215	80	18	462

### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	1.987 <sup>a</sup>	3	.575
Likelihood Ratio	3.407	3	.333
Linear-by-Linear Association	1.302	1	.254
N of Valid Cases	462		

a. 1 cells (12.5%) have expected count less than 5. The minimum expected count is 1.44.

## Living area \* React for Information

		React for Information					Total
		I never answer	I answer the questions	I ask for details before answering	I ask a colleague or a friend for advice	I do not know	
Living area	Urban	294	42	82	6	1	425
	Rural	23	8	6	0	0	37
Total		317	50	88	6	1	462

### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	5.357 <sup>a</sup>	4	.253
Likelihood Ratio	5.037	4	.284
Linear-by-Linear Association	.001	1	.978
N of Valid Cases	462		

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	5.357 <sup>a</sup>	4	.253
Likelihood Ratio	5.037	4	.284
Linear-by-Linear Association	.001	1	.978
N of Valid Cases	462		

a. 4 cells (40.0%) have expected count less than 5. The minimum expected count is .08.

## Living area \* Data Backup

		Data Backup				Total
		Never	Sometimes	Frequently	Everyday	
Living area	Urban	185	161	67	12	425
	Rural	18	16	3	0	37
Total		203	177	70	12	462

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	2.820 <sup>a</sup>	3	.420
Likelihood Ratio	4.011	3	.260
Linear-by-Linear Association	1.804	1	.179
N of Valid Cases	462		

a. 1 cells (12.5%) have expected count less than 5. The minimum expected count is .96.

## Living area \* Information incidents report

		Information incidents report		Total
		No	Yes	
Living area	Urban	339	86	425
	Rural	33	4	37
Total		372	90	462

**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	1.927 <sup>a</sup>	1	.165		
Continuity Correction <sup>b</sup>	1.373	1	.241		
Likelihood Ratio	2.191	1	.139		
Fisher's Exact Test				.198	.117
Linear-by-Linear Association	1.923	1	.166		
N of Valid Cases	462				

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 7.21.

b. Computed only for a 2x2 table

## Organization Sector \* Devices in secured place

		Devices in secured place					Total
		Yes, all the time	Sometime s	No	I don't have such devices	I do not know	
Organization	Military Sector	17	19	11	0	2	49
Sector	Banking & Finance	2	4	0	0	0	6
	Education	41	71	28	3	5	148
	Industry Services	1	1	3	0	0	5
	Trading & Contracting	4	7	8	0	1	20
	Information & Communication	1	0	0	0	0	1
	Health Services	5	9	5	1	0	20
	Food & Agriculture	2	2	1	0	0	5
	Transportation	1	2	1	0	0	4
	Energy	2	0	1	0	0	3
	Water	1	0	0	0	1	2
	Foreign Affairs Sector	0	2	0	0	0	2
	National Economy Sector	2	0	0	0	0	2
	Planning and Housing Sector	0	0	1	0	0	1
	Labour Sector	0	1	0	0	0	1
	Tourism	1	1	1	0	0	3
	Social Affairs Sector	1	0	4	0	1	6
	Justice Sector	1	3	1	1	0	6
	Islamic Affairs Sector	0	0	2	0	0	2
	Media Sector	1	2	2	0	1	6
	Other	51	75	36	2	6	170
Total		134	199	105	7	17	462

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	80.317 <sup>a</sup>	80	.469
Likelihood Ratio	69.278	80	.798
Linear-by-Linear Association	.201	1	.654
N of Valid Cases	462		

a. 90 cells (85.7%) have expected count less than 5. The minimum expected count is .02.

## Organization Sector \* Password Change

		Password Change						Total
		Daily	Weekly	Monthly	Quarterly	Annually	Never	
Organization Sector	Military Sector	1	2	5	6	2	26	42
	Banking & Finance	0	1	3	0	1	1	6
	Education	3	3	5	12	17	76	116
	Industry Services	0	0	1	1	0	2	4
	Trading & Contracting	0	1	0	4	2	10	17
	Information & Communication	1	0	0	0	0	0	1
	Health Services	0	0	1	0	3	8	12
	Food & Agriculture	1	0	1	1	0	0	3
	Transportation	0	0	1	0	0	3	4
	Energy	0	0	0	1	0	0	1
	Water	0	0	2	0	0	0	2
	National Economy Sector	0	0	0	0	1	1	2
	Planning and Housing Sector	0	0	0	0	0	1	1
	Labour Sector	0	0	0	0	1	0	1
	Tourism	0	0	0	1	0	1	2
	Social Affairs Sector	0	0	0	0	1	4	5
	Justice Sector	0	0	0	0	0	4	4
	Islamic Affairs Sector	0	0	0	0	0	2	2
	Media Sector	0	0	0	0	1	3	4
	Other	2	1	10	8	13	90	124
Total		8	8	29	34	42	232	353

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	163.296 <sup>a</sup>	95	.000
Likelihood Ratio	95.884	95	.455
Linear-by-Linear Association	5.438	1	.020
N of Valid Cases	353		

a. 109 cells (90.8%) have expected count less than 5. The minimum expected count is .02.

### Organization Sector \* Do you use private web mail for professional purposes?

		Do you use private web mail for professional purposes?				Total
		Never	Sometimes	Frequently	Everyday	
Organization Sector	Military Sector	10	30	6	3	49
	Banking & Finance	3	2	1	0	6
	Education	38	74	29	7	148
	Industry Services	1	1	3	0	5
	Trading & Contracting	1	11	7	1	20
	Information & Communication	0	1	0	0	1
	Health Services	2	12	5	1	20
	Food & Agriculture	3	1	1	0	5
	Transportation	0	3	1	0	4
	Energy	1	1	0	1	3
	Water	0	0	1	1	2
	Foreign Affairs Sector	1	0	1	0	2
	National Economy Sector	0	1	1	0	2
	Planning and Housing Sector	0	1	0	0	1
	Labour Sector	1	0	0	0	1
	Tourism	2	0	1	0	3
	Social Affairs Sector	0	2	4	0	6
	Justice Sector	1	2	3	0	6
	Islamic Affairs Sector	0	1	1	0	2
	Media Sector	2	2	2	0	6
	Other	83	70	13	4	170



		Do you use private web mail for professional purposes?				Total
		Never	Sometimes	Frequently	Everyday	
Organization	Military Sector	10	30	6	3	49
Sector	Banking & Finance	3	2	1	0	6
	Education	38	74	29	7	148
	Industry Services	1	1	3	0	5
	Trading & Contracting	1	11	7	1	20
	Information & Communication	0	1	0	0	1
	Health Services	2	12	5	1	20
	Food & Agriculture	3	1	1	0	5
	Transportation	0	3	1	0	4
	Energy	1	1	0	1	3
	Water	0	0	1	1	2
	Foreign Affairs Sector	1	0	1	0	2
	National Economy Sector	0	1	1	0	2
	Planning and Housing Sector	0	1	0	0	1
	Labour Sector	1	0	0	0	1
	Tourism	2	0	1	0	3
	Social Affairs Sector	0	2	4	0	6
	Justice Sector	1	2	3	0	6
	Islamic Affairs Sector	0	1	1	0	2
	Media Sector	2	2	2	0	6
	Other	83	70	13	4	170
Total		149	215	80	18	462

#### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	111.327 <sup>a</sup>	60	.000
Likelihood Ratio	105.848	60	.000
Linear-by-Linear Association	22.624	1	.000
N of Valid Cases	462		

a. 69 cells (82.1%) have expected count less than 5. The minimum expected count is .04.

## Organization Sector \* React for Information

		React for Information					Total
		I never answer	I answer the questions	I ask for details before answering	I ask a colleague or a friend for advice	I do not know	
Organization Sector	Military Sector	26	11	12	0	0	49
	Banking & Finance	2	0	4	0	0	6
	Education	108	10	27	3	0	148
	Industry Services	2	2	1	0	0	5
	Trading & Contracting	9	8	3	0	0	20
	Information & Communication	1	0	0	0	0	1
	Health Services	13	3	2	1	1	20
	Food & Agriculture	3	1	1	0	0	5
	Transportation	3	1	0	0	0	4
	Energy	3	0	0	0	0	3
	Water	1	1	0	0	0	2
	Foreign Affairs Sector	1	0	1	0	0	2
	National Economy Sector	1	1	0	0	0	2
	Planning and Housing Sector	0	0	1	0	0	1
	Labour Sector	0	0	1	0	0	1
	Tourism	2	0	1	0	0	3
	Social Affairs Sector	2	3	1	0	0	6
	Justice Sector	4	1	1	0	0	6
	Islamic Affairs Sector	0	1	1	0	0	2
	Media Sector	2	2	2	0	0	6
	Other	134	5	29	2	0	170
Total		317	50	88	6	1	462

### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	123.032 <sup>a</sup>	80	.001
Likelihood Ratio	94.199	80	.133
Linear-by-Linear Association	2.980	1	.084
N of Valid Cases	462		

a. 94 cells (89.5%) have expected count less than 5. The minimum expected count is .00.

### Organization Sector \* Data Backup

		Data Backup				Total
		Never	Sometimes	Frequently	Everyday	
Organization Sector	Military Sector	20	19	8	2	49
	Banking & Finance	1	2	1	2	6
	Education	58	60	26	4	148
	Industry Services	3	2	0	0	5
	Trading & Contracting	13	5	1	1	20
	Information & Communication	0	0	0	1	1
	Health Services	3	12	5	0	20
	Food & Agriculture	1	3	1	0	5
	Transportation	2	1	1	0	4
	Energy	0	0	3	0	3
	Water	1	0	1	0	2
	Foreign Affairs Sector	1	1	0	0	2
	National Economy Sector	1	0	1	0	2
	Planning and Housing Sector	1	0	0	0	1
	Labour Sector	0	1	0	0	1
	Tourism	2	1	0	0	3
	Social Affairs Sector	5	0	1	0	6
	Justice Sector	4	1	1	0	6
	Islamic Affairs Sector	2	0	0	0	2
	Media Sector	2	2	2	0	6
	Other	83	67	18	2	170

		Data Backup				Total
		Never	Sometimes	Frequently	Everyday	
Organization	Military Sector	20	19	8	2	49
Sector	Banking & Finance	1	2	1	2	6
	Education	58	60	26	4	148
	Industry Services	3	2	0	0	5
	Trading & Contracting	13	5	1	1	20
	Information & Communication	0	0	0	1	1
	Health Services	3	12	5	0	20
	Food & Agriculture	1	3	1	0	5
	Transportation	2	1	1	0	4
	Energy	0	0	3	0	3
	Water	1	0	1	0	2
	Foreign Affairs Sector	1	1	0	0	2
	National Economy Sector	1	0	1	0	2
	Planning and Housing Sector	1	0	0	0	1
	Labour Sector	0	1	0	0	1
	Tourism	2	1	0	0	3
	Social Affairs Sector	5	0	1	0	6
	Justice Sector	4	1	1	0	6
	Islamic Affairs Sector	2	0	0	0	2
	Media Sector	2	2	2	0	6
	Other	83	67	18	2	170
Total		203	177	70	12	462

#### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	119.479 <sup>a</sup>	60	.000
Likelihood Ratio	76.764	60	.071
Linear-by-Linear Association	7.802	1	.005
N of Valid Cases	462		

a. 71 cells (84.5%) have expected count less than 5. The minimum expected count is .03.

## Organization Sector \* Information incidents report

		Information incidents report		Total
		No	Yes	
Organization	Military Sector	37	12	49
Sector	Banking & Finance	1	5	6
	Education	117	31	148
	Industry Services	5	0	5
	Trading & Contracting	15	5	20
	Information & Communication	0	1	1
	Health Services	15	5	20
	Food & Agriculture	4	1	5
	Transportation	4	0	4
	Energy	2	1	3
	Water	2	0	2
	Foreign Affairs Sector	1	1	2
	National Economy Sector	1	1	2
	Planning and Housing Sector	1	0	1
	Labour Sector	1	0	1
	Tourism	2	1	3
	Social Affairs Sector	6	0	6
	Justice Sector	4	2	6
	Islamic Affairs Sector	2	0	2
	Media Sector	5	1	6
	Other	147	23	170
Total		372	90	462

### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	34.286 <sup>a</sup>	20	.024
Likelihood Ratio	32.790	20	.036
Linear-by-Linear Association	6.530	1	.011
N of Valid Cases	462		

a. 34 cells (81.0%) have expected count less than 5. The minimum expected count is .19.

## Device InfoSec level \* Participants Background

Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Gender * Device InfoSec level	462	100.0%	0	.0%	462	100.0%
Education * Device InfoSec level	462	100.0%	0	.0%	462	100.0%
Age * Device InfoSec level	462	100.0%	0	.0%	462	100.0%
Organization Type * Device InfoSec level	462	100.0%	0	.0%	462	100.0%
Organization Sector * Device InfoSec level	462	100.0%	0	.0%	462	100.0%
Living area * Device InfoSec level	462	100.0%	0	.0%	462	100.0%

## Gender \* Device InfoSec level

		Device InfoSec level						Total
		not exist	very poor	poor	neutral	good	very good	
Gender	Male	26	30	48	24	22	14	164
	Female	33	42	73	61	36	53	298
Total		59	72	121	85	58	67	462

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	12.356 <sup>a</sup>	5	.030
Likelihood Ratio	12.882	5	.025
Linear-by-Linear Association	8.607	1	.003
N of Valid Cases	462		

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 20.59.

## Education \* Device InfoSec level

		Device InfoSec level						Total
		not exist	very poor	poor	neutral	good	very good	
Education	Doctoral Degree	1	0	2	1	1	3	8
	Master Degree	2	7	8	5	5	2	29
	Undergraduate Degree	26	38	66	51	29	28	238
	Diploma	6	9	21	5	5	10	56
	High School	19	16	18	18	17	23	111
	Intermediate School	5	1	6	5	1	1	19
	None	0	1	0	0	0	0	1
Total		59	72	121	85	58	67	462

### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	40.272 <sup>a</sup>	30	.100
Likelihood Ratio	39.990	30	.105
Linear-by-Linear Association	.169	1	.681
N of Valid Cases	462		

a. 22 cells (52.4%) have expected count less than 5. The minimum expected count is .13.

## Age \* Device InfoSec level

		Device InfoSec level						Total
		not exist	very poor	poor	neutral	good	very good	
Age	18-22	12	5	9	7	12	20	65
	23-27	7	15	40	24	17	17	120
	28-32	17	28	30	32	16	14	137
	33-42	19	20	30	15	6	13	103
	43-59	3	4	12	6	7	3	35
	60-100	1	0	0	1	0	0	2
Total		59	72	121	85	58	67	462

**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	55.968 <sup>a</sup>	25	.000
Likelihood Ratio	55.952	25	.000
Linear-by-Linear Association	10.671	1	.001
N of Valid Cases	462		

a. 8 cells (22.2%) have expected count less than 5. The minimum expected count is .25.

**Organization Type \* Device InfoSec level**

	Device InfoSec level						Total
	not exist	very poor	poor	neutral	good	very good	
Organization Type Government	26	26	59	33	18	21	183
Private Sector	9	18	14	12	13	7	73
Other	24	28	48	40	27	39	206
Total	59	72	121	85	58	67	462

**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	17.870 <sup>a</sup>	10	.057
Likelihood Ratio	17.216	10	.070
Linear-by-Linear Association	5.217	1	.022
N of Valid Cases	462		

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 9.16.



# Organization Sector \* Device InfoSec level

		Device InfoSec level						Total
		not exist	very poor	poor	neutral	good	very good	
Organization Sector	Military Sector	7	10	12	9	7	4	49
	Banking & Finance	1	0	0	2	2	1	6
	Education	19	19	37	27	20	26	148
	Industry Services	2	0	2	1	0	0	5
	Trading & Contracting	0	6	4	5	3	2	20
	Information & Communication	0	0	0	1	0	0	1
	Health Services	3	2	5	4	5	1	20
	Food & Agriculture	2	2	0	0	1	0	5
	Transportation	3	0	1	0	0	0	4
	Energy	0	0	0	0	1	2	3
	Water	1	0	1	0	0	0	2
	Foreign Affairs Sector	0	0	1	0	1	0	2
	National Economy Sector	1	0	1	0	0	0	2
	Planning and Housing Sector	0	0	1	0	0	0	1
	Labour Sector	0	0	1	0	0	0	1
	Tourism	0	0	1	0	1	1	3
	Social Affairs Sector	1	2	2	0	0	1	6
	Justice Sector	0	4	2	0	0	0	6
	Islamic Affairs Sector	0	0	2	0	0	0	2
	Media Sector	0	2	2	0	0	2	6
	Other	19	25	46	36	17	27	170
Total		59	72	121	85	58	67	462

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	112.135 <sup>a</sup>	100	.192
Likelihood Ratio	115.643	100	.136
Linear-by-Linear Association	.002	1	.967
N of Valid Cases	462		

a. 106 cells (84.1%) have expected count less than 5. The minimum expected count is .13.

### Living area \* Device InfoSec level

		Device InfoSec level						Total
		not exist	very poor	poor	neutral	good	very good	
Living area	Urban	55	63	113	79	53	62	425
	Rural	4	9	8	6	5	5	37
Total		59	72	121	85	58	67	462

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	2.574 <sup>a</sup>	5	.765
Likelihood Ratio	2.338	5	.801
Linear-by-Linear Association	.106	1	.744
N of Valid Cases	462		

a. 2 cells (16.7%) have expected count less than 5. The minimum expected count is 4.65.

## Appendix F: InfoSec Chi-Square Relationships Tests

Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Nature of Organization * Does your organization apply any InfoSec standards	124	100.0%	0	.0%	124	100.0%
Nature of Organization * Data protection or InfoSec Law	124	100.0%	0	.0%	124	100.0%
Nature of Organization * InfoSec policy	124	100.0%	0	.0%	124	100.0%
Nature of Organization * Creating and Managing Users' Accounts	124	100.0%	0	.0%	124	100.0%
Nature of Organization * Data Backup and Recovery Policy	124	100.0%	0	.0%	124	100.0%
Nature of Organization * Risk Assessment Process	124	100.0%	0	.0%	124	100.0%
Nature of Organization * Incidents Reporting Plan	124	100.0%	0	.0%	124	100.0%
Nature of Organization * InfoSec Policy Enforcement	124	100.0%	0	.0%	124	100.0%
Organization's Sector * Does your organization apply any InfoSec standards	124	100.0%	0	.0%	124	100.0%
Organization's Sector * Data protection or InfoSec Law	124	100.0%	0	.0%	124	100.0%
Organization's Sector * InfoSec policy	124	100.0%	0	.0%	124	100.0%
Organization's Sector * Creating and Managing Users' Accounts	124	100.0%	0	.0%	124	100.0%
Organization's Sector * Data Backup and Recovery Policy	124	100.0%	0	.0%	124	100.0%
Organization's Sector * Risk Assessment Process	124	100.0%	0	.0%	124	100.0%
Organization's Sector * Incidents Reporting Plan	124	100.0%	0	.0%	124	100.0%
Organization's Sector * InfoSec Policy Enforcement	124	100.0%	0	.0%	124	100.0%
Size of your organization * Does your organization apply any InfoSec standards	124	100.0%	0	.0%	124	100.0%
Size of your organization * Data protection or InfoSec Law	124	100.0%	0	.0%	124	100.0%

Size of your organization * InfoSec policy	124	100.0%	0	.0%	124	100.0%
Size of your organization * Creating and Managing Users' Accounts	124	100.0%	0	.0%	124	100.0%
Size of your organization * Data Backup and Recovery Policy	124	100.0%	0	.0%	124	100.0%
Size of your organization * Risk Assessment Process	124	100.0%	0	.0%	124	100.0%
Size of your organization * Incidents Reporting Plan	124	100.0%	0	.0%	124	100.0%
Size of your organization * InfoSec Policy Enforcement	124	100.0%	0	.0%	124	100.0%
Number of years of the organization * Does your organization apply any InfoSec standards	124	100.0%	0	.0%	124	100.0%
Number of years of the organization * Data protection or InfoSec Law	124	100.0%	0	.0%	124	100.0%
Number of years of the organization * InfoSec policy	124	100.0%	0	.0%	124	100.0%
Number of years of the organization * Creating and Managing Users' Accounts	124	100.0%	0	.0%	124	100.0%
Number of years of the organization * Data Backup and Recovery Policy	124	100.0%	0	.0%	124	100.0%
Number of years of the organization * Risk Assessment Process	124	100.0%	0	.0%	124	100.0%
Number of years of the organization * Incidents Reporting Plan	124	100.0%	0	.0%	124	100.0%
Number of years of the organization * InfoSec Policy Enforcement	124	100.0%	0	.0%	124	100.0%

### Nature of Organization \* Does your organization apply any InfoSec standards

		Does your organization apply any InfoSec standards		Total
		Yes	No	
Nature of Organization	Public sector / Government agency	24	51	75
	Private sector / Business	18	25	43
	Non-for-profit organization	1	5	6
Total		43	81	124

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	2.076 <sup>a</sup>	2	.354
Likelihood Ratio	2.163	2	.339
Linear-by-Linear Association	.088	1	.766
N of Valid Cases	124		

a. 2 cells (33.3%) have expected count less than 5. The minimum expected count is 2.08.

### Nature of Organization \* Data protection or InfoSec Law

		Data protection or InfoSec Law		Total
		Yes	No	
Nature of Organization	Public sector / Government agency	22	53	75
	Private sector / Business	13	30	43
	Non-for-profit organization	1	5	6
Total		36	88	124

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	.479 <sup>a</sup>	2	.787
Likelihood Ratio	.529	2	.767
Linear-by-Linear Association	.106	1	.745
N of Valid Cases	124		

a. 2 cells (33.3%) have expected count less than 5. The minimum expected count is 1.74.

### Nature of Organization \* InfoSec policy

		InfoSec policy		Total
		Yes	No	
Nature of Organization	Public sector / Government agency	29	46	75
	Private sector / Business	19	24	43
	Non-for-profit organization	0	6	6
Total		48	76	124

**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	4.333 <sup>a</sup>	2	.115
Likelihood Ratio	6.410	2	.041
Linear-by-Linear Association	.515	1	.473
N of Valid Cases	124		

a. 2 cells (33.3%) have expected count less than 5. The minimum expected count is 2.32.

### Nature of Organization \* Creating and Managing Users' Accounts

		Creating and Managing Users' Accounts		Total
		Yes	No	
Nature of Organization	Public sector / Government agency	48	27	75
	Private sector / Business	30	13	43
	Non-for-profit organization	3	3	6
Total		81	43	124

**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	1.055 <sup>a</sup>	2	.590
Likelihood Ratio	1.033	2	.597
Linear-by-Linear Association	.001	1	.981
N of Valid Cases	124		

a. 2 cells (33.3%) have expected count less than 5. The minimum expected count is 2.08.

### Nature of Organization \* Data Backup and Recovery Policy

		Data Backup and Recovery Policy		Total
		Yes	No	
Nature of Organization	Public sector / Government agency	49	26	75
	Private sector / Business	27	16	43
	Non-for-profit organization	3	3	6
Total		79	45	124

**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	.589 <sup>a</sup>	2	.745
Likelihood Ratio	.571	2	.752
Linear-by-Linear Association	.419	1	.517
N of Valid Cases	124		

a. 2 cells (33.3%) have expected count less than 5. The minimum expected count is 2.18.

### Nature of Organization \* Risk Assessment Process

		Risk Assessment Process		Total
		Yes	No	
Nature of Organization	Public sector / Government agency	24	51	75
	Private sector / Business	17	26	43
	Non-for-profit organization	0	6	6
Total		41	83	124

**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	3.816 <sup>a</sup>	2	.148
Likelihood Ratio	5.646	2	.059
Linear-by-Linear Association	.148	1	.701
N of Valid Cases	124		

a. 2 cells (33.3%) have expected count less than 5. The minimum expected count is 1.98.

### Nature of Organization \* Incidents Reporting Plan

		Incidents Reporting Plan		Total
		Yes	No	
Nature of Organization	Public sector / Government agency	24	51	75
	Private sector / Business	15	28	43
	Non-for-profit organization	0	6	6
Total		39	85	124

**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	2.998 <sup>a</sup>	2	.223
Likelihood Ratio	4.773	2	.092
Linear-by-Linear Association	.570	1	.450
N of Valid Cases	124		

a. 2 cells (33.3%) have expected count less than 5. The minimum expected count is 1.89.

### Nature of Organization \* InfoSec Policy Enforcement

		InfoSec Policy Enforcement			Total
		Yes	No	Not Sure	
Nature of Organization	Public sector / Government agency	6	38	31	75
	Private sector / Business	4	22	17	43
	Non-for-profit organization	0	6	0	6
Total		10	66	48	124

**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	5.622 <sup>a</sup>	4	.229
Likelihood Ratio	7.912	4	.095
Linear-by-Linear Association	.925	1	.336
N of Valid Cases	124		

a. 4 cells (44.4%) have expected count less than 5. The minimum expected count is .48.



## Organization's Sector \* Does your organization apply any InfoSec standards

		Does your organization apply any InfoSec standards		Total
		Yes	No	
Organization's Sector	Military Sector	3	10	13
	Banking & Finance	9	2	11
	Education	8	21	29
	Industry Services	0	8	8
	Trading & Contracting	5	8	13
	Information & Communication	5	1	6
	Health Services	3	7	10
	Food & Agriculture	2	2	4
	Transportation	1	3	4
	Electricity	1	2	3
	Water	1	2	3
	Foreign Affairs Sector	1	0	1
	Labour Sector	0	2	2
	Tourism	1	3	4
	Social Affairs Sector	0	4	4
	Justice Sector	0	2	2
	Islamic Affairs Sector	0	2	2
	Media Sector	3	2	5
Total		43	81	124

### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	32.262 <sup>a</sup>	17	.014
Likelihood Ratio	37.569	17	.003
Linear-by-Linear Association	.703	1	.402
N of Valid Cases	124		

a. 29 cells (80.6%) have expected count less than 5. The minimum expected count is .35.

## Organization's Sector \* Data protection or InfoSec Law

		Data protection or InfoSec Law		Total
		Yes	No	
Organization's Sector	Military Sector	6	7	13
	Banking & Finance	8	3	11
	Education	7	22	29
	Industry Services	0	8	8
	Trading & Contracting	2	11	13
	Information & Communication	5	1	6
	Health Services	2	8	10
	Food & Agriculture	2	2	4
	Transportation	0	4	4
	Electricity	0	3	3
	Water	0	3	3
	Foreign Affairs Sector	1	0	1
	Labour Sector	0	2	2
	Tourism	1	3	4
	Social Affairs Sector	0	4	4
	Justice Sector	0	2	2
	Islamic Affairs Sector	0	2	2
	Media Sector	2	3	5
Total		36	88	124

### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	37.614 <sup>a</sup>	17	.003
Likelihood Ratio	43.164	17	.000
Linear-by-Linear Association	3.628	1	.057
N of Valid Cases	124		

a. 29 cells (80.6%) have expected count less than 5. The minimum expected count is .29.

## Organization's Sector \* InfoSec policy

		InfoSec policy		Total
		Yes	No	
Organization's Sector	Military Sector	5	8	13
	Banking & Finance	10	1	11
	Education	9	20	29
	Industry Services	1	7	8
	Trading & Contracting	3	10	13
	Information & Communication	6	0	6
	Health Services	3	7	10
	Food & Agriculture	2	2	4
	Transportation	1	3	4
	Electricity	1	2	3
	Water	1	2	3
	Foreign Affairs Sector	1	0	1
	Labour Sector	0	2	2
	Tourism	2	2	4
	Social Affairs Sector	0	4	4
	Justice Sector	1	1	2
	Islamic Affairs Sector	0	2	2
	Media Sector	2	3	5
	Total	48	76	124

### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	34.395 <sup>a</sup>	17	.007
Likelihood Ratio	40.553	17	.001
Linear-by-Linear Association	1.399	1	.237
N of Valid Cases	124		

a. 28 cells (77.8%) have expected count less than 5. The minimum expected count is .39.

## Organization's Sector \* Creating and Managing Users' Accounts

		Creating and Managing Users'			
		Accounts			
		Yes	No		Total
Organization's Sector	Military Sector	8	5	13	
	Banking & Finance	11	0	11	
	Education	19	10	29	
	Industry Services	3	5	8	
	Trading & Contracting	8	5	13	
	Information & Communication	5	1	6	
	Health Services	8	2	10	
	Food & Agriculture	3	1	4	
	Transportation	2	2	4	
	Electricity	1	2	3	
	Water	2	1	3	
	Foreign Affairs Sector	1	0	1	
	Labour Sector	2	0	2	
	Tourism	4	0	4	
	Social Affairs Sector	0	4	4	
	Justice Sector	1	1	2	
	Islamic Affairs Sector	1	1	2	
	Media Sector	2	3	5	
	Total		81	43	124

### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	25.567 <sup>a</sup>	17	.083
Likelihood Ratio	32.099	17	.015
Linear-by-Linear Association	2.247	1	.134
N of Valid Cases	124		

a. 29 cells (80.6%) have expected count less than 5. The minimum expected count is .35.

## Organization's Sector \* Data Backup and Recovery Policy

		Data Backup and Recovery Policy		Total
		Yes	No	
Organization's Sector	Military Sector	8	5	13
	Banking & Finance	11	0	11
	Education	17	12	29
	Industry Services	1	7	8
	Trading & Contracting	7	6	13
	Information & Communication	6	0	6
	Health Services	8	2	10
	Food & Agriculture	2	2	4
	Transportation	3	1	4
	Electricity	1	2	3
	Water	2	1	3
	Foreign Affairs Sector	1	0	1
	Labour Sector	2	0	2
	Tourism	4	0	4
	Social Affairs Sector	0	4	4
	Justice Sector	1	1	2
	Islamic Affairs Sector	1	1	2
	Media Sector	4	1	5
Total		79	45	124

### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	34.467 <sup>a</sup>	17	.007
Likelihood Ratio	43.586	17	.000
Linear-by-Linear Association	.008	1	.929
N of Valid Cases	124		

a. 29 cells (80.6%) have expected count less than 5. The minimum expected count is .36.

## Organization's Sector \* Risk Assessment Process

		Risk Assessment Process		Total
		Yes	No	
Organization's Sector	Military Sector	3	10	13
	Banking & Finance	11	0	11
	Education	7	22	29
	Industry Services	1	7	8
	Trading & Contracting	2	11	13
	Information & Communication	5	1	6
	Health Services	3	7	10
	Food & Agriculture	2	2	4
	Transportation	1	3	4
	Electricity	0	3	3
	Water	1	2	3
	Foreign Affairs Sector	1	0	1
	Labour Sector	0	2	2
	Tourism	3	1	4
	Social Affairs Sector	0	4	4
	Justice Sector	0	2	2
	Islamic Affairs Sector	0	2	2
	Media Sector	1	4	5
Total		41	83	124

### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	46.802 <sup>a</sup>	17	.000
Likelihood Ratio	53.109	17	.000
Linear-by-Linear Association	1.851	1	.174
N of Valid Cases	124		

a. 29 cells (80.6%) have expected count less than 5. The minimum expected count is .33.

### Organization's Sector \* Incidents Reporting Plan

		Incidents Reporting Plan		Total
		Yes	No	
Organization's Sector	Military Sector	5	8	13
	Banking & Finance	10	1	11
	Education	3	26	29
	Industry Services	1	7	8
	Trading & Contracting	2	11	13
	Information & Communication	5	1	6
	Health Services	3	7	10
	Food & Agriculture	2	2	4
	Transportation	1	3	4
	Electricity	0	3	3
	Water	1	2	3
	Foreign Affairs Sector	1	0	1
	Labour Sector	1	1	2
	Tourism	2	2	4
	Social Affairs Sector	0	4	4
	Justice Sector	0	2	2
	Islamic Affairs Sector	0	2	2
	Media Sector	2	3	5
	Total	39	85	124

### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	43.790 <sup>a</sup>	17	.000
Likelihood Ratio	47.380	17	.000
Linear-by-Linear Association	.445	1	.505
N of Valid Cases	124		

a. 29 cells (80.6%) have expected count less than 5. The minimum expected count is .31.

## Organization's Sector \* InfoSec Policy Enforcement

		InfoSec Policy Enforcement			Total
		Yes	No	Not Sure	
Organization's Sector	Military Sector	1	8	4	13
	Banking & Finance	4	1	6	11
	Education	2	12	15	29
	Industry Services	0	7	1	8
	Trading & Contracting	0	10	3	13
	Information & Communication	1	2	3	6
	Health Services	1	5	4	10
	Food & Agriculture	1	2	1	4
	Transportation	0	1	3	4
	Electricity	0	2	1	3
	Water	0	2	1	3
	Foreign Affairs Sector	0	1	0	1
	Labour Sector	0	2	0	2
	Tourism	0	3	1	4
	Social Affairs Sector	0	4	0	4
	Justice Sector	0	0	2	2
	Islamic Affairs Sector	0	2	0	2
	Media Sector	0	2	3	5
	Total	10	66	48	124

### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	44.204 <sup>a</sup>	34	.113
Likelihood Ratio	47.807	34	.058
Linear-by-Linear Association	.087	1	.769
N of Valid Cases	124		

a. 46 cells (85.2%) have expected count less than 5. The minimum expected count is .08.



**Size of your organization \* Does your organization apply any InfoSec standards**

		Does your organization apply any InfoSec standards		Total
		Yes	No	
Size of your organization	1 - 50 Employees	4	13	17
	51 – 100 Employees	3	22	25
	101 – 500 Employees	6	21	27
	501 - 1000 Employees	4	7	11
	More than 1000 Employees	26	18	44
Total		43	81	124

**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	20.048 <sup>a</sup>	4	.000
Likelihood Ratio	20.610	4	.000
Linear-by-Linear Association	15.887	1	.000
N of Valid Cases	124		

a. 1 cells (10.0%) have expected count less than 5. The minimum expected count is 3.81.

**Size of your organization \* Data protection or InfoSec Law**

		Data protection or InfoSec Law		Total
		Yes	No	
Size of your organization	1 - 50 Employees	6	11	17
	51 – 100 Employees	3	22	25
	101 – 500 Employees	5	22	27
	501 - 1000 Employees	4	7	11
	More than 1000 Employees	18	26	44
Total		36	88	124

**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	8.591 <sup>a</sup>	4	.072
Likelihood Ratio	9.155	4	.057
Linear-by-Linear Association	3.230	1	.072
N of Valid Cases	124		

a. 2 cells (20.0%) have expected count less than 5. The minimum expected count is 3.19.

### Size of your organization \* InfoSec policy

		InfoSec policy		Total
		Yes	No	
Size of your organization	1 - 50 Employees	5	12	17
	51 – 100 Employees	2	23	25
	101 – 500 Employees	7	20	27
	501 - 1000 Employees	4	7	11
	More than 1000 Employees	30	14	44
Total		48	76	124

**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	28.551 <sup>a</sup>	4	.000
Likelihood Ratio	30.620	4	.000
Linear-by-Linear Association	20.872	1	.000
N of Valid Cases	124		

a. 1 cells (10.0%) have expected count less than 5. The minimum expected count is 4.26.

### Size of your organization \* Creating and Managing Users' Accounts

		Creating and Managing Users' Accounts		Total
		Yes	No	
Size of your organization	1 - 50 Employees	10	7	17
	51 – 100 Employees	11	14	25
	101 – 500 Employees	15	12	27
	501 - 1000 Employees	9	2	11
	More than 1000 Employees	36	8	44
Total		81	43	124

#### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	13.079 <sup>a</sup>	4	.011
Likelihood Ratio	13.483	4	.009
Linear-by-Linear Association	9.342	1	.002
N of Valid Cases	124		

a. 1 cells (10.0%) have expected count less than 5. The minimum expected count is 3.81.

### Size of your organization \* Data Backup and Recovery Policy

		Data Backup and Recovery Policy		Total
		Yes	No	
Size of your organization	1 - 50 Employees	10	7	17
	51 – 100 Employees	8	17	25
	101 – 500 Employees	14	13	27
	501 - 1000 Employees	9	2	11
	More than 1000 Employees	38	6	44
Total		79	45	124

**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	24.017 <sup>a</sup>	4	.000
Likelihood Ratio	25.204	4	.000
Linear-by-Linear Association	15.955	1	.000
N of Valid Cases	124		

a. 1 cells (10.0%) have expected count less than 5. The minimum expected count is 3.99.

### Size of your organization \* Risk Assessment Process

		Risk Assessment Process		Total
		Yes	No	
Size of your organization	1 - 50 Employees	4	13	17
	51 – 100 Employees	0	25	25
	101 – 500 Employees	5	22	27
	501 - 1000 Employees	4	7	11
	More than 1000 Employees	28	16	44
Total		41	83	124

**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	34.264 <sup>a</sup>	4	.000
Likelihood Ratio	40.861	4	.000
Linear-by-Linear Association	25.228	1	.000
N of Valid Cases	124		

a. 1 cells (10.0%) have expected count less than 5. The minimum expected count is 3.64.

### Size of your organization \* Incidents Reporting Plan

		Incidents Reporting Plan		Total
		Yes	No	
Size of your organization	1 - 50 Employees	2	15	17
	51 – 100 Employees	2	23	25
	101 – 500 Employees	4	23	27
	501 - 1000 Employees	4	7	11
	More than 1000 Employees	27	17	44
Total		39	85	124

**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	31.283 <sup>a</sup>	4	.000
Likelihood Ratio	32.391	4	.000
Linear-by-Linear Association	26.767	1	.000
N of Valid Cases	124		

a. 1 cells (10.0%) have expected count less than 5. The minimum expected count is 3.46.

## Size of your organization \* InfoSec Policy Enforcement

		InfoSec Policy Enforcement			Total
		Yes	No	Not Sure	
Size of your organization	1 - 50 Employees	0	13	4	17
	51 – 100 Employees	0	19	6	25
	101 – 500 Employees	0	16	11	27
	501 - 1000 Employees	0	5	6	11
	More than 1000 Employees	10	13	21	44
Total		10	66	48	124

**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	31.364 <sup>a</sup>	8	.000
Likelihood Ratio	34.549	8	.000
Linear-by-Linear Association	.030	1	.862
N of Valid Cases	124		

a. 6 cells (40.0%) have expected count less than 5. The minimum expected count is .89.

### Number of years of the organization \* Does your organization apply any InfoSec standards

		Does your organization apply any InfoSec standards		Total
		Yes	No	
Number of years of the organization	Less than 1 year	1	2	3
	Between 1 to 5 years	2	15	17
	Between 6 to 10 years	7	16	23
	Between 11 to 20 years	4	12	16
	Between 21 to 30 years	5	10	15
	More than 30 years	24	26	50
Total		43	81	124

#### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	8.716 <sup>a</sup>	5	.121
Likelihood Ratio	9.340	5	.096
Linear-by-Linear Association	6.763	1	.009
N of Valid Cases	124		

a. 2 cells (16.7%) have expected count less than 5. The minimum expected count is 1.04.

### Number of years of the organization \* Data protection or InfoSec Law

		Data protection or InfoSec Law		Total
		Yes	No	
Number of years of the organization	Less than 1 year	1	2	3
	Between 1 to 5 years	3	14	17
	Between 6 to 10 years	8	15	23
	Between 11 to 20 years	4	12	16
	Between 21 to 30 years	6	9	15
	More than 30 years	14	36	50
Total		36	88	124

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	2.493 <sup>a</sup>	5	.777
Likelihood Ratio	2.542	5	.770
Linear-by-Linear Association	.118	1	.731
N of Valid Cases	124		

a. 5 cells (41.7%) have expected count less than 5. The minimum expected count is .87.

### Number of years of the organization \* InfoSec policy

		InfoSec policy		Total
		Yes	No	
Number of years of the organization	Less than 1 year	2	1	3
	Between 1 to 5 years	4	13	17
	Between 6 to 10 years	8	15	23
	Between 11 to 20 years	4	12	16
	Between 21 to 30 years	5	10	15
	More than 30 years	25	25	50
Total		48	76	124

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	6.926 <sup>a</sup>	5	.226
Likelihood Ratio	7.029	5	.219
Linear-by-Linear Association	2.625	1	.105
N of Valid Cases	124		

a. 2 cells (16.7%) have expected count less than 5. The minimum expected count is 1.16.

### Number of years of the organization \* Creating and Managing Users' Accounts

		Creating and Managing Users' Accounts		Total
		Yes	No	
Number of years of the organization	Less than 1 year	2	1	3
	Between 1 to 5 years	9	8	17
	Between 6 to 10 years	18	5	23
	Between 11 to 20 years	10	6	16
	Between 21 to 30 years	7	8	15
	More than 30 years	35	15	50
Total		81	43	124

#### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	5.696 <sup>a</sup>	5	.337
Likelihood Ratio	5.669	5	.340
Linear-by-Linear Association	.125	1	.724
N of Valid Cases	124		

a. 2 cells (16.7%) have expected count less than 5. The minimum expected count is 1.04.

### Number of years of the organization \* Data Backup and Recovery Policy

		Data Backup and Recovery Policy		Total
		Yes	No	
Number of years of the organization	Less than 1 year	3	0	3
	Between 1 to 5 years	8	9	17
	Between 6 to 10 years	13	10	23
	Between 11 to 20 years	9	7	16
	Between 21 to 30 years	7	8	15
	More than 30 years	39	11	50
Total		79	45	124



**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	10.947 <sup>a</sup>	5	.052
Likelihood Ratio	12.108	5	.033
Linear-by-Linear Association	3.407	1	.065
N of Valid Cases	124		

a. 2 cells (16.7%) have expected count less than 5. The minimum expected count is 1.09.

### Number of years of the organization \* Risk Assessment Process

		Risk Assessment Process		Total
		Yes	No	
Number of years of the organization	Less than 1 year	1	2	3
	Between 1 to 5 years	1	16	17
	Between 6 to 10 years	9	14	23
	Between 11 to 20 years	4	12	16
	Between 21 to 30 years	4	11	15
	More than 30 years	22	28	50
Total		41	83	124

**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	9.507 <sup>a</sup>	5	.090
Likelihood Ratio	11.190	5	.048
Linear-by-Linear Association	4.527	1	.033
N of Valid Cases	124		

a. 3 cells (25.0%) have expected count less than 5. The minimum expected count is .99.

### Number of years of the organization \* Incidents Reporting Plan

		Incidents Reporting Plan		Total
		Yes	No	
Number of years of the organization	Less than 1 year	1	2	3
	Between 1 to 5 years	1	16	17
	Between 6 to 10 years	8	15	23
	Between 11 to 20 years	3	13	16
	Between 21 to 30 years	4	11	15
	More than 30 years	22	28	50
Total		39	85	124

#### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	10.287 <sup>a</sup>	5	.068
Likelihood Ratio	11.843	5	.037
Linear-by-Linear Association	5.629	1	.018
N of Valid Cases	124		

a. 3 cells (25.0%) have expected count less than 5. The minimum expected count is .94.

### Number of years of the organization \* InfoSec Policy Enforcement

		InfoSec Policy Enforcement			Total
		Yes	No	Not Sure	
Number of years of the organization	Less than 1 year	0	1	2	3
	Between 1 to 5 years	0	12	5	17
	Between 6 to 10 years	1	14	8	23
	Between 11 to 20 years	1	10	5	16
	Between 21 to 30 years	2	9	4	15
	More than 30 years	6	20	24	50
Total		10	66	48	124

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	10.002 <sup>a</sup>	10	.440
Likelihood Ratio	11.494	10	.320
Linear-by-Linear Association	.000	1	.999
N of Valid Cases	124		

a. 8 cells (44.4%) have expected count less than 5. The minimum expected count is .24.

## Software packages updated/ Training \* Organizations Background

Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Nature of Organization * Operating systems and or software packages updated	124	100.0%	0	.0%	124	100.0%
Nature of Organization * InfoSec Training	124	100.0%	0	.0%	124	100.0%
Organization's Sector * Operating systems and or software packages updated	124	100.0%	0	.0%	124	100.0%
Organization's Sector * InfoSec Training	124	100.0%	0	.0%	124	100.0%
Size of your organization * Operating systems and or software packages updated	124	100.0%	0	.0%	124	100.0%
Size of your organization * InfoSec Training	124	100.0%	0	.0%	124	100.0%
Number of years of the organization * Operating systems and or software packages updated	124	100.0%	0	.0%	124	100.0%
Number of years of the organization * InfoSec Training	124	100.0%	0	.0%	124	100.0%

## Nature of Organization \* Operating systems and or software packages updated

		Operating systems and or software packages updated						Total
		Daily	Weekly	Monthly	Quarterly	Annually	Never	
Nature of Organization	Public sector / Government agency	1	2	3	6	37	26	75
	Private sector / Business	3	2	3	4	19	12	43
	Non-for-profit organization	0	0	1	0	1	4	6
Total		4	4	7	10	57	42	124

### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	9.496 <sup>a</sup>	10	.486
Likelihood Ratio	9.652	10	.471
Linear-by-Linear Association	.922	1	.337
N of Valid Cases	124		

a. 13 cells (72.2%) have expected count less than 5. The minimum expected count is .19.

## Nature of Organization \* InfoSec Training

		InfoSec Training		Total
		Yes	No	
Nature of Organization	Public sector / Government agency	20	55	75
	Private sector / Business	17	26	43
	Non-for-profit organization	0	6	6
Total		37	87	124

### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	4.843 <sup>a</sup>	2	.089
Likelihood Ratio	6.454	2	.040
Linear-by-Linear Association	.039	1	.844
N of Valid Cases	124		

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	4.843 <sup>a</sup>	2	.089
Likelihood Ratio	6.454	2	.040
Linear-by-Linear Association	.039	1	.844
N of Valid Cases	124		

a. 2 cells (33.3%) have expected count less than 5. The minimum expected count is 1.79.

### Organization's Sector \* Operating systems and or software packages updated

	Operating systems and or software packages updated						Total
	Daily	Weekly	Monthly	Quarterly	Annually	Never	
Organization's Sector							
Military Sector	0	1	0	0	8	4	13
Banking & Finance	2	2	0	4	3	0	11
Education	1	0	2	1	13	12	29
Industry Services	0	0	0	0	6	2	8
Trading & Contracting	0	0	0	0	6	7	13
Information & Communication	0	0	3	2	1	0	6
Health Services	0	1	1	2	3	3	10
Food & Agriculture	1	0	1	0	1	1	4
Transportation	0	0	0	1	2	1	4
Electricity	0	0	0	0	1	2	3
Water	0	0	0	0	2	1	3
Foreign Affairs Sector	0	0	0	0	1	0	1
Labour Sector	0	0	0	0	0	2	2
Tourism	0	0	0	0	4	0	4
Social Affairs Sector	0	0	0	0	0	4	4
Justice Sector	0	0	0	0	1	1	2
Islamic Affairs Sector	0	0	0	0	1	1	2
Media Sector	0	0	0	0	4	1	5
Total	4	4	7	10	57	42	124

**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	113.724 <sup>a</sup>	85	.020
Likelihood Ratio	100.254	85	.124
Linear-by-Linear Association	4.547	1	.033
N of Valid Cases	124		

a. 103 cells (95.4%) have expected count less than 5. The minimum expected count is .03.

**Organization's Sector \* InfoSec Training**

		InfoSec Training		Total
		Yes	No	
Organization's Sector	Military Sector	1	12	13
	Banking & Finance	11	0	11
	Education	7	22	29
	Industry Services	1	7	8
	Trading & Contracting	4	9	13
	Information & Communication	5	1	6
	Health Services	2	8	10
	Food & Agriculture	2	2	4
	Transportation	1	3	4
	Electricity	0	3	3
	Water	0	3	3
	Foreign Affairs Sector	1	0	1
	Labour Sector	0	2	2
	Tourism	1	3	4
	Social Affairs Sector	0	4	4
	Justice Sector	0	2	2
	Islamic Affairs Sector	0	2	2
	Media Sector	1	4	5
Total		37	87	124

**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	49.432 <sup>a</sup>	17	.000
Likelihood Ratio	55.010	17	.000
Linear-by-Linear Association	4.058	1	.044
N of Valid Cases	124		

a. 29 cells (80.6%) have expected count less than 5. The minimum expected count is .30.

### Size of your organization \* Operating systems and or software packages updated

	Operating systems and or software packages updated						Total
	Daily	Weekly	Monthly	Quarterly	Annually	Never	
Size of your organization 1 - 50 Employees	0	0	0	1	7	9	17
51 – 100 Employees	0	0	1	0	12	12	25
101 – 500 Employees	0	0	2	1	11	13	27
501 - 1000 Employees	0	0	0	1	10	0	11
More than 1000 Employees	4	4	4	7	17	8	44
Total	4	4	7	10	57	42	124

#### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	40.907 <sup>a</sup>	20	.004
Likelihood Ratio	48.521	20	.000
Linear-by-Linear Association	22.599	1	.000
N of Valid Cases	124		

a. 21 cells (70.0%) have expected count less than 5. The minimum expected count is .35.

### Size of your organization \* InfoSec Training

		InfoSec Training		Total
		Yes	No	
Size of your organization	1 - 50 Employees	2	15	17
	51 – 100 Employees	0	25	25
	101 – 500 Employees	5	22	27
	501 - 1000 Employees	5	6	11
	More than 1000 Employees	25	19	44
Total		37	87	124

#### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	31.517 <sup>a</sup>	4	.000
Likelihood Ratio	37.629	4	.000
Linear-by-Linear Association	27.071	1	.000
N of Valid Cases	124		

a. 1 cells (10.0%) have expected count less than 5. The minimum expected count is 3.28.

### Number of years of the organization \* Operating systems and or software packages updated

		Operating systems and or software packages updated						Total
		Daily	Weekly	Monthly	Quarterly	Annually	Never	
Number of years of the organization	Less than 1 year	0	0	0	0	2	1	3
	Between 1 to 5 years	0	0	1	0	6	10	17
	Between 6 to 10 years	1	1	3	3	8	7	23
	Between 11 to 20 years	0	0	1	0	11	4	16
	Between 21 to 30 years	0	1	1	1	6	6	15
	More than 30 years	3	2	1	6	24	14	50
Total		4	4	7	10	57	42	124

#### Chi-Square Tests



	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	20.592 <sup>a</sup>	25	.715
Likelihood Ratio	24.937	25	.466
Linear-by-Linear Association	1.976	1	.160
N of Valid Cases	124		

a. 26 cells (72.2%) have expected count less than 5. The minimum expected count is .10.

### Number of years of the organization \* InfoSec Training

		InfoSec Training		Total
		Yes	No	
Number of years of the organization	Less than 1 year	0	3	3
	Between 1 to 5 years	2	15	17
	Between 6 to 10 years	8	15	23
	Between 11 to 20 years	4	12	16
	Between 21 to 30 years	4	11	15
	More than 30 years	19	31	50
Total		37	87	124

#### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	6.039 <sup>a</sup>	5	.302
Likelihood Ratio	7.320	5	.198
Linear-by-Linear Association	3.573	1	.059
N of Valid Cases	124		

a. 4 cells (33.3%) have expected count less than 5. The minimum expected count is .90.

### Nature of Organization \* Two factors authentication implementation

		Two factors authentication implementation		Total
		Yes	No	
Nature of Organization	Public sector / Government agency	24	51	75
	Private sector / Business	15	28	43
	Non-for-profit organization	3	3	6
Total		42	82	124

**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	.834 <sup>a</sup>	2	.659
Likelihood Ratio	.797	2	.671
Linear-by-Linear Association	.584	1	.445
N of Valid Cases	124		

a. 2 cells (33.3%) have expected count less than 5. The minimum expected count is 2.03.

### Nature of Organization \* Vulnerability Assessment

		Vulnerability Assessment						Total
		Not Exist	Very Poor	Poor	Neutral	Good	Very Good	
Nature of Organization	Public sector / Government agency	9	14	25	16	9	2	75
	Private sector / Business	3	9	11	6	9	5	43
	Non-for-profit organization	2	2	0	1	0	1	6
Total		14	25	36	23	18	8	124

**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	13.985 <sup>a</sup>	10	.174
Likelihood Ratio	15.453	10	.116
Linear-by-Linear Association	.537	1	.464
N of Valid Cases	124		

a. 9 cells (50.0%) have expected count less than 5. The minimum expected count is .39.

### Nature of Organization \* Process/practice in setting passwords

		Process/practice in setting passwords						Total
		Not Exist	Very Poor	Poor	Neutral	Good	Very Good	
Nature of Organization	Public sector / Government agency	3	19	20	19	12	2	75
	Private sector / Business	0	8	16	3	9	7	43
	Non-for-profit organization	2	0	3	0	0	1	6
Total		5	27	39	22	21	10	124

#### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	32.734 <sup>a</sup>	10	.000
Likelihood Ratio	30.439	10	.001
Linear-by-Linear Association	.601	1	.438
N of Valid Cases	124		

a. 9 cells (50.0%) have expected count less than 5. The minimum expected count is .24.

### Nature of Organization \* Firewall system

		Firewall system						Total
		Not Exist	Very Poor	Poor	Neutral	Good	Very Good	
Nature of Organization	Public sector / Government agency	2	9	17	24	17	6	75
	Private sector / Business	0	5	8	13	8	9	43
	Non-for-profit organization	1	0	4	0	0	1	6
Total		3	14	29	37	25	16	124

#### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	19.067 <sup>a</sup>	10	.039
Likelihood Ratio	19.174	10	.038
Linear-by-Linear Association	.057	1	.811
N of Valid Cases	124		

a. 9 cells (50.0%) have expected count less than 5. The minimum expected count is .15.

### Nature of Organization \* wireless connection access restriction

		wireless connection access restriction						Total
		Not Exist	Very Poor	Poor	Neutral	Good	Very Good	
Nature of Organization	Public sector / Government agency	4	17	16	23	13	2	75
	Private sector / Business	0	8	11	8	8	8	43
	Non-for-profit organization	0	4	0	0	1	1	6
Total		4	29	27	31	22	11	124

#### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	20.909 <sup>a</sup>	10	.022
Likelihood Ratio	23.572	10	.009
Linear-by-Linear Association	1.434	1	.231
N of Valid Cases	124		

a. 9 cells (50.0%) have expected count less than 5. The minimum expected count is .19.

### Nature of Organization \* Internet sites access restriction

		Internet sites access restriction						Total
		Not Exist	Very Poor	Poor	Neutral	Good	Very Good	
Nature of Organization	Public sector / Government agency	2	19	23	16	15	0	75
	Private sector / Business	0	10	12	9	8	4	43
	Non-for-profit organization	0	4	0	0	2	0	6
Total		2	33	35	25	25	4	124

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	16.383 <sup>a</sup>	10	.089
Likelihood Ratio	19.770	10	.032
Linear-by-Linear Association	.369	1	.543
N of Valid Cases	124		

a. 10 cells (55.6%) have expected count less than 5. The minimum expected count is .10.

### Nature of Organization \* Anti-virus Software

		Anti-virus Software						Total
		Not Exist	Very Poor	Poor	Neutral	Good	Very Good	
Nature of Organization	Public sector / Government agency	2	6	5	30	26	6	75
	Private sector / Business	0	2	8	12	9	12	43
	Non-for-profit organization	1	0	3	1	1	0	6
Total		3	8	16	43	36	18	124

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	28.946 <sup>a</sup>	10	.001
Likelihood Ratio	25.550	10	.004
Linear-by-Linear Association	.125	1	.724
N of Valid Cases	124		

a. 10 cells (55.6%) have expected count less than 5. The minimum expected count is .15.

### Nature of Organization \* Intrusion detection software

		Intrusion detection software						Total
		Not Exist	Very Poor	Poor	Neutral	Good	Very Good	
Nature of Organization	Public sector / Government agency	8	14	24	17	10	2	75
	Private sector / Business	2	13	6	6	11	5	43
	Non-for-profit organization	1	2	1	1	0	1	6
Total		11	29	31	24	21	8	124

**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	16.118 <sup>a</sup>	10	.096
Likelihood Ratio	17.140	10	.071
Linear-by-Linear Association	.908	1	.341
N of Valid Cases	124		

a. 9 cells (50.0%) have expected count less than 5. The minimum expected count is .39.

### Nature of Organization \* Encryption

		Encryption						Total
		Not Exist	Very Poor	Poor	Neutral	Good	Very Good	
Nature of Organization	Public sector / Government agency	21	21	8	15	10	0	75
	Private sector / Business	15	7	2	7	8	4	43
	Non-for-profit organization	3	2	0	0	1	0	6
Total		39	30	10	22	19	4	124

**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	13.976 <sup>a</sup>	10	.174
Likelihood Ratio	16.505	10	.086
Linear-by-Linear Association	.036	1	.849
N of Valid Cases	124		

a. 9 cells (50.0%) have expected count less than 5. The minimum expected count is .19.

### Nature of Organization \* Server room physical security

		Server room physical security						Total
		Not Exist	Very Poor	Poor	Neutral	Good	Very Good	
Nature of Organization	Public sector / Government agency	4	8	6	14	20	23	75
	Private sector / Business	8	1	2	7	10	15	43
	Non-for-profit organization	3	0	0	1	0	2	6
Total		15	9	8	22	30	40	124

#### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	17.328 <sup>a</sup>	10	.067
Likelihood Ratio	17.354	10	.067
Linear-by-Linear Association	1.894	1	.169
N of Valid Cases	124		

a. 9 cells (50.0%) have expected count less than 5. The minimum expected count is .39.

### Nature of Organization \* Input devices restriction

		Input devices restriction						Total
		Not Exist	Very Poor	Poor	Neutral	Good	Very Good	
Nature of Organization	Public sector / Government agency	2	28	21	16	7	1	75
	Private sector / Business	1	14	9	6	9	4	43
	Non-for-profit organization	1	2	1	1	1	0	6
Total		4	44	31	23	17	5	124

#### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	12.541 <sup>a</sup>	10	.250
Likelihood Ratio	10.749	10	.377
Linear-by-Linear Association	1.248	1	.264
N of Valid Cases	124		

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	12.541 <sup>a</sup>	10	.250
Likelihood Ratio	10.749	10	.377
Linear-by-Linear Association	1.248	1	.264
N of Valid Cases	124		

a. 10 cells (55.6%) have expected count less than 5. The minimum expected count is .19.

### Organization's Sector \* Two factors authentication implementation

		Two factors authentication implementation		Total
		Yes	No	
Organization's Sector	Military Sector	2	11	13
	Banking & Finance	10	1	11
	Education	9	20	29
	Industry Services	1	7	8
	Trading & Contracting	0	13	13
	Information & Communication	5	1	6
	Health Services	3	7	10
	Food & Agriculture	2	2	4
	Transportation	1	3	4
	Electricity	0	3	3
	Water	1	2	3
	Foreign Affairs Sector	1	0	1
	Labour Sector	0	2	2
	Tourism	1	3	4
	Social Affairs Sector	0	4	4
	Justice Sector	1	1	2
	Islamic Affairs Sector	1	1	2
	Media Sector	4	1	5
Total		42	82	124



**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	45.498 <sup>a</sup>	17	.000
Likelihood Ratio	52.412	17	.000
Linear-by-Linear Association	.177	1	.674
N of Valid Cases	124		

a. 29 cells (80.6%) have expected count less than 5. The minimum expected count is .34.

**Organization's Sector \* Vulnerability Assessment**

		Vulnerability Assessment						Total
		Not Exist	Very Poor	Poor	Neutral	Good	Very Good	
Organization's Sector	Military Sector	2	1	5	4	1	0	13
	Banking & Finance	0	0	0	2	4	5	11
	Education	3	5	11	8	1	1	29
	Industry Services	2	1	3	1	1	0	8
	Trading & Contracting	0	4	5	2	2	0	13
	Information & Communication	0	0	1	0	4	1	6
	Health Services	2	3	2	1	1	1	10
	Food & Agriculture	0	1	1	0	2	0	4
	Transportation	0	0	3	1	0	0	4
	Electricity	0	0	2	1	0	0	3
	Water	1	1	0	1	0	0	3
	Foreign Affairs Sector	0	0	0	1	0	0	1
	Labour Sector	0	2	0	0	0	0	2
	Tourism	0	2	0	1	1	0	4
	Social Affairs Sector	1	2	1	0	0	0	4
	Justice Sector	1	1	0	0	0	0	2
	Islamic Affairs Sector	1	1	0	0	0	0	2
	Media Sector	1	1	2	0	1	0	5
	<b>Total</b>	<b>14</b>	<b>25</b>	<b>36</b>	<b>23</b>	<b>18</b>	<b>8</b>	<b>124</b>

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	117.798 <sup>a</sup>	85	.011
Likelihood Ratio	113.981	85	.020
Linear-by-Linear Association	9.283	1	.002
N of Valid Cases	124		

a. 105 cells (97.2%) have expected count less than 5. The minimum expected count is .06.

### Organization's Sector \* Process/practice in setting passwords

		Process/practice in setting passwords						Total
		Not Exist	Very Poor	Poor	Neutral	Good	Very Good	
Organization's Sector	Military Sector	2	2	3	6	0	0	13
	Banking & Finance	0	0	1	0	5	5	11
	Education	2	8	8	7	2	2	29
	Industry Services	0	3	3	1	1	0	8
	Trading & Contracting	0	3	6	2	2	0	13
	Information & Communication	0	0	1	0	5	0	6
	Health Services	0	3	2	2	2	1	10
	Food & Agriculture	0	1	1	0	0	2	4
	Transportation	0	1	2	0	1	0	4
	Electricity	0	0	3	0	0	0	3
	Water	0	1	2	0	0	0	3
	Foreign Affairs Sector	0	0	0	0	1	0	1
	Labour Sector	0	2	0	0	0	0	2
	Tourism	0	0	1	2	1	0	4
	Social Affairs Sector	1	1	2	0	0	0	4
	Justice Sector	0	1	0	1	0	0	2
	Islamic Affairs Sector	0	0	2	0	0	0	2
	Media Sector	0	1	2	1	1	0	5

		Process/practice in setting passwords						Total
		Not Exist	Very Poor	Poor	Neutral	Good	Very Good	
Organization's Sector	Military Sector	2	2	3	6	0	0	13
	Banking & Finance	0	0	1	0	5	5	11
	Education	2	8	8	7	2	2	29
	Industry Services	0	3	3	1	1	0	8
	Trading & Contracting	0	3	6	2	2	0	13
	Information & Communication	0	0	1	0	5	0	6
	Health Services	0	3	2	2	2	1	10
	Food & Agriculture	0	1	1	0	0	2	4
	Transportation	0	1	2	0	1	0	4
	Electricity	0	0	3	0	0	0	3
	Water	0	1	2	0	0	0	3
	Foreign Affairs Sector	0	0	0	0	1	0	1
	Labour Sector	0	2	0	0	0	0	2
	Tourism	0	0	1	2	1	0	4
	Social Affairs Sector	1	1	2	0	0	0	4
	Justice Sector	0	1	0	1	0	0	2
	Islamic Affairs Sector	0	0	2	0	0	0	2
	Media Sector	0	1	2	1	1	0	5
	Total	5	27	39	22	21	10	124

#### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	125.706 <sup>a</sup>	85	.003
Likelihood Ratio	115.987	85	.014
Linear-by-Linear Association	1.729	1	.189
N of Valid Cases	124		

a. 105 cells (97.2%) have expected count less than 5. The minimum expected count is .04.

## Organization's Sector \* Firewall system

		Firewall system						Total
		Not Exist	Very Poor	Poor	Neutral	Good	Very Good	
Organization's Sector	Military Sector	0	2	1	8	1	1	13
	Banking & Finance	0	0	0	1	2	8	11
	Education	3	4	5	10	4	3	29
	Industry Services	0	1	2	3	2	0	8
	Trading & Contracting	0	2	3	6	2	0	13
	Information & Communication	0	0	0	2	2	2	6
	Health Services	0	1	4	2	2	1	10
	Food & Agriculture	0	2	0	0	1	1	4
	Transportation	0	0	2	1	1	0	4
	Electricity	0	0	2	1	0	0	3
	Water	0	0	2	1	0	0	3
	Foreign Affairs Sector	0	0	0	0	1	0	1
	Labour Sector	0	1	1	0	0	0	2
	Tourism	0	0	0	1	3	0	4
	Social Affairs Sector	0	0	4	0	0	0	4
	Justice Sector	0	1	0	0	1	0	2
	Islamic Affairs Sector	0	0	2	0	0	0	2
	Media Sector	0	0	1	1	3	0	5
Total		3	14	29	37	25	16	124

### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	128.917 <sup>a</sup>	85	.002
Likelihood Ratio	117.014	85	.012
Linear-by-Linear Association	1.164	1	.281
N of Valid Cases	124		

a. 105 cells (97.2%) have expected count less than 5. The minimum expected count is .02.

### Organization's Sector \* wireless connection access restriction

		wireless connection access restriction						Total
		Not Exist	Very Poor	Poor	Neutral	Good	Very Good	
Organization's Sector	Military Sector	0	3	3	6	1	0	13
	Banking & Finance	0	0	0	2	4	5	11
	Education	2	7	2	10	6	2	29
	Industry Services	0	1	4	1	1	1	8
	Trading & Contracting	0	4	4	2	3	0	13
	Information & Communication	0	0	0	2	4	0	6
	Health Services	0	3	4	1	1	1	10
	Food & Agriculture	0	2	0	0	0	2	4
	Transportation	0	0	3	1	0	0	4
	Electricity	0	0	2	1	0	0	3
	Water	1	0	2	0	0	0	3
	Foreign Affairs Sector	0	0	0	0	1	0	1
	Labour Sector	0	2	0	0	0	0	2
	Tourism	0	1	0	2	1	0	4
	Social Affairs Sector	0	3	1	0	0	0	4
	Justice Sector	1	1	0	0	0	0	2
	Islamic Affairs Sector	0	2	0	0	0	0	2
	Media Sector	0	0	2	3	0	0	5
Total		4	29	27	31	22	11	124

#### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	142.062 <sup>a</sup>	85	.000
Likelihood Ratio	129.070	85	.001
Linear-by-Linear Association	9.223	1	.002
N of Valid Cases	124		

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	142.062 <sup>a</sup>	85	.000
Likelihood Ratio	129.070	85	.001
Linear-by-Linear Association	9.223	1	.002
N of Valid Cases	124		

a. 104 cells (96.3%) have expected count less than 5. The minimum expected count is .03.

### Organization's Sector \* Internet sites access restriction

		Internet sites access restriction						Total
		Not Exist	Very Poor	Poor	Neutral	Good	Very Good	
Organization's Sector	Military Sector	0	3	3	6	1	0	13
	Banking & Finance	0	0	1	1	6	3	11
	Education	2	9	6	8	4	0	29
	Industry Services	0	2	4	1	1	0	8
	Trading & Contracting	0	5	3	3	2	0	13
	Information & Communication	0	0	0	3	3	0	6
	Health Services	0	4	4	0	2	0	10
	Food & Agriculture	0	1	1	0	1	1	4
	Transportation	0	1	2	1	0	0	4
	Electricity	0	0	3	0	0	0	3
	Water	0	0	2	1	0	0	3
	Foreign Affairs Sector	0	0	0	0	1	0	1
	Labour Sector	0	2	0	0	0	0	2
	Tourism	0	1	1	1	1	0	4
	Social Affairs Sector	0	3	1	0	0	0	4
	Justice Sector	0	1	0	0	1	0	2
	Islamic Affairs Sector	0	1	0	0	1	0	2
	Media Sector	0	0	4	0	1	0	5
	Total	2	33	35	25	25	4	124

**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	108.767 <sup>a</sup>	85	.042
Likelihood Ratio	103.424	85	.085
Linear-by-Linear Association	1.958	1	.162
N of Valid Cases	124		

a. 104 cells (96.3%) have expected count less than 5. The minimum expected count is .02.

**Organization's Sector \* Anti-virus Software**

		Anti-virus Software						Total
		Not Exist	Very Poor	Poor	Neutral	Good	Very Good	
Organization's Sector	Military Sector	0	1	1	5	6	0	13
	Banking & Finance	0	0	0	0	3	8	11
	Education	3	2	3	12	8	1	29
	Industry Services	0	1	1	4	2	0	8
	Trading & Contracting	0	1	3	4	3	2	13
	Information & Communication	0	0	0	0	2	4	6
	Health Services	0	1	2	4	2	1	10
	Food & Agriculture	0	0	1	1	2	0	4
	Transportation	0	0	1	1	2	0	4
	Electricity	0	0	0	3	0	0	3
	Water	0	0	0	3	0	0	3
	Foreign Affairs Sector	0	0	0	0	0	1	1
	Labour Sector	0	1	0	1	0	0	2
	Tourism	0	0	0	1	2	1	4
	Social Affairs Sector	0	0	3	1	0	0	4
	Justice Sector	0	1	0	0	1	0	2
	Islamic Affairs Sector	0	0	1	1	0	0	2
	Media Sector	0	0	0	2	3	0	5

		Anti-virus Software						Total
		Not Exist	Very Poor	Poor	Neutral	Good	Very Good	
Organization's Sector	Military Sector	0	1	1	5	6	0	13
	Banking & Finance	0	0	0	0	3	8	11
	Education	3	2	3	12	8	1	29
	Industry Services	0	1	1	4	2	0	8
	Trading & Contracting	0	1	3	4	3	2	13
	Information & Communication	0	0	0	0	2	4	6
	Health Services	0	1	2	4	2	1	10
	Food & Agriculture	0	0	1	1	2	0	4
	Transportation	0	0	1	1	2	0	4
	Electricity	0	0	0	3	0	0	3
	Water	0	0	0	3	0	0	3
	Foreign Affairs Sector	0	0	0	0	0	1	1
	Labour Sector	0	1	0	1	0	0	2
	Tourism	0	0	0	1	2	1	4
	Social Affairs Sector	0	0	3	1	0	0	4
	Justice Sector	0	1	0	0	1	0	2
	Islamic Affairs Sector	0	0	1	1	0	0	2
	Media Sector	0	0	0	2	3	0	5
Total		3	8	16	43	36	18	124

#### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	125.236 <sup>a</sup>	85	.003
Likelihood Ratio	112.287	85	.025
Linear-by-Linear Association	.816	1	.366
N of Valid Cases	124		

a. 106 cells (98.1%) have expected count less than 5. The minimum expected count is .02.



## Organization's Sector \* Intrusion detection software

		Intrusion detection software						Total
		Not Exist	Very Poor	Poor	Neutral	Good	Very Good	
Organization's Sector	Military Sector	1	4	3	4	1	0	13
	Banking & Finance	0	0	0	2	5	4	11
	Education	5	6	8	7	2	1	29
	Industry Services	1	1	3	3	0	0	8
	Trading & Contracting	0	5	5	1	2	0	13
	Information & Communication	0	0	0	1	3	2	6
	Health Services	2	2	4	0	1	1	10
	Food & Agriculture	0	2	0	0	2	0	4
	Transportation	0	1	2	0	1	0	4
	Electricity	0	1	1	1	0	0	3
	Water	1	1	0	1	0	0	3
	Foreign Affairs Sector	0	0	0	0	1	0	1
	Labour Sector	0	2	0	0	0	0	2
	Tourism	0	1	0	2	1	0	4
	Social Affairs Sector	0	2	2	0	0	0	4
	Justice Sector	1	0	0	0	1	0	2
	Islamic Affairs Sector	0	1	0	1	0	0	2
	Media Sector	0	0	3	1	1	0	5
Total		11	29	31	24	21	8	124

### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	109.966 <sup>a</sup>	85	.036
Likelihood Ratio	116.319	85	.014
Linear-by-Linear Association	.692	1	.405
N of Valid Cases	124		

a. 105 cells (97.2%) have expected count less than 5. The minimum expected count is .06.

## Organization's Sector \* Encryption

		Encryption						Total
		Not Exist	Very Poor	Poor	Neutral	Good	Very Good	
Organization's Sector	Military Sector	2	6	1	1	3	0	13
	Banking & Finance	0	0	0	3	4	4	11
	Education	10	8	3	6	2	0	29
	Industry Services	4	3	0	1	0	0	8
	Trading & Contracting	5	3	1	4	0	0	13
	Information & Communication	0	1	0	1	4	0	6
	Health Services	3	3	2	1	1	0	10
	Food & Agriculture	2	0	0	0	2	0	4
	Transportation	2	1	0	1	0	0	4
	Electricity	1	0	1	1	0	0	3
	Water	2	1	0	0	0	0	3
	Foreign Affairs Sector	0	0	0	0	1	0	1
	Labour Sector	2	0	0	0	0	0	2
	Tourism	0	1	1	1	1	0	4
	Social Affairs Sector	2	2	0	0	0	0	4
	Justice Sector	1	0	0	1	0	0	2
	Islamic Affairs Sector	2	0	0	0	0	0	2
	Media Sector	1	1	1	1	1	0	5
Total		39	30	10	22	19	4	124

### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	118.257 <sup>a</sup>	85	.010
Likelihood Ratio	106.860	85	.055
Linear-by-Linear Association	2.667	1	.102
N of Valid Cases	124		

a. 105 cells (97.2%) have expected count less than 5. The minimum expected count is .03.

## Organization's Sector \* Server room physical security

		Server room physical security						Total
		Not Exist	Very Poor	Poor	Neutral	Good	Very Good	
Organization's Sector	Military Sector	0	2	2	2	1	6	13
	Banking & Finance	0	0	0	0	4	7	11
	Education	2	5	2	7	6	7	29
	Industry Services	1	1	1	1	4	0	8
	Trading & Contracting	2	0	1	5	2	3	13
	Information & Communication	0	0	0	0	1	5	6
	Health Services	1	0	1	0	4	4	10
	Food & Agriculture	2	0	0	0	0	2	4
	Transportation	1	0	0	1	2	0	4
	Electricity	0	0	0	1	2	0	3
	Water	2	0	0	0	1	0	3
	Foreign Affairs Sector	0	0	0	0	1	0	1
	Labour Sector	0	0	1	1	0	0	2
	Tourism	0	0	0	2	1	1	4
	Social Affairs Sector	3	0	0	1	0	0	4
	Justice Sector	0	1	0	0	0	1	2
	Islamic Affairs Sector	1	0	0	0	0	1	2
	Media Sector	0	0	0	1	1	3	5
	Total	15	9	8	22	30	40	124

### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	112.305 <sup>a</sup>	85	.025
Likelihood Ratio	115.158	85	.016
Linear-by-Linear Association	1.698	1	.193
N of Valid Cases	124		

a. 105 cells (97.2%) have expected count less than 5. The minimum expected count is .06.

## Organization's Sector \* Input devices restriction

		Input devices restriction						Total
		Not Exist	Very Poor	Poor	Neutral	Good	Very Good	
Organization's Sector	Military Sector	0	4	3	5	1	0	13
	Banking & Finance	0	0	1	3	4	3	11
	Education	2	12	8	4	2	1	29
	Industry Services	1	3	2	2	0	0	8
	Trading & Contracting	0	7	2	2	2	0	13
	Information & Communication	0	0	1	2	3	0	6
	Health Services	0	6	1	1	2	0	10
	Food & Agriculture	0	2	0	0	1	1	4
	Transportation	0	1	2	1	0	0	4
	Electricity	0	0	3	0	0	0	3
	Water	1	1	1	0	0	0	3
	Foreign Affairs Sector	0	0	0	0	1	0	1
	Labour Sector	0	2	0	0	0	0	2
	Tourism	0	1	1	1	1	0	4
	Social Affairs Sector	0	2	2	0	0	0	4
	Justice Sector	0	2	0	0	0	0	2
	Islamic Affairs Sector	0	1	0	1	0	0	2
	Media Sector	0	0	4	1	0	0	5
Total		4	44	31	23	17	5	124

### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	107.221 <sup>a</sup>	85	.052
Likelihood Ratio	100.800	85	.116
Linear-by-Linear Association	2.169	1	.141
N of Valid Cases	124		

a. 105 cells (97.2%) have expected count less than 5. The minimum expected count is .03.

## Size of your organization \* Two factors authentication implementation

		Two factors authentication implementation		Total
		Yes	No	
Size of your organization	1 - 50 Employees	6	11	17
	51 – 100 Employees	1	24	25
	101 – 500 Employees	6	21	27
	501 - 1000 Employees	4	7	11
	More than 1000 Employees	25	19	44
Total		42	82	124

### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	21.985 <sup>a</sup>	4	.000
Likelihood Ratio	25.091	4	.000
Linear-by-Linear Association	12.495	1	.000
N of Valid Cases	124		

a. 1 cells (10.0%) have expected count less than 5. The minimum expected count is 3.73.

## Size of your organization \* Vulnerability Assessment

		Vulnerability Assessment						Total
		Not Exist	Very Poor	Poor	Neutral	Good	Very Good	
Size of your organization	1 - 50 Employees	4	6	3	2	2	0	17
	51 – 100 Employees	2	7	13	3	0	0	25
	101 – 500 Employees	2	8	9	6	2	0	27
	501 - 1000 Employees	0	1	6	1	3	0	11
	More than 1000 Employees	6	3	5	11	11	8	44
Total		14	25	36	23	18	8	124

**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	51.913 <sup>a</sup>	20	.000
Likelihood Ratio	58.961	20	.000
Linear-by-Linear Association	20.818	1	.000
N of Valid Cases	124		

a. 21 cells (70.0%) have expected count less than 5. The minimum expected count is .71.

### Size of your organization \* Process/practice in setting passwords

		Process/practice in setting passwords						Total
		Not Exist	Very Poor	Poor	Neutral	Good	Very Good	
Size of your organization	1 - 50 Employees	0	6	6	4	1	0	17
	51 – 100 Employees	0	10	10	4	1	0	25
	101 – 500 Employees	3	4	11	5	2	2	27
	501 - 1000 Employees	0	2	4	1	4	0	11
	More than 1000 Employees	2	5	8	8	13	8	44
Total		5	27	39	22	21	10	124

**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	40.009 <sup>a</sup>	20	.005
Likelihood Ratio	44.348	20	.001
Linear-by-Linear Association	17.441	1	.000
N of Valid Cases	124		

a. 21 cells (70.0%) have expected count less than 5. The minimum expected count is .44.

### Size of your organization \* Firewall system

		Firewall system						Total
		Not Exist	Very Poor	Poor	Neutral	Good	Very Good	
Size of your organization	1 - 50 Employees	0	5	6	4	1	1	17
	51 – 100 Employees	0	6	8	10	0	1	25
	101 – 500 Employees	2	1	9	9	5	1	27
	501 - 1000 Employees	0	0	2	4	5	0	11
	More than 1000 Employees	1	2	4	10	14	13	44
Total		3	14	29	37	25	16	124

#### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	54.091 <sup>a</sup>	20	.000
Likelihood Ratio	59.687	20	.000
Linear-by-Linear Association	26.762	1	.000
N of Valid Cases	124		

a. 19 cells (63.3%) have expected count less than 5. The minimum expected count is .27.

### Size of your organization \* wireless connection access restriction

		wireless connection access restriction						Total
		Not Exist	Very Poor	Poor	Neutral	Good	Very Good	
Size of your organization	1 - 50 Employees	0	10	2	2	1	2	17
	51 – 100 Employees	0	9	7	7	1	1	25
	101 – 500 Employees	1	4	8	11	2	1	27
	501 - 1000 Employees	0	1	5	3	2	0	11
	More than 1000 Employees	3	5	5	8	16	7	44
Total		4	29	27	31	22	11	124

**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	49.970 <sup>a</sup>	20	.000
Likelihood Ratio	50.152	20	.000
Linear-by-Linear Association	13.287	1	.000
N of Valid Cases	124		

a. 20 cells (66.7%) have expected count less than 5. The minimum expected count is .35.

### Size of your organization \* Internet sites access restriction

		Internet sites access restriction						Total
		Not Exist	Very Poor	Poor	Neutral	Good	Very Good	
Size of your organization	1 - 50 Employees	0	9	4	1	3	0	17
	51 – 100 Employees	0	8	9	6	2	0	25
	101 – 500 Employees	1	8	9	6	3	0	27
	501 - 1000 Employees	0	2	5	2	2	0	11
	More than 1000 Employees	1	6	8	10	15	4	44
Total		2	33	35	25	25	4	124

**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	29.860 <sup>a</sup>	20	.072
Likelihood Ratio	31.833	20	.045
Linear-by-Linear Association	15.357	1	.000
N of Valid Cases	124		

a. 18 cells (60.0%) have expected count less than 5. The minimum expected count is .18.



### Size of your organization \* Anti-virus Software

		Anti-virus Software						Total
		Not Exist	Very Poor	Poor	Neutral	Good	Very Good	
Size of your organization	1 - 50 Employees	1	2	4	7	2	1	17
	51 – 100 Employees	0	1	5	13	6	0	25
	101 – 500 Employees	1	1	6	14	4	1	27
	501 - 1000 Employees	0	0	0	1	8	2	11
	More than 1000 Employees	1	4	1	8	16	14	44
Total		3	8	16	43	36	18	124

### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	51.874 <sup>a</sup>	20	.000
Likelihood Ratio	57.973	20	.000
Linear-by-Linear Association	17.240	1	.000
N of Valid Cases	124		

a. 21 cells (70.0%) have expected count less than 5. The minimum expected count is .27.

### Size of your organization \* Intrusion detection software

		Intrusion detection software						Total
		Not Exist	Very Poor	Poor	Neutral	Good	Very Good	
Size of your organization	1 - 50 Employees	2	6	4	3	2	0	17
	51 – 100 Employees	1	11	8	5	0	0	25
	101 – 500 Employees	2	8	8	7	2	0	27
	501 - 1000 Employees	0	2	4	1	4	0	11
	More than 1000 Employees	6	2	7	8	13	8	44
Total		11	29	31	24	21	8	124

**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	46.926 <sup>a</sup>	20	.001
Likelihood Ratio	55.646	20	.000
Linear-by-Linear Association	17.784	1	.000
N of Valid Cases	124		

a. 21 cells (70.0%) have expected count less than 5. The minimum expected count is .71.

## Size of your organization \* Encryption

		Encryption						Total
		Not Exist	Very Poor	Poor	Neutral	Good	Very Good	
Size of your organization	1 - 50 Employees	8	4	0	3	2	0	17
	51 – 100 Employees	14	6	1	3	1	0	25
	101 – 500 Employees	9	10	2	3	3	0	27
	501 - 1000 Employees	2	3	1	4	1	0	11
	More than 1000 Employees	6	7	6	9	12	4	44
Total		39	30	10	22	19	4	124

**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	35.598 <sup>a</sup>	20	.017
Likelihood Ratio	37.800	20	.009
Linear-by-Linear Association	20.579	1	.000
N of Valid Cases	124		

a. 21 cells (70.0%) have expected count less than 5. The minimum expected count is .35.

### Size of your organization \* Server room physical security

		Server room physical security						Total
		Not Exist	Very Poor	Poor	Neutral	Good	Very Good	
Size of your organization	1 - 50 Employees	5	2	3	1	3	3	17
	51 – 100 Employees	4	3	4	6	3	5	25
	101 – 500 Employees	4	1	1	8	5	8	27
	501 - 1000 Employees	0	0	0	2	5	4	11
	More than 1000 Employees	2	3	0	5	14	20	44
Total		15	9	8	22	30	40	124

### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	36.478 <sup>a</sup>	20	.014
Likelihood Ratio	39.636	20	.006
Linear-by-Linear Association	18.409	1	.000
N of Valid Cases	124		

a. 21 cells (70.0%) have expected count less than 5. The minimum expected count is .71.

### Size of your organization \* Input devices restriction

		Input devices restriction						Total
		Not Exist	Very Poor	Poor	Neutral	Good	Very Good	
Size of your organization	1 - 50 Employees	0	10	3	3	0	1	17
	51 – 100 Employees	0	13	10	2	0	0	25
	101 – 500 Employees	1	9	8	6	3	0	27
	501 - 1000 Employees	0	4	3	2	2	0	11
	More than 1000 Employees	3	8	7	10	12	4	44
Total		4	44	31	23	17	5	124

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	35.648 <sup>a</sup>	20	.017
Likelihood Ratio	43.531	20	.002
Linear-by-Linear Association	14.739	1	.000
N of Valid Cases	124		

a. 20 cells (66.7%) have expected count less than 5. The minimum expected count is .35.

### Number of years of the organization \* Two factors authentication implementation

		Two factors authentication implementation		Total
		Yes	No	
Number of years of the organization	Less than 1 year	0	3	3
	Between 1 to 5 years	4	13	17
	Between 6 to 10 years	12	11	23
	Between 11 to 20 years	6	10	16
	Between 21 to 30 years	4	11	15
	More than 30 years	16	34	50
Total		42	82	124

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	6.308 <sup>a</sup>	5	.277
Likelihood Ratio	7.118	5	.212
Linear-by-Linear Association	.005	1	.943
N of Valid Cases	124		

a. 2 cells (16.7%) have expected count less than 5. The minimum expected count is 1.02.

### Number of years of the organization \* Vulnerability Assessment

		Vulnerability Assessment						Total
		Not Exist	Very Poor	Poor	Neutral	Good	Very Good	
Number of years of the organization	Less than 1 year	1	0	1	1	0	0	3
	Between 1 to 5 years	0	6	7	3	1	0	17
	Between 6 to 10 years	3	4	6	3	4	3	23
	Between 11 to 20 years	3	5	4	1	3	0	16
	Between 21 to 30 years	1	4	4	2	2	2	15
	More than 30 years	6	6	14	13	8	3	50
Total		14	25	36	23	18	8	124

#### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	21.496 <sup>a</sup>	25	.665
Likelihood Ratio	25.808	25	.418
Linear-by-Linear Association	1.384	1	.239
N of Valid Cases	124		

a. 30 cells (83.3%) have expected count less than 5. The minimum expected count is .19.

### Number of years of the organization \* Process/practice in setting passwords

		Process/practice in setting passwords						Total
		Not Exist	Very Poor	Poor	Neutral	Good	Very Good	
Number of years of the organization	Less than 1 year	0	1	1	1	0	0	3
	Between 1 to 5 years	1	5	7	3	1	0	17
	Between 6 to 10 years	1	5	6	1	6	4	23
	Between 11 to 20 years	0	3	7	4	2	0	16
	Between 21 to 30 years	1	5	2	3	4	0	15
	More than 30 years	2	8	16	10	8	6	50
Total		5	27	39	22	21	10	124

**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	21.507 <sup>a</sup>	25	.664
Likelihood Ratio	27.307	25	.341
Linear-by-Linear Association	1.792	1	.181
N of Valid Cases	124		

a. 28 cells (77.8%) have expected count less than 5. The minimum expected count is .12.

### Number of years of the organization \* Firewall system

		Firewall system						Total
		Not Exist	Very Poor	Poor	Neutral	Good	Very Good	
Number of years of the organization	Less than 1 year	0	1	1	1	0	0	3
	Between 1 to 5 years	1	2	4	9	1	0	17
	Between 6 to 10 years	0	4	4	4	6	5	23
	Between 11 to 20 years	0	2	7	3	3	1	16
	Between 21 to 30 years	0	3	3	5	1	3	15
	More than 30 years	2	2	10	15	14	7	50
Total		3	14	29	37	25	16	124

**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	27.550 <sup>a</sup>	25	.329
Likelihood Ratio	31.769	25	.165
Linear-by-Linear Association	3.545	1	.060
N of Valid Cases	124		

a. 28 cells (77.8%) have expected count less than 5. The minimum expected count is .07.

### Number of years of the organization \* wireless connection access restriction

		wireless connection access restriction						Total
		Not Exist	Very Poor	Poor	Neutral	Good	Very Good	
Number of years of the organization	Less than 1 year	0	2	0	1	0	0	3
	Between 1 to 5 years	0	5	3	4	3	2	17
	Between 6 to 10 years	0	8	3	5	4	3	23
	Between 11 to 20 years	0	4	6	3	2	1	16
	Between 21 to 30 years	0	5	2	3	3	2	15
	More than 30 years	4	5	13	15	10	3	50
Total		4	29	27	31	22	11	124

#### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	22.525 <sup>a</sup>	25	.605
Likelihood Ratio	25.163	25	.453
Linear-by-Linear Association	.211	1	.646
N of Valid Cases	124		

a. 29 cells (80.6%) have expected count less than 5. The minimum expected count is .10.

### Number of years of the organization \* Internet sites access restriction

		Internet sites access restriction						Total
		Not Exist	Very Poor	Poor	Neutral	Good	Very Good	
Number of years of the organization	Less than 1 year	0	2	0	1	0	0	3
	Between 1 to 5 years	0	6	5	4	2	0	17
	Between 6 to 10 years	0	8	6	3	4	2	23
	Between 11 to 20 years	0	7	4	2	3	0	16
	Between 21 to 30 years	0	5	2	4	4	0	15
	More than 30 years	2	5	18	11	12	2	50

		Internet sites access restriction						Total
		Not Exist	Very Poor	Poor	Neutral	Good	Very Good	
Number of years of the organization	Less than 1 year	0	2	0	1	0	0	3
	Between 1 to 5 years	0	6	5	4	2	0	17
	Between 6 to 10 years	0	8	6	3	4	2	23
	Between 11 to 20 years	0	7	4	2	3	0	16
	Between 21 to 30 years	0	5	2	4	4	0	15
	More than 30 years	2	5	18	11	12	2	50
Total		2	33	35	25	25	4	124

#### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	23.884 <sup>a</sup>	25	.526
Likelihood Ratio	28.002	25	.308
Linear-by-Linear Association	3.668	1	.055
N of Valid Cases	124		

a. 30 cells (83.3%) have expected count less than 5. The minimum expected count is .05.

### Number of years of the organization \* Anti-virus Software

		Anti-virus Software						Total
		Not Exist	Very Poor	Poor	Neutral	Good	Very Good	
Number of years of the organization	Less than 1 year	0	0	1	2	0	0	3
	Between 1 to 5 years	1	2	2	7	4	1	17
	Between 6 to 10 years	0	0	6	7	6	4	23
	Between 11 to 20 years	1	1	3	4	5	2	16
	Between 21 to 30 years	0	1	0	7	4	3	15
	More than 30 years	1	4	4	16	17	8	50
Total		3	8	16	43	36	18	124

#### Chi-Square Tests



	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	18.665 <sup>a</sup>	25	.813
Likelihood Ratio	22.958	25	.580
Linear-by-Linear Association	2.400	1	.121
N of Valid Cases	124		

a. 27 cells (75.0%) have expected count less than 5. The minimum expected count is .07.

## Number of years of the organization \* Intrusion detection software

	Intrusion detection software						Total
	Not Exist	Very Poor	Poor	Neutral	Good	Very Good	
Number of years of the organization Less than 1 year	0	2	0	1	0	0	3
Between 1 to 5 years	1	7	4	4	1	0	17
Between 6 to 10 years	1	5	7	3	4	3	23
Between 11 to 20 years	2	6	3	2	2	1	16
Between 21 to 30 years	1	4	4	2	2	2	15
More than 30 years	6	5	13	12	12	2	50
Total	11	29	31	24	21	8	124

### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	23.230 <sup>a</sup>	25	.564
Likelihood Ratio	25.506	25	.434
Linear-by-Linear Association	2.181	1	.140
N of Valid Cases	124		

a. 30 cells (83.3%) have expected count less than 5. The minimum expected count is .19.

### Number of years of the organization \* Encryption

		Encryption						Total
		Not Exist	Very Poor	Poor	Neutral	Good	Very Good	
Number of years of the organization	Less than 1 year	1	2	0	0	0	0	3
	Between 1 to 5 years	9	2	0	5	1	0	17
	Between 6 to 10 years	6	5	3	5	2	2	23
	Between 11 to 20 years	8	3	0	1	4	0	16
	Between 21 to 30 years	6	3	1	1	3	1	15
	More than 30 years	9	15	6	10	9	1	50
Total		39	30	10	22	19	4	124

#### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	28.701 <sup>a</sup>	25	.277
Likelihood Ratio	32.792	25	.136
Linear-by-Linear Association	2.591	1	.107
N of Valid Cases	124		

a. 28 cells (77.8%) have expected count less than 5. The minimum expected count is .10.

### Number of years of the organization \* Server room physical security

		Server room physical security						Total
		Not Exist	Very Poor	Poor	Neutral	Good	Very Good	
Number of years of the organization	Less than 1 year	0	1	1	0	1	0	3
	Between 1 to 5 years	3	1	2	5	2	4	17
	Between 6 to 10 years	4	1	1	3	6	8	23
	Between 11 to 20 years	5	0	1	1	2	7	16
	Between 21 to 30 years	0	1	0	4	4	6	15
	More than 30 years	3	5	3	9	15	15	50
Total		15	9	8	22	30	40	124

**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	28.867 <sup>a</sup>	25	.270
Likelihood Ratio	30.737	25	.198
Linear-by-Linear Association	2.703	1	.100
N of Valid Cases	124		

a. 28 cells (77.8%) have expected count less than 5. The minimum expected count is .19.

### Number of years of the organization \* Input devices restriction

		Input devices restriction						Total
		Not Exist	Very Poor	Poor	Neutral	Good	Very Good	
Number of years of the organization	Less than 1 year	0	2	0	1	0	0	3
	Between 1 to 5 years	1	11	3	2	0	0	17
	Between 6 to 10 years	0	10	4	3	6	0	23
	Between 11 to 20 years	1	6	3	4	2	0	16
	Between 21 to 30 years	0	6	2	4	1	2	15
	More than 30 years	2	9	19	9	8	3	50
Total		4	44	31	23	17	5	124

**Chi-Square Tests**

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	32.269 <sup>a</sup>	25	.150
Likelihood Ratio	37.289	25	.054
Linear-by-Linear Association	7.347	1	.007
N of Valid Cases	124		

a. 27 cells (75.0%) have expected count less than 5. The minimum expected count is .10.