

Raising the Information Security Awareness Level in Saudi Arabian Organizations Through an Effective Culturally Aware Information Security Framework

A doctoral thesis in partial fulfillment of the requirements for the award of
Doctor of Philosophy of Loughborough University

By
Hend Khalid Alkahtani
Department of Computer Science
Loughborough University

Supervisors
Professor Ray Dawson
And
Doctor Russell Lock

January 2018

© by Hend Alkahtani

ACKNOWLEDGEMENT

First I would like to thank Allah for all the blessings and for answering my prayers during my stressful years of my study. I would like to thank my advisors Prof Ray Dawson and Dr Russell Lock for their invaluable advice, support, patience and guidance throughout my period of study. Their support and encouragement had pushed me forward and strengthen my thesis.

I would like to thank my family starting with my husband for his patience, encouragement, loving and financial support. My mom my father my kids my sisters and brothers for their support and encouragement and believing on me. I also would like to thank my best friend and her parents for praying for me and for their moral support.

I would like also to thank the formed information security team members especially kholoud Baselm and Sammer Aldbass for their contribution, support, patience and continuous help during the development of the produced culturally aware information security framework.

A special thanks and appreciation to my country Saudi Arabia for its encouragement for a better education and makes the abroad education easy for everyone. My gratitude and thanks to The Saudi Arabia cultural of bureau for sponsorship my study.

Abstract

The focus of the research is to improve the security of information systems in Saudi Arabian knowledge-intensive organisations by raising the awareness level among all types of information system users. This is achieved by developing a culturally aware information security framework that requires the involvement of all types of information system user. Saudi Arabia has a unique culture that affects the security of information systems and, hence, the development of this information security framework. The research uses Princess Nora bint Abdul Rahman University (PNU), the largest all female university in Saudi Arabia, as a case study.

The level of information security awareness among employees at Saudi Arabia Universities was tested. Surveys and interviews were conducted to gather data related to the information security system and its uses. It was found that most employees in Saudi Arabian organisations and universities are not involved in the development of any information security policy and, therefore, they are not fully aware of the importance of the security of information. The purpose of this study is to develop a cultural aware information security framework that does involve all types of employees contributing to the development of information security policy. The framework, consists of nine steps that were adapted, modified and arranged differently from the international best practice standard ISO 27K framework to fit the unique culture in Saudi Arabia. An additional step has been added to the framework to define and gather knowledge about the organisations population to justify its fit into the segregated working environment of many Saudi Arabian institutions. Part of the research objective is to educate employees to use this information security framework in order to help them recognise and report threats and risks they may encounter during their work, and therefore improve the overall level of information security awareness. The developed information security framework is a collection of ISO 27k best practice steps, re-ordered, and with the addition of one new step to enable the framework to fit the situation in Saudi Arabian segregation working environments.

A before-assessment methodology was applied before the application of the culturally aware information security policy framework between two universities, Imam University which has ISO27K accreditation and PNU, the case study, to measure and compare their users' information security awareness level. Then, an after-assessment methodology is used to demonstrate the framework effectiveness by comparing the level of awareness before the application of the culturally aware information security policy framework with the level of the awareness knowledge gained after the application.

Keywords - Information systems, Information security, Security awareness, Saudi Arabian Culture, Security policy.

List of Publications

H. Alkahtani, R.J.Dawson, RLock, 2013, "The Impact of Culture on Saudi Arabian Information Systems Security". The 21st International Conference on Software Quality Management (SQM 2013), London.

H. Alkahtani, R.J.Dawson, RLock, 2015, "Communication and Effective Email Usage in Saudi Arabia". International Conference on Software Quality Management (SQM 2015). Loughborough University Loughborough, UK.

TABLE OF CONTENTS

Chapter 1	Introduction	1
1.1	Statement of the Problem	2
1.2	Research Aim and Objectives	4
1.3	Research Structure	8
1.4	Conclusion	12
Chapter 2	Literature Review	13
2.1	Introduction	13
2.2	Information Security	13
2.3	Threats and Risks to Information Technology	16
2.3.1	Risk Management	17
2.3.2	Risk Assessment	18
2.3.3	Threats and risks associated with people.....	19
2.3.4	Technology Risk	20
2.4	Laws and Regulation for IT	22
2.5	Implementing Information Security	23
2.5.1	Auditing	26
2.5.2	Technical Controls	27
2.5.2.1	Preventive Controls	27
2.5.2.2	Detective and Recovery Control	30
2.5.3	Security Policy controls	31
2.5.4	People Controls	35
2.6	Human Compliance	37
2.6.1	Approaches to insure compliance	38
2.6.1.1	Training and education	38
2.6.1.2	Sanction	39
2.6.1.3	Annual personal performance plan	40
2.7	Management and information security	42
2.8	Information security in Saudi Arabia	43
2.8.1	Information system outsourced in Saudi Arabia	44
2.8.2	Information system attacks in Saudi Arabia	46
2.8.3	Saudi Arabia cultural effect in information security	47
2.9	Conclusion	49
Chapter 3	The Impact of Culture on Saudi Arabian Information Systems Security	51
3.1	Introduction	51
3.2	Language Barriers	52
3.3	Text direction	53
3.4	Hierarchy	54

3.5	Gender communication	56
3.6	Fear of losing face	56
3.7	Nepotism	57
4.8	Wealth	58
4.9	Conclusion	59
Chapter 4	Methodology	60
4.1	Research Methodology	60
4.2	Research Philosophy	61
4.2.1	Positivistic	61
4.2.2	Interpretivist/Phenomenological	61
4.2.3	Choice of Philosophy	63
4.3	Research approach	64
4.3.1	Type of Research	64
4.3.2	Quantitative vs qualitative	65
4.3.3	Subjective vs Objective	66
4.3.4	Deductive vs inductive	68
4.3.5	Choice of Approach	68
4.4	Research Strategy	69
4.4.1	Choice of strategy	70
4.5	Data Collection Methods for the Research	72
4.5.1	Literature Review	74
4.5.2	Survey	74
4.5.2.1	Initial Questionnaires	75
4.5.2.2	Second Questionnaires	76
4.5.2.3	The interviews	77
4.6	Summary	78
Chapter 5	Data collection-Survey.....	79
5.1	Questionnaires aim	79
5.2	Data collection-Survey process.....	79
5.2.1	Distribution of Questionnaires	79
5.2.2	Questionnaire distribution results	80
5.2.3	Questionnaire distribution results	80
5.3	Data collection analysis process	80
5.3.1	Q1: Gender (male/female).....	81
5.3.2	Q2: Age Group.....	82
5.3.3	Q3: What is your highest qualification?.....	83
5.3.4	Q4: Do you have any IT related qualification at undergraduate / postgraduate level?.....	84
5.3.5	Q5: Have you attended any IT related training courses?.....	84

5.3.6	Q6: Position held at PNU.....	85
5.3.7	Q7: Which of the University’s computer systems do you use?.....	86
5.3.8	Q8: Do you often face problems when using the University’s computer systems?.....	87
5.3.9	Q9: When dealing with IT related tasks, do you consider yourself someone more likely to have to help others, or to ask for help yourself?.....	87
5.3.10	Q10: Please list and rate (1-5) any problems that you have faced in the past month.....	88
5.3.11	Q 11: On a scale of 1 – 5 how computer literate do you see yourself?.....	89
5.3.12	Q12: Do you feel the IT systems at PNU are difficult to use?.....	91
5.3.13	Q13: How many passwords do you use to access the various IT systems at PNU?.....	92
5.3.14	Q14: Which parts of the current IT systems do you find the most difficulty with?.....	93
5.3.15	Q15: If you would like to add any additional information in relation to using the IT facilities at PNU please write it below.....	93
5.3.16	Non-IT staff survey analysis conclusion.....	94
5.4	IT-employee survey analysis	94
5.4.1	Q1: Gender.....	94
5.4.2	Q2: Age group.....	95
5.4.3	Q3: What is your highest qualification?.....	95
5.4.4	Q4: Is your education IT related?.....	96
5.4.5	Q5: Have you attended any IT related training courses?.....	97
5.4.6	Q6: Position held at PNU.....	97
5.4.7	Q7: Which of the tasks below do you perform whilst at the University?.....	98
5.4.8	Q8: Which of the University’s computer systems do you use?.....	99
5.4.9	Q9: Do you often face problems when using the University’s computer systems?.....	100
5.4.10	Q10: Do you find yourself asking others for help, or helping others?.....	100
5.4.11	Q11: Please list and rate (1-5) any problems that you have faced in the past month.....	101
5.4.12	Q12: On a scale of 1 – 5 how computer literate do you see yourself?.....	101
5.4.13	Q13: Do you feel the IT systems at PNU are difficult to use?.....	103
5.4.14	Q14: How many passwords do you use to access the various IT systems at PNU?.....	104
5.4.15	Q15: How much training on the Banner systems have you received?.....	105
5.4.16	Q16: What do you see the solution being to improve the computer systems at PNU?.....	106
5.4.17	Q17: How much external support does PNU currently utilise for the current information systems?.....	107
5.4.18	Q18: Do you feel the current IT department is managed correctly?.....	107

5.4.19	Q19: Have you found this training to be beneficial?.....	108
5.4.20	Q20: How secure do you feel the current computer systems are at PNU?...	108
5.4.21	IT Staff Survey Conclusion.....	109
5.5	Summary of the finding results.....	110
Chapter 6	Data collection: Interview	112
6.1	The goal of the Interviews	112
6.2	Interview Techniques	116
6.2.1	The first interview collection technique	117
6.2.2	The second interview collection technique	118
6.2.3	The third interview technique	119
6.3	The data collection interview design	120
6.4	Initial interview	121
6.4.1	Part 1: Vulnerability of PNU's information systems	122
6.4.2	Part 2: Employee and users awareness	129
6.4.3	Part 3: Training programmes	134
6.5	Second interview: Interviewing females at the University	137
6.5.1	General problems	138
6.5.2	Staff problems	139
6.6.2	Students problem with the system	139
6.6	The results and finding for the first and second interviews	140
6.7	Third interview: ISO interviews	142
6.8	Recommendations	145
6.8.1	Communication solution	145
6.8.2	Feedback awareness	147
6.9	Conclusion.....	147
Chapter 7	Formation of Information Security Policy framework.....	149
7.1	The development of information security framework	149
7.2	First phase: Prior implementation	155
7.2.1	Step 0: Formation of an information security team	155
7.2.2	Step 1: Identification and collection of information security requirements.....	156
7.2.2.1	ISO / Best practice	157
7.2.2.2	Law and regulations	162
7.2.2.3	Auditing	163
7.2.2.4	Risk assessment and treatment	166
7.2.2.5	Identifying culture problems	169
7.2.2.5.1	Trusting culture	170
7.2.2.5.2	Gender communication	172
7.2.3	Step 2: Identification of the population of an organisation	174

	7.2.3.1 Gender (male/female)	175
	7.2.3.2 Age	176
	7.2.3.3 Language	176
	7.2.3.4 Education level	177
	7.2.3.5 Information security awareness level	178
7.3	Second phase: Implementation	178
7.3.1	Step 3: Definition of roles and responsibilities	179
7.3.2	Step 4: Definition of system information procedures and standards	182
	7.3.2.1 Identities and accounts	182
	7.3.2.2 Authentication	184
	7.3.2.3 Authorisation	186
7.3.3	Step 5: Classification of asset risk and threat	187
7.3.4	Step 6: Classification of the System Information	188
7.3.5	Step 7: Definition of the rules and access controls for handling system Information	189
	7.3.5.1 Laws and regulations	190
	7.3.5.2 Storage	190
	7.3.5.3 Access controls	191
	7.3.5.4 Copying data	192
	7.3.5.5 Retention and disposal	193
	7.3.5.6 Exchange information and use of email	195
7.3.6	Step 8: Definition and selection of information security controls	196
	7.3.6.1 Technical controls	196
	7.3.6.2 Physical controls	197
	7.3.6.3 Procedural controls	198
7.3.7	Step 9: Definition of an incident management and business continuity plan.....	201
7.4	Post implementation phase	204
7.4.1	Step 10: Conduct policy gap analysis and Evaluation of the framework	204
7.5	Conclusion	204
Chapter 8	Framework pre-implementation phase 1 and pre-assessment and information security awareness survey analysis.....	206
8.1	Application and evaluation technique	206
8.2	The application of Phase 1 (pre-implementation).....	208
	8.2.1 The formation of the information security framework team: Step (0).....	208
	8.2.1.1 The team scheduled meeting	210
	8.2.2 Identification and collection of the current information security data:Step1.	211
	8.2.3 The application of Phase 1: Step 2	215
	8.2.3.1 The application of Sub Step 2: Measure IT security awareness level	217

8.2.3.2 Pre-assessment awareness survey analysis	219
8.2.3.2.1 The survey prior analysis first method	219
8.2.3.2.2 The survey prior analysis second method	222
8.3 Conclusion	229
Chapter 9: Evaluation of a culturally aware information security policy framework	232
9.1 The application of Phase 2: Step 3 - Definition of roles and responsibilities	232
9.2 The Application of Phase 2: Step 4 - Definition of information system procedures and standards	235
9.3 The Application of Phase 2: Step 5 - Risk and threat assessment and classification	237
9.4 The application of Phase 2: Step 6 - Classification of the System Information	240
9.5 The application of Phase 2: Step 7 - Defining rules and access controls	241
9.6 The application of Phase 2: Step 8 - Information security controls are defined and selected	244
9.7 The application of Phase 2: Step 9 - The incident management and business continuity plan	247
9.8 The application of Phase 3: Step 10–Application of the Information Security Policy...	249
9.8.1 Testing the produced information security policy at PNU.....	249
9.9 Factors affect the application of the framework	257
9.10 Chapter Conclusion	258
Chapter 10: Recommendation, Conclusion and Future work	259
10.1 Research contributions and achievements	259
10.2 Research Limitations	264
10.3 Conclusions	265
10.4 Future work	267
10.5 The success of this PhD Research	269
References	271
Appendices	
Appendix A - Surveys and interviews Questionnaires.....	284
Appendix B - Sample of Interviews Responses.....	303

Appendix C - Employee Security Awareness Survey	319
Appendix D – Example of tables filled by students	341
Appendix E - The produced information security policies	347

List of Figures

Figure 1.1: The overall process used to gather and analyse information to develop an information security framework	7
Figure 1.2: Research Thesis Structre	11
Figure 2.1: Types of threat Source: Handbook for ISO/IEC 27001 (2010)	17
Figure 2.2: a typical life cycle of a computer virus Source: whitepaper F-secure Corporation 2001	21
Figure 2.3: a typical life cycle of a computer worm Source: whitepaper F-secure Corporation 2001	21
Figure 2.4: Three types of cryptography: secret-key, public key, and hash function adopted from Kessler (2016).	29
Figure 2.5: Supporting Activities for Effective Information Security Policy adopted from Höne and Eloff (2003)	33
Figure 2.6: Personal Information Security Plan adopted from Wylder (2003).....	40
Figure 2.7: Percentage of Female Students at All School Levels (1974–75 and 2004–05)	47
Figure 2.8: Female Graduate Degrees by Department (2004–05)	48
Figure 3.1: Cultural problems in a Saudi Arabian organisation	52
Figure 3.2: PNU Information technology structure (PNU website)	55
Figure 4.1 Nested Approach (Kagioglou et al, 1998)	60
Figure 4.2: Research Stages.....	73
Figure 5.1 Gender	81
Figure 5.2 Age group	83
Figure 5.3 Qualification	83
Figure 5.4 Training courses	85
Figure 5.5: Position held at PNU	85
Figure 5.6: Computer systems used at PNU	86
Figure 5.7: Computer system problem faced.....	87
Figure 5.8: IT related tasks	88
Figure 5.9: computer literate.....	89
Figure 5.10: IT systems difficulty of use at PNU	91

Figure 5.11: Number of passwords used	92
Figure 5.12: Age group	95
Figure 5.13: Qualification	96
Figure 5.14: IT related education	96
Figure 5.15: IT related training courses	97
Figure 5.16: Position held at PNU	98
Figure 5.17: Tasks performed	99
Figure 5.18: Computer system used at PNU	99
Figure 5.19: Problems faces with computer system	100
Figure 5.20: asking for help/helping others	101
Figure 5.21 Computer literate	102
Figure 5.22 Perceived IT system difficulty of use	104
Figure 5.23: Number of passwords used	105
Figure 5.24: Training on the Banner System	106
Figure 5.25: Solutions to improve the computer system	106
Figure 5.26: External support	107
Figure 5.27: The IT department management approval	108
Figure 5.28: Security of the current computer system	109
Figure 6.1: The Structure of PNU IT Management	114
Figure 6.2: PNU campus map Source PNU website 2013	115
Figure 6.3: Communication between end users and IT technician at PNU	141
Figure 6.4: PNU Communication Structure	146
Figure 7.1: Phase 1: Prior to implementation phase of the Information security framework.....	151
Figure 7.2: Phase 2: Implementation phase of the Information security framework	152
Figure 7.3: Phase 3: Post implementation phase of the Information security framework...	153
Figure 7.4: Elements required for an information security policy framework	157
Figure 7.5: PNU employee share work password with a co-worker or someone else	170
Figure 8.1: Communication structure among the selected team	210
Figure 8.2: Position within the university	218
Figure 9.1: Does the university have an information security team?	233

Figure 9.2: Do you know who to contact in case you are hacked or if your computer is infected?	234
Figure 9.3: Do you know what an email scam is and how to identify one?	237
Figure 10.1: The research process in developing the framework	264

List of Tables

Table 2.1: Three Maturity models to improve information security Adopted from Xiao-yana, Yu-qing, and Li-lei (2011)	25
Table 4.1: Positivism and Phenomenology Research Philosophy (Source: Easterby-Smith <i>et al.</i> , 1991)	63
Table 4.2: Quantitative and qualitative approaches adopted from Neville (2007)	66
Table 4.3: Key Research Implications of the Subjective and Objective Perspectives: Easterby-Smith <i>et al.</i> (1991).....	67
Table 4.4: Deductive and inductive approaches adopted from Neville (2007).....	68
Table 4.5: Research strategies used for each research objectives	71
Table 4.6: Research methods: Quantitative and Qualitative (Source: MacDonald <i>et al.</i> , 2011).....	72
Table 4.7: Face-to-face vs Telephone (Source: MacDonald <i>et al.</i> , 2011).....	77
Table 5.1: Correlations between age group and qualification.....	84
Table 5.2: The Relationship Between academic qualification, number of training courses attended and the participants view of their own computer literacy.....	90
Table 5.3: the relationship between: Qualification, Number of training and Computer literate.....	103
Table 5.4: Correlations between System difficulty and IT qualification.....	104
Table 6.1: Summary of the first part of the first interview	128
Table 6.2: Summary of part two of the interview	133
Table 6.3: Summary of part three of the interview	136
Table 6.4: ISO27K interviews with two universities, PNU and ImamU	143
Table 7.1: PNU execution of ISO 27K elements	159
Table 7.2: Recording information assets (adopted from Oxford University IS Policy, 2012).....	166
Table 7.3: Listing threats (adopted from Oxford University IS Policy, 2012)	166
Table 7.4: Threat rating (adopted from Oxford University IS Policy, 2012)	166
Table 7.5: workshop and seminar timing schedule	171

Table 7.6: Email response rate at PNU.....	173
Table 7.7: information assets classification definitions and types (adapted from Hill, 2012).....	187
Table 8.1: Meeting schedule for the framework application	210
Table 8.2: Risk Levels (adapted from Bond, 2013)	221
Table 8.3: Personal computer security questions.....	223
Table 8.4: University security policy questions	224
Table 8.5: User knowledge and security awareness questions	226
Table 8.6: User experience questions	227
Table 8.7: User security practise questions	228
Table 9.1: Recording and reporting information assets problems	238
Table 9.2: Risk rating	238
Table 9.3: Recording information assets	239
Table 9.4: Listing threats (adopted from Oxford University IS Policy, 2012)	239
Table 9.5: PNU IS Department Risk level before and after the application of the cultural aware information security framework	250
Table 9.6: Personal computer security questions	251
Table 9.7: University security policy questions	252
Table 9.8: User knowledge and security awareness questions	254
Table 9.9: User experience questions	255
Table 9.10: User security practise questions	256

LIST OF ABBREVIATIONS

BPO	: Business Process Outsource
CCTV	: Closed-Circuit Television
CSO	: Chief Security Officer
DDoS	: Distributed Denial-Of-Service
ImamU	: Imam University
ISO/IEC 27k	: The International Organisation for Standardisation/ the International Electrotechnical Commission
ISO (TC)	: International Organisation for Standardisation (Technical Committees)
ISP	: Internet Service Provider
IT	: Information Technology
MCIT	: Saudi Arabia Ministry of Communication and Information Technology
PNU	: Princess Nora bint Abdul Rahman University.
STC	: Saudi Telecom Company
SASO	: Saudi Arabian Standard Organisation

Chapter 1: Introduction

Up until recently, knowledge-intensive organisations such as universities in Saudi Arabia and most Gulf and Middle Eastern countries had no computerised information systems. Most of the work processes were completed manually using pen and paper. At this point, students' grades were the only information that was computerized, using basic office application software including Word, Excel and Access. None of the universities had networked systems; in fact, the internet was not available in most of the knowledge-intensive organisations at that point. Many of the Saudi Arabian knowledge-intensive organisations for females have no access to the internet and access for males remains limited, (Al-furaih, 2002; Al-Lehaibi, 2001). The adoption of the internet in Saudi Arabian universities was limited due to a number of barriers, such as culture, religion and language (Al-Wehaibi et al., 2008; Alfuraih, 2002).

Universities in Saudi Arabia consist of an aggregation of individual colleges. Princess Nora bint Abdul Rahman University (PNU), for example, was formed from six colleges and later four other new colleges were added. It is currently considered the largest all female university in the world. PNU initially used traditional, relatively manual methods of handling information, which focused mainly on student records, such as grades and transcripts. The privacy of student records was the responsibility of the registrar who controlled access to records. With the increased use of electronic networks around the world, PNU has now shifted to an electronic networked information system environment. The new electronic networked technologies were designed to provide effective and efficient service to the students and staff.

In 2009, a new information system, the Banner information system, was introduced to most universities in Saudi Arabia and some other Gulf and Middle Eastern countries. The Banner system is used in number of USA Universities such as the University of North Carolina, University of New Mexico, University of California, Davis (UC Davis), and Virginia State University; and UK Universities such as Leeds Metropolitan University, Ulster University and Southampton University. The Banner information system is a comprehensive information database system that contains information about students, faculty, staff and courses. The

Banner system consists of a number of modules such as admission, registration and graduate student information. Students at PNU or any other university using Banner are able to register online, access their own grades, transcripts, course schedules and much more.

However, this shift is not without challenges and the protection of information privacy has become a more complex issue. Therefore, many Saudi Arabian universities have established new departments, often called the Directorate General of Information & Communication Technology to cope with the technological development and challenges. In many universities in Saudi Arabia, this department is managed mostly by men, working in a separate building or, in the case of PNU, underneath the main university buildings, in which the entire hardware network system and utilities of PNU are located. Special tunnels and other service areas exist, which are designed to remove male staff from public areas. According to the PNU website (2013), the Directorate General of Information & Communication Technology department goals are “to support a culture of using information technology among the employees of the University by providing high-tech and sophisticated equipment and instruments, and implementing suitable information and programming systems to provide an integrated quality of information technology and communication services.”

1.1 Statement of the problem

It has been recognised worldwide that there is still a significant problem faced by organisations, especially universities, in securing information systems. In knowledge-intensive organisations, such as universities, it is an increasingly complex and challenging activity to guarantee the security of information systems (Doherty, et al. 2009).

This research uses Princess Nora University (PNU) as a case study. The research is focused on studying PNU’s information security system. The reason for this selection is that PNU is:

- A new university that is just starting to establish its policies. Findings related to PNU can be used to help other new universities to develop their new security policy.

- An all-female university lead by IT male administrators which has a potential gap in the communication between them. This may help in finding a solution for the communication gap in any other organisations in Saudi Arabia, the Gulf or Middle East or any religious organisation that faces a similar situation.
- PNU is new to the concept of IT system security, and as such the risks and threats it faces are high. This will also apply to many of the government organisations in Saudi Arabia.

With the recent shifting to an electronic networked information system, many Saudi Arabian universities, including PNU, now have specific issues related to people awareness, culture, law, and natural disasters that have a strong impact on their information system security.

Although people are considered as assets to help reduce risk to information, they are also the main threat to the information system security (Bulgurcu, Cavusoglu et al. 2010, Rotvold 2008). According to Dr Nasser, the director of the Directorate General of Information & Communication Technology department in PNU (2013), much of the damage caused to the information system so far has been as a result of human error. The main reason could be the lack of knowledge and experience with computers. The use of computers in secondary schools only started in 2005 in Saudi Arabia (Almunajjed, 2009). Therefore, some of the faculty and senior students are not computer illiterate. Further, some are either afraid of, or do not like, using computers. The lack of computer knowledge could make some of the tasks beyond the employee's ability and can easily cause human error such as:

- Inaccurate data entry.
- Accidental introduction and spreading of malware software when opening unknown e-mails or downloading infected programs.
- Unknowingly encouraging electronic attackers when choosing an easily guessed password, sharing a password or not protecting their password.

According to the culture and Islamic religion, adult females in Saudi Arabia wear veils outside their homes or when they are around male strangers. PNU is all female university and since students, staff and faculty don't wear veils on the university campus, the families of all the students and employees will not allow CCTV cameras to record them. Therefore, with the lack of physical security systems around the university, no one knows whom to accuse when thefts occur. Thefts could involve students, faculty or administrative employees, or auxiliary staff such as cleaners, who are predominantly male, who come every day after the university closes at 4:00 pm. In the case of the auxiliary staff, the use of tunnels and other service areas provides an ideal environment to move unobtrusively. Several cases of hardware and software thefts have been reported in PNU.

Some actions have been taken to deter hackers and the theft of software in Saudi Arabia. Royal decree no. M/17 8 Rabi 1 1428 / 26 March 2007 decreed the Anti-Cyber Crime Law. This Law aims to combat cyber-crimes by identifying such crimes and determining their punishments to ensure the following:

1. Enhancing information security.
2. Protecting the rights of legitimate use of computers and information networks.
3. Protecting public interest, morals, and common values.
4. Protecting the national economy.

However, although this law is available online in the MCIT, Saudi Arabia Ministry of Communication and Information Technology website, most Saudi Arabian online users are not aware of it (AlQahtani, 2016).

1.2 Research Aim and Objectives

The aims of this research are to determine what policies will provide protection for the information systems that best fit the unique culture of Saudi Arabia for universities in particular, and, in general, for service and government organisations in Saudi Arabia, the Gulf countries, Middle Eastern countries or any other organisations with a similar work culture environment.

To achieve this aim, the following objectives have been identified:

1. Carry out a literature review to discover
 - a. What technology, policies and actions are regarded as best practice to safeguard the security of information systems in an organisation.
 - b. What are the potential dangers and types of attack that could be a threat to the security of IT systems, and whether any of these dangers pose a greater risk in Saudi Arabia than elsewhere.
 - c. What are the potential barriers to a successful implementation of these technologies, policies and actions, and, in particular, whether the awareness levels, cultural attitudes, practices and the law in Saudi Arabia contribute to these barriers.
 - d. What are the possible policies and actions to overcome these barriers and whether these could be applied in Saudi Arabia.
2. By means of interviews, surveys and experiments, determine what is the current state of IT security at PNU, the case study, in particular:
 - a. How adequate are the IT security policies and practices at PNU and how susceptible to possible attacks and dangers are the PNU information systems?
 - b. Could the IT security best practice identified in the literature review be applied at PNU?
 - c. Do the dangers to IT security identified in the literature review exist at PNU and are there any other dangers particular to PNU?
3. Analyse the findings from Objective 2 to formulate a practical and effective policy and action plan for any Saudi Arabian knowledge-intensive organisation to improve their IT security, with particular emphasis on overcoming the

awareness, cultural specific and legal barriers to IT security at Saudi Arabian knowledge-intensive organisations.

4. Test the policy and action plan by means of experiment, where possible, and by expert opinion otherwise.
5. By conducting interviews and/or surveys at other organisations, determine how common are the dangers and barriers to information system security in other service organisations in Saudi Arabia, and how much of the plan for PNU would be applicable to other organisations in Saudi Arabia.
6. By analysing the results from Objective 5, produce a framework of recommendations for policy and action to improve information system security in Saudi Arabian organisations.
7. Test the developed culturally aware information security framework using a quantitative approach to test the framework by mean of survey questionnaires.

The research uses the case study of Princess Nora Bin Abdurrahman University (PNU) and Imam University, a university which has ISO27K accreditation, to gather requirements for, develop and test an information security framework designed to take into consideration Saudi Arabia culture, laws and regulations and the local university regulations and culture (see Figure 1.1).

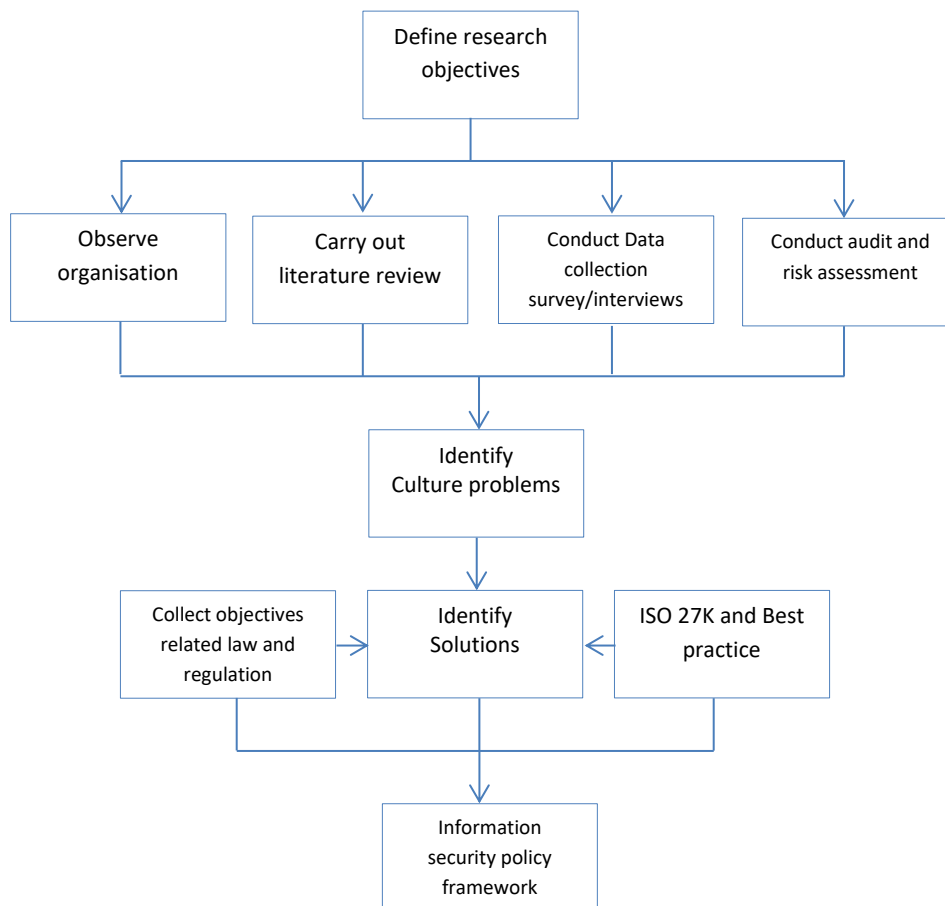


Figure 1.1: The overall process used to gather and analyse information to develop an information security framework

The initial step was to identify and establish the research objectives. Based on the objectives, an in-depth literature review was carried out to identify and review the role of information security policy and best practice in securing an information system. This was followed by primary data collection through a survey and interviews to investigate the state of information systems. An audit and risk assessment were conducted to determine the current security situation at PNU and to identify problems and potential solutions. Other implementation requirements to be considered included the Saudi Arabian Ministry of Higher Education's requirements and PNU related laws and regulations. Moreover, since Saudi

Arabia and most of the Middle Eastern countries have not developed their own information security policy standards, International and regional standards, such as ISO 27k and international best practice were considered and adapted in the implementation and development of the information security policy and framework.

1.3 Research Structure

This thesis consists of nine chapters, Figure 1.2. Chapter 1 is the introductory chapter that gives a brief description of the purpose of this research. It covers the background of the problem, statement of the problem, the research aim and objectives and then concludes with this outline of the thesis structure.

Chapter 2 is the Literature Review chapter. It is a discussion of related documents that were previously written about information technology, information security, information security policy, potential threats, risks, attacks and human compliance that can be potential barriers to a successful implementation of information security. Approaches and techniques are presented in this chapter, such as the use of annual personnel performance, that can be used to ensure and enforce employee compliance at PNU or any other university in Saudi Arabia.

Chapter 3 covers the effect of Saudi Arabia culture on the security of information systems. It focuses on the impact of the environment and culture of Saudi Arabia on information security and makes some suggestions on how these problems may be overcome. This chapter highlights additional problems created by the culture in Saudi Arabia. It also makes suggestions on ways forward for the investigation to resolve the problems identified.

Chapter 4 is the methodology chapter. It provides a description of all the methods used in this research. It presents the research approach, philosophy and methodology adopted for this study to achieve the research objectives outlined in this chapter. It starts by describing some general research types, philosophies and methodologies and then the researcher's choice of the research type, philosophy and methodology.

Chapter 5 discusses the data collection surveys. The chapter covers the description and analysis of the initial data collection, survey and questionnaire. The purpose of this study

was to get an overall idea of what the employees think of the system they are using, focusing on its security. Two types of questionnaire were distributed, one for Information Technology (IT) staff and one for non-IT staff, faculty members and students who are the end users of the IT system.

Chapter 6 explores the data collection interviews. The chapter covers the description and analysis of the second part of data collection, interview and questionnaire. Three interview techniques were used to collect data: structured, unstructured, and semi-structured interviews. Moreover, three types of interview have been used in this study: telephone interviews, face-to-face interviews and group interviews.

Chapter 7 describes the formation of the information security framework. This chapter focuses on the development of an information security policy framework and workflow so that the employees of any information system can use it to implement their own security policy based on that framework. This gives an initial implementation of information security policy that is suitable for the Saudi Arabian knowledge-intensive organisations.

Chapter 8 covers the framework pre-implementation phase 1 and pre-assessment and information security awareness survey analysis. This chapter covers the application and evaluation of the implementation and pre-implementation phase 1 of the developed culturally aware information security policy framework. The framework focuses on raising the level of information security awareness among employees working in an environment with cultural differences. This chapter covers, the application technique used to develop the culturally aware information security policy framework, the formation of the information security framework team, the application of the framework phase 1 pre-implementation of steps 0 to 2, the issues raised while applying each step and the resolution of those issues.

Chapter 9 is the application and evaluation of the implementation and post implementation phases of the developed culturally aware information security policy framework. This chapter has sections covering the application technique used to develop the culturally aware information security policy framework, the formation of the information security framework team, the application of the framework phases 2 and 3 and steps 3 to 10, the issues raised while applying each step and the resolution of the those issues.

Chapter 10 gives the research contributions and achievements of the developed culturally-aware information security framework. The chapter also reviews the final research results and summarises the research overall findings. The last sections of the chapter present the research limitations, recommendations and suggestions for future work.

Figure 1.2 shows the structure of the research and how it is presented in the chapters of this thesis.

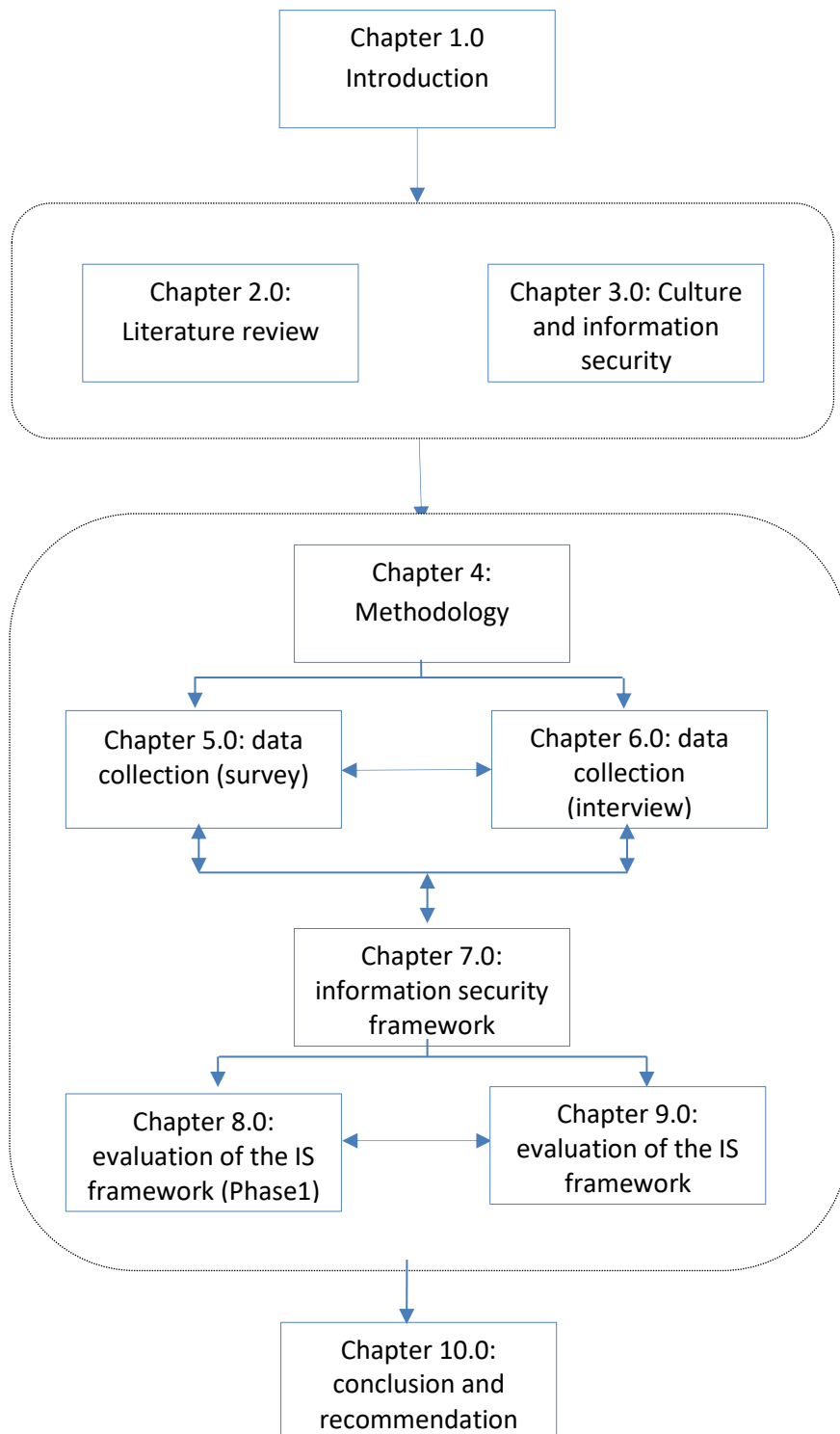


Figure 1.2: Research Thesis Structure

As shown in Figure 1.2, Chapter 1 covers the research starting point. Chapter 2 and chapter 3 describe the initial collection of related documents that have impact in the development of the reseach. Chapter 4 discusses the methodolgy used in analysing the data collection in chapters 5 and 6 (survey and interview). Chapter 7 describes the formation of the information security framework. Chapters 8 and 9 cover the evaluation of the IS framework. Finally, Chapter 10 gives the conclusion and recommendations of the study.

1.4 Conclusion

The introductory chapter gives a brief description of the main purpose of the study. It introduces the problem background, giving a statement of the contributing factors of the security problem, such as human error, culture, laws and natural disaster. The research uses Princess Nora University as a case study.

The main aim of this research is to develop a culturally-aware information security system framework and test it in Princess Nora University, the case study, and compare PNU collected information with Imam University, a university which has ISO27K accreditation. The results can then be used as a benchmark for any other university information security system in Saudi Arabia or any developing countries with a similar culture and environment. This involved improving the auditing technique, implementing a suitable information security policy which takes into consideration Saudi Arabia culture, laws and regulations, and the university regulations and culture. This has led to developing an IT security framework.

The next chapter, the literature review, covers the related documents that were previously written about information technology, information security, and information security policy and have impact in the development of this research.

Chapter 2: Literature Review

2.1 Introduction:

The need for Information security was recognized many centuries ago, long before computers and electronics existed. At the start of the computer revolution, protecting information used to be a relatively simple task as computers that held the information were either standalone or only available via local networks which could be subject to physical security (Diffie, 2008). Information security was then just the process of protecting the confidentiality of information and protecting information from any kind of unauthorised access (Diffie, 2008).

Since that time technology has evolved considerably and commerce relies on electronic data and sophisticated methods to protect it. The rapid changes in information communication and technology have increased the number of potential solutions for protecting organisation information assets (Dhillon and Backhouse, 2000). Moreover, with the increase of new information nearly doubling every two years, this could overwhelm the information security specialist with an “information avalanche” and challenge the security of information (Poore, 2001). Today, the need for information security has grown exponentially and is recognised throughout the world (Diffie 2008).

This chapter examines previous studies that have been conducted on information security, implementation of information security, management of information security, information security policy, human compliance to information security policy and information security in Saudi Arabia.

2.2 Information security

Data are a collection of facts and figures such as words, numbers, and symbols that have no meaning on their own (Fatmax 2007). Information is a collection of valuable data and knowledge of a specific event, thing or person. Information can exist in many forms such as printed or hand written on paper, electronically stored or sent via post or email (Kapp,

2000). Knowledge is the ability to understand the rules and the relationship between information in order to transpose information (Fatmax 2007). Today, information is considered as a business asset with different value levels and sensitivity (Humphreys, 2010). Information is now exposed to an increasing number of threats because of the growing switch to networked environments and it is essential to protect information assets as they are just as important as any other asset in an organisation (Humphreys, 2010). Guo, et al. (2011) add that the rapid and continued use of the Internet and wireless network is jeopardizing information systems (IS) security. Information is an asset that has value to the organisation just like any organisation asset and, therefore, it has to be protected (Kapp, 2000; Burney, 2003). The organisation must realize that information is a valuable asset and that protecting it is necessary to reach a successful business goal and mission (Burney 2003).

Information Security is the process of protecting the availability, confidentiality, authenticity, reliability and integrity of information assets and information systems in an organisation. Information security refers to the process of safeguarding information from any form of unauthorised access. According to Hill (2007), an information security system is the process of protecting the confidentiality, reliability and availability of creation, storing, processing, and/or transmitting of data in computerised information systems. Information security can be defined as the protection of information's confidentiality, integrity and availability under organisation control (Kapp, 2000). SANS (SANS organisation website May 4, 2013) define information security as "the processes and methodologies which are designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption." ISO/IEC 27001 (2005) and BS ISO/IEC 27002 (2005) define information security as maintaining the information confidentiality, integrity, authenticity, availability and reliability:

- **Confidentiality** is the most fundamental aim of an information security system. Confidentiality ensures that information is not exposed or made available to unauthorised entities, whether they are individuals or processes.

- **Integrity** means to ensure that information and the methods used to process and manage it are accurate and complete (ISO/IEC 27001, 2005 and BS ISO/IEC 27002, 2005).
- **Authenticity** refers to the process of approving the identity of an entity, person or computer software, when working in an open network (Laudon, Traver 2012; Tuban et al., 2013).
- **Availability** means that an asset, which could be data or a service such as information, systems, facilities, networks and computers, is accessible and usable when needed by authorised parties (ISO/IEC 27001, 2005 and BS ISO/IEC 27002, 2005). A person or a system with legitimate access should not be prevented from accessing a particular set of objects if they are authorized at appropriate times (Pfleeger and Pfleeger, 2007).
- **Reliability** is the ability of a person or system to accomplish and preserve its functions in normal circumstances, as well as in an adverse or unexpected situation (ISO/IEC 27001, 2005).

The main goal of information security is to guarantee business continuity in an organisation by reducing risk and threats to information assets. Xiao-yana, Yu-qing, and Li-lei (2011) emphasise that the goal of information security is to protect information from any form of threat or risk by making information access secure and enforcing information security policy. Xiao-yana, Yu-qing, and Li-lei (2011) believe that today information security plays a major part in the development of the structure and function of organisation. Therefore, Burney (2003) states that protecting the organisation's information should be the daily responsibility of all the employees in an organisation, from the top level to junior workers.

Implementation of good Information security programmes would help ensure protection of an organisation's information (Burney 2003). In 2003, the USA's Federal Financial Institutions Examination Council (FFIEC) issued guidance that states: "senior management should designate one or more individuals as information security officers" (DeMauro and Grottke, 2008). The Information System Security Officer (ISSO) should be responsible for implementing information security programmes that cover information security planning, policies,

standards, guidelines and training. The ISSO should also advise and assist the management in information security issues. The ISSO is responsible for the success of these programmes (Burney 2003) . The roles and responsibility of the ISSO should be to administrate the information security programme by supervising and overseeing the process of information technology (IT) risk assessment, the implementation of IT security policies, standards, and procedures, and the reporting of the progress of information security.

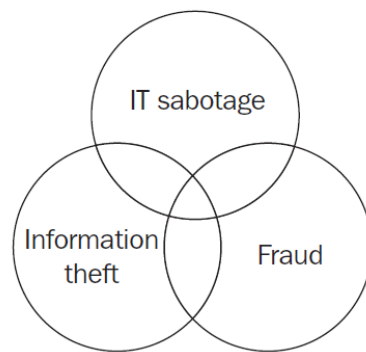
Information is now as important as any other organisational asset and, therefore, the need to clarify the meaning of a secure information system is important as well. The first research objective part “a” is to look for technology and action that leads to the safeguarding of information. This section contributes to this objective by identifying that the development of a strong information security system must start with understanding the meaning, the elements and the processes of an information security system that makes a strong IS system. Also, the management of a university should designate an Information System Security Officer (ISSO) to administrate and supervise the IS system and its processes. The role of the ISSO should include the formation of the information security policy.

2.3 Threats and risks to information technology

A threat, in this context, is an event or act which has the potential to harm an information system through unauthorised access, destruction, disclosure, modification of data, or denial of a service. A threat can be a person or a thing, or could be a process or technology likely to cause damage or danger. A threat can also be deliberate or accidental and it could be human or computer related (Pfleeger and Pfleeger 2007).

Humphrey (2010) classifies threat problems into:

- 1- Insider IT sabotage
- 2- Information theft
- 3- Fraud: document fraud, identity fraud and computer fraud.



Source: Handbook for ISO/IEC 27001 (2010)

Figure 2.1: Types of threat

As seen in figure 2.1 there is a relationship between all three types of threat. They are overlapping with each other and sometimes it is not possible to distinguish one from another. They all do intentionally or accidentally cause damage to information assets. For example, IT insiders can sabotage the organisation information system when they exploit their authority to perpetrate insider document, identity or computer fraud.

Risk is “a situation involving exposure to danger” (Oxford Dictionary, 2013). Risk can be controlled and managed by the process of identifying assessing, prioritising risk and controlling threat. The next subsections identify some of the potential threats, risks and attacks that could threaten the security of the information system. Risk identification, risk assessment, threats and risks associated with people and technology risk are explained next subsections 2.3.1-2.3.4.

2.3.1 Risk identification

Risk can be internally created by a member of an organisation or externally created by people or events outside the organisation.

1- Internal risk:

Accidental risk:

One of the main causes of this kind of risk would be that employees may not get good training or awareness programmes when using new applications, services or systems. For example, employees may make mistakes and bad decisions if they don't receive appropriate training. Humphreys (2010) states that not getting the appropriate training and awareness could be the cause of accidental risk.

Intentional risk:

Intentional risk is driven by the motive to damage. Employees may put organisational services, systems or applications at risk when they use them for personal gain or for revenge, if they lose their job or position, or for political reasons.

2- External risk:

Accidental risk: This kind of risk would be that any entity/person that is independent of the organisation, such as customers or suppliers, accidentally cause an unwanted event that has negative impact on a system.

Intentional risk: this kind of risk is caused by people independent of the organisation, such as those acting out of political reasons, social activity terrorists or protestors, with the intention to cause damage (Humphreys, 2010).

2.3.2 Risk assessment

Risk assessment is the process of detecting and evaluating risks that could endanger the business continuity of an organisation. Risk assessment consists of four steps, preparing,

conducting, communicating, and maintaining which can help identify, estimate, and prioritise risk (Radack 2012). According to BS ISO/IEC 27002 (2005) (the International Organisation for Standardisation/ the International Electro technical Commission), risk assessment is the process of recognising, monitoring and ranking risk according to sets of organisational criteria.

2.3.3 Threats and risks associated with people

Although people are considered as assets to help reduce information risk, they are also the main threat to the information system security (Bulgurcu et al. 2010; Rotvold 2008). People who attack a computer system can be characterised in many different ways, the most common ones are:

A hacker is a person who gains unauthorised access to a computer system without any intention to damage it (Rouse, 2013). A hacker could be a white hat, a blue hat, black hat or a grey hacker. PC Magazine Encyclopaedia (2013) defines a white hacker as the “good guy” and could be either a concerned employee or a security professional that is paid to find the vulnerabilities of a computer system. A blue hat hacker is a security professional employed by Microsoft to find the weaknesses in Windows. The USLEGAL website (2013) defines a grey hat as a skilled hacker who is a combination of white hat and black hat and acts for offensive purpose or defensive purposes. A grey hat usually does not have a malicious intention but sometimes may commit a crime during a course of technological exploitation. However, a cracker or a black hat is a person who gains unauthorised access to a computer system for malicious reasons.

According to Pfleeger and Pfleeger (2007), three components are necessary for an attack: method (the tool and techniques the attacker uses), opportunity and motive. Knowing the motive could give an idea of who would attack the system. Challenge, power, fame, money and ideology are the most common motives for attacking a computer system (Pfleeger and Pfleeger, 2007).

Most Saudi Arabian universities use the networked information system software, Banner. It is possible that a failing student could get into this system and change their grades into

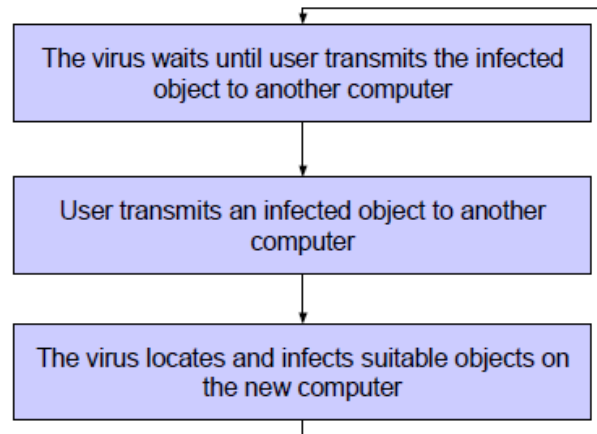
passing grades. According to the UC Davis website (2011), the Banner students information system contains all the information about students records and if the student is an evil cracker, then the Banner system would be the system to hack and change information in it such as student grades. The fact that hacking instructions are available for free online from YouTube exacerbates this problem.

2.3.4 Technology Risk

Technology is the scientific knowledge of methods, systems and devices used for practical purpose. According to Liang and Xue (2009), technology is a double edged sword. It can help improve the organisational performance when it is applied for virtuous purposes. However, when it is used for malicious purposes it can damage individuals, organisations and society (Liang and Xue, 2009). Software is a technology that can be harmful, such as malicious code. Every product, whether software or hardware, has vulnerabilities, when exploited, that can lead to extensive damage (Keller et al., 2005).

Malicious code is programming software that can access and change data and programs maliciously while the user is unaware (Ballou, 2003). Examples are viruses, Trojan horses, bots and worms. Nearly 162 million malicious files were reported in 2012 by Microsoft (Laudon and Traver, 2012) and more than two million new malware programs in the Internet were reported by security firm G Data, (Laudon and Traver, 2012).

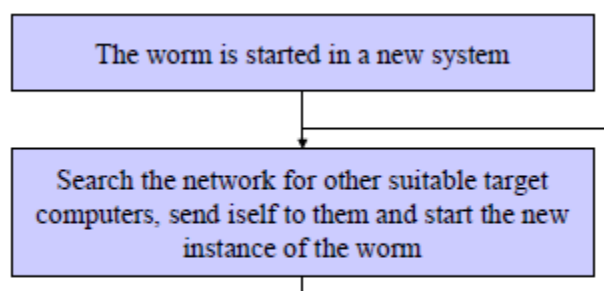
- **Viruses** are programs that can automatically make copies of themselves and spread to other users. The spreading of a virus depends on both the virus technical features and the computer user behaviour (F-secure, 2001). They need a carrier like a file to spread, as shown in Figure 2.2. To users, they look like normal programs but they attach themselves to a transmitted file to create unwanted and unpleasant results (Keller et al., 2005). According to the Computer Security Institute (Keller et al., 2005), based on an annual survey (Gordon et al., 2004) of mid- to large-sized companies, 40% of the total loss from security damage, equal to \$141,496,560, was done by a virus. In the 2002 Computer Security/FBI survey of Computer Security Issues and Trends, the top three causes of financial loss were viruses, laptop theft and Net abuse (Wylder 2003).



Source: whitepaper F-secure Corporation 2001

Figure 2.2: a typical life cycle of a computer virus

- **Worms** are computer programs that work alone without the need for human intervention or a host program and make a functional copy of themselves to create damage in a similar way to computer viruses (CISCO, 2014). They spread by using the breaches on a big system or by social engineering, (CISCO, 2014). The difference between a worm and a virus is that viruses depend on human intervention or a host program to spread, whereas worms don't depend on these factors, see figure 2.3. Therefore, a worm can spread faster than viruses, (F-secure, 2001).



Source: whitepaper F-secure Corporation 2001

Figure 2.3: a typical life cycle of a computer worm

- **Bot (short for Robot)** is a virus program design to interact with networks services to control infected networked computers or computers connected to the internet from outside sources (CISCO, 2014). Huge numbers of Bots can be put on a server (Bot network) for the purpose of command-and-control. This bot network can be used for phishing fraud, spam mails or DDoS attacks (Distributed Denial-Of-Service attack) which is when a number of electronic systems attack a specified system causing denial of service for that system's users (IPA, 2006).
- **A Trojan horse** is a software program, named after the Greek's horse used in the Trojan War. It is a program which appears funny or useful and does what the user needs but contains hidden malicious code that is designed to harm the user's computer (Bowles and Hernandez-Castro, 2015). This can happen to anyone using the World Wide Web who has not protected their computer with any anti-viruses programs (Durkota and Dormann, 2008). Unlike a virus or worm, a Trojan does not replicate itself.

This section has identified some of the potential threats, risks and attacks that could threaten the security of the information system. The research considers these as potential threats to the information security system to most universities in Saudi Arabia.

2.4 Laws and regulation for IT

The law is a system of rules established in a country or community to regulate the actions of its members and which may be enforced by the imposition of penalties (Oxford Dictionary, 2013). Cyberspace needs legal measures, coordination and cooperation, as it is considered the fifth common space, after land, sea, air and outer space (Schjolberg, 2012). A new international legal mechanism is needed for protection against global cyber-attacks and other global cybercrime. As cyber-attacks increase, the international community should be aware of the need for a global response (Schjolberg, 2012).

Saudi Arabia has its own law against cyber-crime. In March 26th 2007 a royal decree no. M/17 8 Rabi 1 1428 / 26 March 2007 decreed the Anti-Cyber Crime Law. This law aims at

combating cyber-crimes by identifying such crimes and determining their punishments to ensure the following:

1. Enhancing information security.
2. Protecting the rights of legitimate use of computers and information networks.
3. Protecting public interest, morals, and common values.
4. Protecting the national economy.

This law can be found online on the MCIT website. However, it is not known to the majority of Saudi citizens. According to AlQahtani (2016), Saudi Arabian online users don't know that they are committing cyber-crime that could lead them to jail since they are not aware of Saudi Arabia cyber-crimes. This law needs other ways to publicise it, such as TV advertisements, to make sure it is known to all online users.

In this research, laws and regulation are considered as legal measures to regulate the action of Saudi Arabian citizens in information security. Compliance with the law should contribute to a successful development of a strong information security system.

2.5 Implementing Information Security

The word 'implement' means putting into effect or the fulfilment of a course of action, process, or method to do something (Oxford Dictionary, 2013). Thus, implementing information security is to carry out and put into effect a process, method, or design to protect confidentiality, integrity, authenticity, availability and reliability of information. Xiaoyana, Yu-qing, and Li-lei (2011) express that developing, monitoring, reviewing and improving a set of controls, such as policies, procedures, hardware and software security mechanisms, are important in implementing information security. Veiga and Eloff (2007) state that information security is made of three controls: technical controls, such as passwords, biometrics and firewalls; process controls, such as policies; and human behaviour controls, such as regulation and training. They also believe that technical controls alone cannot relieve threats to information and that processes and human behaviour should be considered when implementing information security.

The organisation is responsible for choosing suitable security controls, making security controls appropriate, and ensuring that the security controls meet the organisation's security requirement (Locke and Gallagher, 2011). Höne and Eloff (2002a) believe that in order to accomplish effective information security in an organisation, controls and measures such as technical controls, regulation agreement and management involvement need to be part of the implementation process. A successful information security programme is a combination of technical solutions such as firewalls, passwords and non-technical approaches such as policies and human behaviour controls (Wylder 2003). Wylder (2003) adds that implementing information security can be achieved in three steps:

- First, implement a complete plan that evaluates the risks and threats to the organisation.
- Next, implement a set of policies and strategies to control those risks.
- Finally, supervise and compel the use of the policies and procedures.

Salton (1980) adds that securing information privacy is not just a technological issue, but is also social, legal, and political, where social and technological issues are often inseparable. For this reason, certain technological policies dealing with the confidentiality and security of stored information include a description of the principal nontechnical privacy issues and an examination of the existing legal framework dealing with the privacy problem (Salton 1980).

Understanding the maturity level in security information is another way that helps an organisation improve its current information security (Xiao-yana, Yu-qing and Li-lei, 2011). Xiao-yana, Yu-qing and Li-lei (2011) presented three maturity models that help an organisation decide the extent of their information security (see Table 2.1):

1. the Systems Security Engineering-Capability Maturity Model (SSE-CMM);
2. the Control Objectives for Information Related Technology (COBIT) Maturity Model;
3. the National Institute of Standards and Technology (NIST) Maturity Model..

Table 2.1: Three Maturity models to improve information security
Adopted from Xiao-yana, Yu-qing, and Li-lei (2011)

Maturity Model	Levels	Focus
SSE-CMM Model	<ol style="list-style-type: none"> 1. Conducted informal design 2. Planned and tracked 3. Well defined 4. Quantitatively controlled 5. Continuous improvement 	Safety of the design engineering software
COBIT Model	<ol style="list-style-type: none"> 0. Non-existent 1. Initial/ad hoc 2. Repeatable but intuitive 3. Defined process 4. Managed and measurable 5. Optimized 	Specific audit procedures
NIST Model	<ol style="list-style-type: none"> 1. Policy 2. Procedure 3. Implementation 4. Testing 5. Integration 	Documentation

As seen in Table 2.1 there are three maturity models, each with different levels of maturity and each has a different focus. For example, the SSE-CMM model focusses on the safety of information security engineering software design. It has five levels including directing informal design, planning and tracking, defining, controlling, and continuously improving the safety of the design of information security. Whereas, the COBIT model focuses in auditing information system processes with five maturity levels that describe the possible state of the process. The NIST model focuses in the documentation needed in an organisation. Each level in all models must be complete before moving to the higher level. The SSE-CMM model, the COBIT model and the NIST model each has different focus and developed separately from each other but need to interact with each other in order for them to perform best.

According to GAO (2011), weaknesses in information security policies and practices such as access control, configuration management segregation of duties, continuity of operations and security management, place the confidentiality, integrity, and availability of sensitive

information and information systems at risk. There is a need to strengthen information security by strengthening controls over technology, security policy and people. Effective Information security can be achieved by the integration of technical controls, policy control, and people controls, and each will be discussed in detail in Sections 2.5.2, 2.5.3 and 2.5.4. Section 2.5.1 covers auditing techniques.

2.5.1 Auditing

An audit is the process of providing official assessment or examination of a person, organisation, systems, process, or product. Auditing, according to Wright (2007), has two types, internal and external, in which internal auditing is a feedback process based on auditor advice after auditing a system. However, external auditing is undertaken by external parties and will provide a report of a feedback of the overall process and no advice. The success of the information security management depends on the auditing process. Information security auditing is a tool used to achieve an adequate level of security in an organisation (Kohzer, S. et al., 2016).

Auditing involves identifying and evaluating the management of organisational assets, information, and resources, computers and networks, to fulfil set of standards, policies and regulations (Caballero, 2006). There are three types of audit:

- **Self-auditing:** This is undertaken by special software applications that monitor IT systems and report on the security status according to the organisation's security policy. These applications can send an alert message, lock an account, and undo an event, when an unauthorised security action occurs.
- **Internal auditing:** This is undertaken by employees from the organisation who perform the audit, possibly with the help of an outside company.
- **External auditing:** This is an independent audit undertaken by third party firms. The advantage of this kind of auditing is that it is not prejudiced. According to Caballero (2006), external auditing is disinterested and not biased.

2.5.2 Technical controls

Technical controls can be defined as user authentication and authorization, logical access controls, antivirus software, and firewalls. They are the building block of computer security that prevent unauthorised people or processes from entering an automated information system (Caballero, 2010). According to Dillard, et al. (2006), there are different kinds of security technical controls, depending on their complexity. In addition, technical controls can be divided into two different categories: preventative controls, including authentication, authorisation, cryptography, access control and protected communication, and detective and recovery controls, including audit systems, antivirus programs and system integrity tools. Operational considerations are important when implementing technical controls and they should be coordinated by the organisation's security management (Caballero, 2010). Technical controls that will be covered in this section are preventive controls and detective and recovery controls which are discussed in the subsections 2.5.2.1 and 2.5.2.2.

2.5.2.1 Preventive controls

A preventive control is the process of preventing errors from occurring through the use of authentication, authorisation, access control and protected communication. Authentication is a process of legitimizing the credentials of a person, computer, process or device. Authorisation is the process of allowing a person, computer process, or device access to certain information or services. The identity of the person, computer process or device requesting access and authorisation is checked through authentication. Examples of authentication technologies include, but are not restricted to, cryptography, digital signatures, biometric data and passwords. Some of these examples are described in more detail as follows:

- Passwords were the first type of technology based and were initially introduced in the early 1960s (Diffie 2008). Pfleeger and Pfleeger (2007) expressed that although the password is the most common authentication mechanism to secure systems, people derogate its quality. According to Banks (1990), an individual should choose

their password and this password should be regularly changed; it should be no less than eight characters, and must be used by its owner only.

According to ABC chief business and economic correspondent, Garbs (2013), passwords are the codes that are supposed to keep all online personal information safe. Garbs found out that, today, 90% of the passwords created are vulnerable to hacking, based on an ABC interview with Pozadzides, an international security expert, who explained that hacking, can happen to companies and people all the time and it takes a hacker minutes and sometimes seconds to get someone's personal passwords. Some of Pozadzides' password tips were:

- 1- Use a password 8 or 9 character long.
- 2- Never use a name, obscenity, or common words such as 'love' and 'god'.
- 3- Use symbols such as an asterisk and capital letters. This could change the time to hack the password from minutes to days and years, the more unique the harder to hack.
- 4- Never use the same password twice.

Hunt (2011) believes that the only secure password is the one that you cannot remember and it can be achieved by doing the following:

- 1- Create a unique password and never use the same one twice.
- 2- Use different characters such as uppercase lowercase letters, numbers and punctuation.

- **Cryptography** is a secret encoding of writing used to secure the confidentiality of communication. However, cryptography is unable to carry out most of the functions asked of it today (Diffie 2008). Computer based cryptography started in the 60s where protecting the operating system focused on the cryptographic algorithm (Trčcek et al., 2007). World War I marked the beginning of mechanical cryptography. In World War II, electromechanical machines were used to combine modular arithmetic with a number of table lookups in most military mechanized cryptography (Diffie 2008). The more the knowledge of cryptography the more effective it could be. Cryptography has five primary functions (Kessler, 2017):

- Privacy: make sure that only the intended receiver is able to read the message.
- Authentication: a process used to ensure one authorised identity
- Integrity: make sure that the original message has not been altered when received.
- Non-repudiation: a mechanism used to ensure that the message is sent by the real sender.
- Key exchange: the use of crypto keys between the sender and receiver.

There are three different types of cryptographic algorithms (figure 2.4).

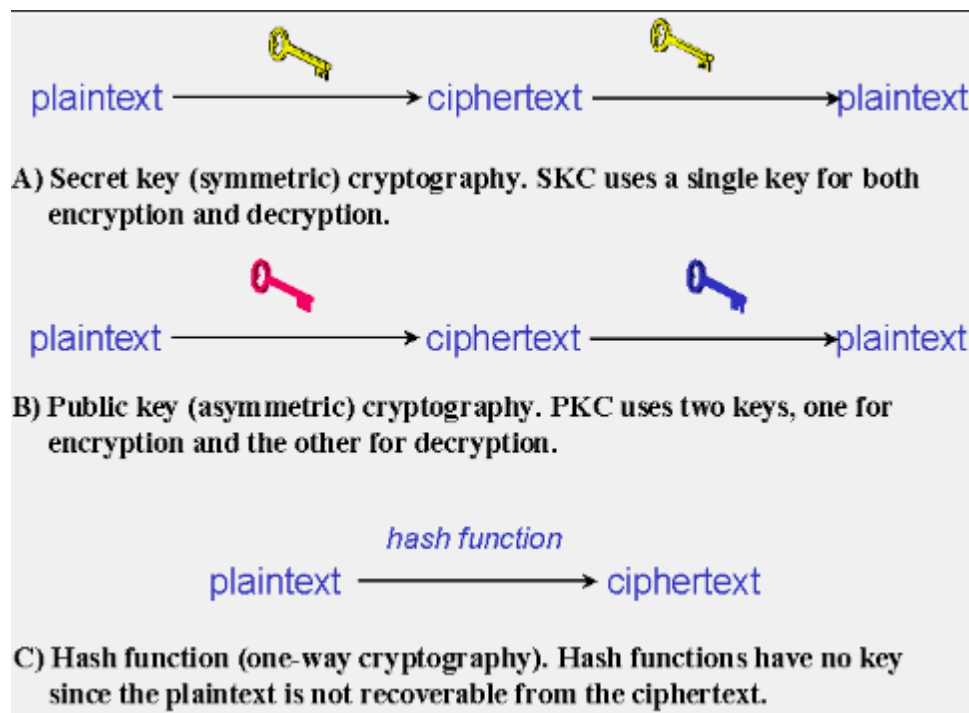


Figure 2.4: Three types of cryptography: secret-key, public key, and hash function adopted from Kessler (2017).

According to figure 2.4, secret key/symmetric cryptography algorithm (SKC) is used to ensure privacy and confidentiality of the message and only the intended receiver can read the message by the use of a single key for both encryption and decryption. A public key/ asymmetric cryptography algorithm (PKC) is used to ensure the authentication, non-repudiation and key exchange by the use of two keys, one key for en-

ryption and another for decryption. Hash Functions are used to ensure the integrity of the message sent by the use of a digital fingerprint mathematical transformation to irreversibly "encrypt" information.

- **Biometrics** is used to verify the identity of an individual, based on physical or behavioural characteristics. The most common biometric devices are thumbprint or fingerprint, retinal scan, voice scan, and digital signature which is a data string used to assign a digital message to only one individual.
- **A firewall** is a device that is able to control access and traffic at the application level (Snyder 2012). A firewall's main process is to traffic filtering the information between an organisation's trusted networks and the outside untrusted networks (Pfleeger and Pfleeger 2007). Laudon and Traver (2012) state that firewalls are hardware and software that protect the network based on security policies, from untrusted communication networks.

2.5.2.2 Detective and recovery control

Detective controls and recovery are controls that are designed to detect and correct errors when they have occurred. They include anti-virus programs and useful software, such as cloud computing and sandboxing, that helps protect and secure computer information from any kind of attachment. Examples of useful software are:

- **Anti-virus software** is utility software made to protect computers from malicious software such as viruses, spyware and Trojan horses. Some factors are important in measuring the performance of anti-virus programs, such as usability and efficiency; some anti-virus suites are user-friendly, and some use the computer's resources more efficiently (PC World, 2012).
- **A Sandbox** is software that acts as an isolated environment while running unfamiliar programs and processes (Geier 2012). Sandboxing applications perform as an additional set of protection for a computer. Geier (2012) added that having sandboxed software can protect an information system from malware, which could

be mishandled by the current anti-virus utilities, giving extra protection to the computer information when working online or accessing suspicious websites.

Although technical controls are important for the security of information systems, they are not enough to give complete security (Salton 1980). Other controls are necessary to reach a complete secure environment for information assets (Salton 1980). A documented information security policy is a necessary control for a comprehensive information security, explained in the next subsection.

2.5.3 Security policy controls

Information security policy is defined as a high-level document that provides definitions of the broad boundaries of information security in an organisation (Höne and Eloff , 2002b). Information security policy identifies information as a valuable asset in an organisation, and provides guidance to perform safe and secure business functions (Kadam 2007). Palmer et al. (2006) define Information Security Policies as:

“Policies are brief technology- and solution-independent documents. They provide the necessary authority to establish and implement technology- and solution specific standards. In general, policies remain relevant and applicable for a period of time, and only require revisions when there is a fundamental change to an organisation’s business or operational objectives and environment.”

The effectiveness of information security policy depends on helping the employees understand the rights and responsibilities of information resources, focusing on the safety and security of information handled in daily tasks (Höne and Eloff , 2002b). The most important part of security policies is the documentation, which is a set of directional rules defining the acceptable level of information security in organisations. It is essential for employees and other business partners to conform with information security policy rules (Yildirima et al., 2010).

Implementing an effective information system security policy is essential for an information security programme. The information security programme of an organisation relies on a well-designed information security policy to be trustful (Kadam 2007). Tracy (2007) believes that organisations should implement the information security policy first, before exploiting information security solutions. However, if most organisations already have their technical information security, such as firewalls and anti-virus systems, then the organisations need to establish their security goals and formulate policies that take existing tools into account.

Höne and Eloff (2002b) believe that an effective information security policy would directly result in effective information security. However, writing information security policy that meets the organisation's mission and vision is not an easy task. Various supporting activities should be considered when writing the information security policy and they should focus on user's needs - from the writing style and the way in which it is displayed, to the dissemination of the document. Users' needs should influence information security policy documentation and any other documentation activities, such as the writing style, the way in which it is presented and the distribution of the document (Höne and Eloff, 2002b). For example:

- **Styling** of the document, which describes the style of writing. The style and tone should be clear and user friendly to make sure that the information policy is easy to understand and use. It should fit the original style of the rest of organisation official documents, not just 'cut and paste', to eliminate the risk of providing unfamiliar information security policy document.
- **Developing** of the information security policy should be conducted with representatives of all the stakeholders who need the policy to succeed. In order to be effective, the development of the security policy should be accepted by all.
- **Presenting** the document should be interesting and get the users' attention.
- **Committing** top management and all levels of an organisation is important, in order to have an effective information security policy.
- **Disseminating** can be done through distributing either hardcopies or softcopies of the document, the document on the intranet, or a summary of the policy in brochures.

- **Maintaining** a security policy should grow and develop in conjunction with the organisation development and growth, to make sure that it can sustain the fulfilment of the organisation's vision and mission (Figure 2.5).

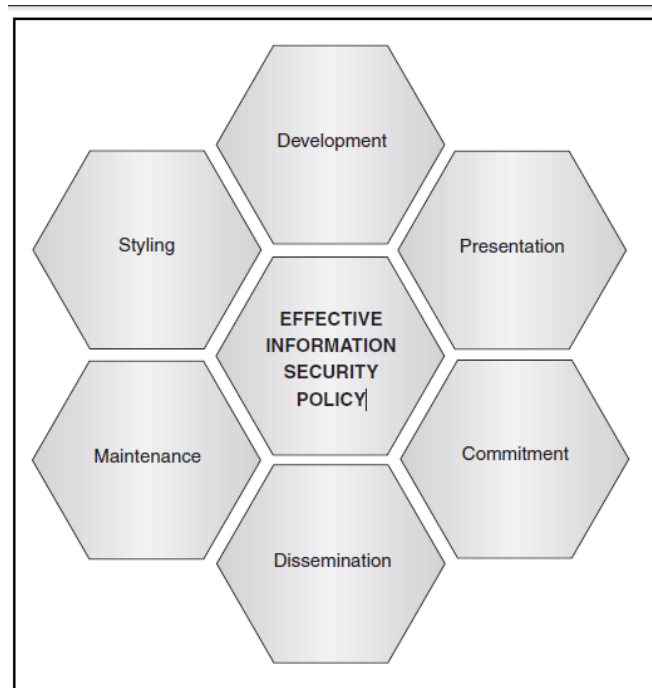


Figure 2.5: Supporting Activities for Effective Information Security Policy adopted from Höne and Eloff (2002b)

ISO/IEC 27001 (2005) and BS ISO/IEC 27002 (2005) define an information security policy statement as “management’s commitment to the implementation, maintenance, and improvement of its information security management system.” Kark (2008) define policies as documents of direction to control corporate behaviour. Each organisation should implement their security policy’s rules, which are different from any other organisation (Yildirima et al., 2010). Höne and Eloff (2002b) agree that a security policy document is not always easy to write because of the different opinions within the organisation as to what constitutes a policy.

The information security policy should be comprehensive, including all information system elements such as data, programs, computers, networks, facilities, people, and processes.

Confidentiality, integrity and availability are security parameters used to measure the security value of each element and the need to protect them, and that varies between different organisations (Chandra 2008). Part of information security policy is confidentiality policy, where users of the system are specified and so are those who are not allowed access (Biskup et al. 2004).

An information security policy structure provides an organisation with brief, as well as extensive, planning security solutions to protect organisational objectives (Palmer et al., 2006). Users of information resources at all levels of an organisation need a documented information security policy to clarify the need for Information security. It should supplement the organisation objectives and emphasise that the aim of organisation management is to have a controlled and secure environment (Höne and Eloff 2002b). A well-written manual or automated procedure should be made available that covers all security violations, reasons for their occurrence, and recurrent incidents.

Xiao-yana, Yu-qing, and Li-lei (2011) point out that ISO 17799 deals with objectives and activities of security policy that complement business objectives:

- *“Clear management commitment and support*
- *Proper distribution and guidance on security policy to all employees and contractors.*
- *Effective 'marketing' of security to employees (including managers)*
- *Provision of adequate education and training.*
- *A sound understanding of security risk analysis, risk management and security requirements.*
- *An approach to security implementation, which, is consistent with the organisation's own culture.*
- *A balanced and comprehensive measurement system to evaluate the performance of information security.*
- *Management and feedback suggestions for improvement.”*

Tracy (2007) believes that information security policy should be developed first before investing in information security technical solutions. However, since most organisations al-

ready have their technical information security, such as firewalls and anti-virus systems, then the organisations need to establish security policies that take existing technical security into account.

Implementing a clear, easy to use, and effective Information security policy will increase the effectiveness of the information security. It should be developed first before implementing any of the information security controls.

2.5.4 People controls

People may have significant influence in security strategy. People in information security should involve government regulators, shareholders, customers, employees and business partners (Vijayan, 2005). According to Son (2011), security management is significantly influenced by people; therefore, the aim of any organisation should be to focus on engaging employees in the improvement of the performance of security in organisations. Human factors have great influence in information systems security. Therefore, security technology, human behaviour and organisation security policies need to be considered to obtain effective security in enhancing the performance of information systems (Trčcek et al., 2007). The effectiveness of controls in a security system, such as security technology, organisational security policies and procedures and government regulations and laws, depend on the compliance and contribution of the users, especially employees within the organisations (Hu et al., 2011).

Son (2011) explains that there is a positive relationship between people motivation and the performance of security in which motivating the employee improves the performance of the security so motivating employees improves security in organisations. Spears and Barki (2010) state that users may be a valuable resource for information security by providing needed business knowledge that contributes to more effective security measures, and it is necessary to engage users in protecting sensitive information in their business processes. Therefore, when people engage in the classification, analysis, design, implementation, test-

ing and monitoring of security controls within their organisation, they help improve the information security system (Spears and Barki 2010).

Most information system security problems are created by people. Wylder (2003) recognises that 80% of the information security problems are made by 20% of the people. Veiga and Eloff (2007) found that people's behaviour and the information security culture within organisations have to be recognised, since they are the causes of most information security problems in any organisation. Rotvold (2008) expresses that technological methods of protecting information may be effective; however, some of the information losses are not caused by a lack of technology or defective technology, but rather by people's use of technology and user behaviour flaws. "People can be a threat because they can be involved in intentional abuse (e.g., data theft, data destruction, etc.) or unintentional or accidental events (e.g., forgetting to change a password, forgetting to log off, etc.)," (Son 2011). People can not only be part of the problem, but they can, and should be, part of the solution. People must be part of any organisation's information security protection system.

The phrase "the weakest link" has been used by many information system researchers, when talking about people. According to Spears and Barki (2010), people are considered to be "the weakest link" in information systems security management in an organisation. They unintentionally use information systems in unprotected ways in which they could cause violation of security policies. Few studies, however, have focused on the reasons why users engage in the violation of security policies behaviour (Guo et al. 2011). Many organisations found that their people's compliance with information security can help minimise information security risks, even though they are considered as the weakest link in information security. Therefore, understanding employees' compliance behaviour is crucial for organisations, to strengthen their information system security (Bulgurcu et al. 2010). People are still the weakest link in an organisation since people errors and negligence can help outside attacks to threaten the organisation (Hu et al. 2011).

This section has identified the information security controls of technology, security policy and people. The integration of technical controls, policy control, and people controls can lead to effective Information security system. Some considerations that are needed to im-

plement a successful information security system are presented in this section and could be used as a guideline to implement university information policy at Saudi Arabia. These actions and policy could minimise and overcome threats and dangers to a university information system in Saudi Arabia.

The involvement of employees in implementation of information security helps minimise security risk and strengthen the information security system. Special attention should be paid to how to encourage people to be part of the information security system as human compliance is essential to the success of the information security programs.

2.6 Human Compliance

The Oxford dictionary (2013) defines compliance as “action or fact in accordance with a wish or command.” Human compliance is an organisation's business related commitment to laws, regulations and policies, in which, if violated, often results in legal penalties (Rouse, 2013).

Information security policy is considered the most fundamental control in information security it should be part of an overall organisation security policy. People involved in responsibilities contained in security policy must understand and accept it (Banks 1990). Security policy documents contain guidance on threat and risk estimation, control development and compliance authority and liabilities for information security (Chandra 2008).

Human compliance can have a positive influence on the implementation of information security policy. The aim of information security professionals should be to form and document security policies and ensure policy compliance (Wylder, 2003). Employees should understand that compliance with the information security policy is not a choice nor should it be left to chance. Compliance should be enforced for everyone at all levels of the organisation and the consequences of failure to comply should be made clear. Documentation and management enquiries should help auditors ensure employee compliance to information policy by determining if there is a compatible mechanism that outlines the authority and responsibility for information security. Moreover, adequate measures such as incorporating employ-

ees' compliance in their job descriptions should be included in the organisation security policy. Vance, Siponen, and Pahnla (2012) found that, based on the result of "an empirical test habitual (a routinized form of past behaviour)", information systems security compliance strongly reinforces the employee intention for future compliance. Past studies have not considered that an employee decision to comply is affected by the influence of past and automatic behaviour, even though past behaviour has strongly affected decision-making (Vance, Siponen, and Pahnla 2012).

Information technology security managers and the organisations must not underestimate the risk of employees' failure to comply with IS security procedures. Therefore, different approaches have been developed to ensure and enforce employee compliance.

2.6.1 Approaches to ensure compliance

Employee compliance is crucial to success of information security policy. Therefore, special approaches are needed to enforce employee compliance. Moreover, effective communications with people and human resources management are necessary (White 2009). Human compliance can be approached by considering laws, ethical principles, codes of conduct and society-driven needs (Spears, Barki 2010). An ineffective security solution can be the result of users' failure to comply with IS security policies. Employees who are not willing to comply with information security policies could jeopardize the company's assets. Therefore, in order to increase users' compliance to the IS security policy, effective communication about the IS security policy compliance is advocated by Puhakainen and Siponen (2010). Different IS security policy compliance approaches have been suggested, such as training and education, sanctions and enforcing compliance with an annual personal performance plan, to increase employee compliance.

2.6.1.1 Training and education

Training is considered the most effective IS security policy compliance approach. According to Puhakainen and Siponen (2010), different types of people need different and advanced

education and training in order to obtain more effective compliance. Security management professionals should insist on close education and training, since education and training are necessary to reach the skills the business needed to prevent companies from new threats (Hill, 2007). Recent research, based on human behavioural theories, has suggested the development of comprehensive information security policies and procedures and the provision of training for employees (Hu et al., 2011). However, it is not an easy task to create an effective training programme. Effective training needs the following (Dalto, 2014):

- Assessment
- Recognise participants' different learning characteristics such as:
 - Being self-directed
 - Being goal-oriented
 - Liking task-oriented training
 - Needing to be respected
 - Liking relevant training
- A list of learning objectives that the participants achieve after the training is completed.
- Training evaluation.

2.6.1.2 Sanction

Information security policy violations involve the use of computers, hardware and software, against an organisation security policy. However, having security policy sanctions could reduce computer misuse and improve employee compliance. Hu et al., (2011) state that according to recent research, based on human behavioural theories, creating sharp and easily understood security sanctions would minimize and stop future security policy violations by employees.

Siponen and Vance, (2010) state that sanction is suggested by a number of studies to minimize computer misuse and increase employee compliance with IS policy. To understand employees' refusal to comply with the IS security, deterrence theory and sanctions, were used by a number of IS security researchers (Siponen and Vance, 2010). Son (2011) states

that number of studies have been done using deterrence theory in order to understand employees' violation or compliance with security rules in an organisation.

2.6.1.3 Annual personal performance plan

People have played a significant role in managing information security. Therefore, different approaches have been used to encourage employees to improve the performance of information security in an organisation. Wylder (2003) discusses a new approach to enforce policy by integrating employee compliance with annual personnel performance, see Figure 2.6.

EXHIBIT 1 Personal Information Security Plan		
XXX Company		
Personal Information Security Plan		
Date:		
Plan period From:	To:	
Employee Name:	Location:	Network user ID:
1. Home computer profile		
Computer make, type (if a laptop is used, describe the type of locking mechanism used):		
Home ISP: AOL___ WorldNet___ MSN___ Earthlink___ Other___		
Access type: Dial-up___ DSL___ Cable modem___		
Number of times a week used for work:		
Home network (if applicable): Ethernet___ Token Ring___ Wireless___		
2. Home protection profile (Please describe methodologies or technology used at home to protect computers and networks.)		
Anti-virus software (vendor, version):		
Personal firewall (vendor, version):		
Other:		
3. Annual security plan goals (List courses to be taken, preventative measures to be undertaken in the upcoming year. Include skills courses, awareness courses, and any continuing education classes that are applicable.)		
I agree that this accurately represents my use of corporate computer resources. In addition, I have read and understand the corporate information security policies for my position.		
_____ Employee Signature		_____ Manager Signature
This section to be completed by supervisor:		
From annual security audit describe any security violations or compliance issues:		
Numbers of time passwords were manually reset:		
Number of violations of Web access policies (if any):		
Indicate any involvement of employee in any audit points:		
Changes in employee access profile or security clearance:		

Figure 2.6: Personal Information Security Plan adopted from Wylder (2003)

Figure 2.6 shows a personal information plan that can be used to enforce employee compliance with information security policy. The use of this plan can help an organisation control their end users external access, know about the user's external network used to access the organisation's systems and know how secure their users' personal computers are and which antivirus software or firewall they are using for security. The personal information plan can also raise the level of information security awareness among end users as, by filling in this personal information plan, the users would enable them to recognise the type of their access network, the security of their personal computer and the number of times they violate the access web policies. The disadvantage of this plan is that it does not include the type of violation of web access policies.

Puhakainen and Siponen suggested that future research is needed, focusing on achieving a positive behaviour in employees' compliance with IS security policies. Future research should also focus on testing the use of change agents and IS security campaigns in increasing compliance of employees with IS security policies. According to Hu et al., (2011)

“With this understanding of employee information security behaviour, our results reveal what might help companies effectively reduce the policy violations by employees: lowering the perceived value of the data assets in corporate information systems and screening for individuals with high self-control and high moral standards.”

Human compliance can be a potential barrier to a successful implementation of a university information security system in Saudi Arabia. However, some of the approaches and techniques presented in this section, such as the use of annual personnel performance, can be used to ensure and enforce employee compliance at any knowledge-intensive organisation in Saudi Arabia.

The areas covered by the previous sections all need to be addressed through information security management, and the managers responsible need to believe in the need for comprehensive processes to be in place in order to convince others to take security seriously.

2.7 Management and information security

Information security management can be defined as the managing of all the policies, procedures, plans, processes, practices, roles, responsibilities, resources and structures that are used to protect and preserve information. It includes all of the elements that organisations use to manage and control their information security (ISO/IEC 27001, 2005 and BS ISO/IEC 27002, 2005). Management involvement in the implementation and the development of information security is essential for the fulfilment of the organisation's vision and mission. Top management approval of an information security policy would strengthen the commitment of an organisation toward security and expand knowledge of security needs. To reach

an acceptable level of information security, an organisation's senior management needs to be involved (Veiga and Eloff 2007). Information security in an organisation can be accomplished by having an infrastructure approach at management level. Just as information and data characteristics are different at the different levels of management, information security has different characteristics at the different levels of management (White 2009). Therefore, senior management must recognise and endorse the need for a formal policy and controls. A policy statement should be considered as an organisation policy, and it should be signed by the board of directors. The involvement of senior management in enforcing the employees' compliance tends to lead to positive outcomes (Wylder 2003).

The improvement of the communications and operations management and security policy has significant benefits on other security elements in an organisation, such as organisational, personnel and physical and environmental securities (Yildirima et al., 2010). A company's security policies should be considered as a security requirement that should be documented, measured, assessed and reported to the organisation. It should be a priority aim for information security management. Effective security is achieved by encouraging and assessing positive behaviour rather than protecting information from threats and damage (Tracy, 2007). Management should also be involved in the security auditing programme.

It can be concluded that it is important for management to be involved in the process of information security. Management should make sure that an information security system is performing against a set of organisation standards and policies. Management should also make sure that all employees understand the importance of information and the risk of not protecting it and that all employees are involved in the implementation of an information security system.

This section shows that senior management support and involvement can lead to a successful implementation of information security systems. To achieve the objectives of this research, senior management support is considered as a necessary action to strengthen the implementation of a strong information security system at PNU or any other university in Saudi Arabia.

2.8 Information security in Saudi Arabia

In Saudi Arabia and Arab Gulf States, one of the major motivations to introduce information technology (IT) was to support a new policy of controlling the flow of foreign labour. This had been adopted because of economic and social problems which started appearing as a result of the uncontrolled flow of foreign labour (Al-Gahtani, 2003). However, the rapid development of information technology is challenging for Saudi Arabia. In 2003, Saudi Arabia realised the importance of digitalising government information. Therefore, a royal decree no. A/2 was issued in May 2003 to change the name of the Ministry of Posts, Telegraphs and Telephones (MoPTT) to the Ministry of Communications and Information Technology (MCIT). The goal of this transfer was to be part of information society. Also in 2003, and based on Saudi Arabia Royal Decree (7/B/2427) dated 16/1/1424H, the Ministry of finance was instructed to establish an e-government programme. In 2005 two Saudi Arabian Ministries, the Ministry of Communication and Information Technology (MCIT) and Ministry of Finance were joined to establish an e-government programme called YESSER. According to the YESSER website (2014), the YESSER programme's objectives were:

- *“Raising the public sector’s productivity and efficiency.*
- *Providing better and easy-to-use services for individual and business customers.*
- *Increasing return on investment (ROI)*
- *Providing the required information in a timely and highly accurate fashion.”*

The government of Saudi Arabia decided to make the transition to e-Government mainly because of the enormous benefits to the national economy (YESSER website, 2014). Another essential reason for organisations' adoption of IT is because of the increased need for the Internet and electronic commerce (Al-Gahtani, 2003). However, user acceptance of the information technology transformation should be considered as a priority for this adoption of IT to be achieved. Most organisations aimed to improve the performance of employees by using information technology and the end users just had to accept it (Al-Gahtani, 2003). However, the slow spread of IT in developing countries could be a problem due to poor infrastructure, high costs, language barriers, social factors and politics (Al-Gahtani, 2003).

In 2011, because of the Saudi Arabia Ministry of Communications and Information Technology (MCIT) awareness of the importance of securing information assets and infrastructure, it approved the development of a National Information Security Strategy (NISS) project. The NISS project objectives were (MCIT website, 2011):

1. To provide the ability to use and share free and secure information.
2. To improve online information security, safety, and integrity to encourage more use of information technology.
3. To develop flexible information systems.
4. To enhance awareness and education on security risk and information protection.
5. To develop national guidelines and policies for information security management, risk management and business continuity based on international standards and best practices.

2.8.1 Information system outsourced in Saudi Arabia

Most Saudi Arabian organisations have hired outsourcing companies to either do partial or total development of information systems and security activities, usually the development and maintenance of the software, hardware, and integrated information systems, and the training and education of staff and end users. According to Abu-Musa (2011), most of the organisations in Saudi Arabia are either partially or totally outsourcing their information systems and IT. In order to minimise the outsourcing risk of failure to accomplish their mission, Saudi organisations prefer to have more than one supplier. The most significant advantage of Saudi organisations outsourcing information systems and IT is to improve information technology in an enterprise. Other advantages would be to enhance the quality and efficiency of information services and to have professional information systems and IT personnel.

The main disadvantages of outsourcing information systems and IT in Saudi organisations would be the lack of credibility of service providers, a lack of protection and enhancement of the confidentiality and security of information, mishandling of a company's secrets and

intellectual property, and the fact that many of the outsource workers are unqualified and unprofessional in handling occasional and unexpected problems (Abu-Musa 2011).

An example of an outsource company in Saudi Arabia is Cisco System Inc. In 2006, Saudi Arabia revealed five year, \$265 million plans with Cisco System Inc. The plan was to create jobs for about 530 employees, to open a technology and contractual demonstration centre, and to contribute networking equipment and training services in low-income areas of the country (Gross, IDG News Service 2006). Gross also states that, according to Chambers, “Cisco plans to provide space for Saudi start-up companies and R&D operations, plus equipment, training and support services for Internet connections to 2,000 homes in underprivileged areas.”

Saudi Arabia is still one of the developing countries that has relatively recently started to use interconnected computer networks. Protecting information systems has been recognised by the Arabia Ministry of Communications and Information Technology (MCIT) (MCIT website, 2011), but the development of processes and activities that secure information in most Saudi Arabia organisations has been done either partially or totally by outsource companies.

2.8.2 Information system attacks in Saudi Arabia

A number of Saudi Arabian organisations’ information systems have suffered different kinds of attack. A recent attack was on May 25th 2013 when an Algerian hacker hacked nine Saudi government websites and posted an Algerian flag in the middle of all of the attacked websites. This attack occurred just after an attack on May 17th 2013, which was a distributed denial of service (DDoS) attack on the systems of several government websites, including the Ministry of Interior, causing the system to temporarily lose service. Although this kind of attack does not result in loss of information, it can cost the Ministry money and time, (Al Arabiya News, 2013).

In 2012, it took hackers only minutes to hack 16 official government organization sites in Saudi Arabia, including the National Campaign for Electric Consumption Guidance, which is part of the Ministry of Water and Electricity, the Technical and Vocational Training Corporation and the Human Rights Commission. The hacker, called “sejeal”, had sent a message, “Memorial of Gaza Martyrs”, to all of the 16 sites but no damage had been reported (Grimey, 2013).

According to Vijayan (2012), the Saudi Arabia Aramco Company, one of the largest energy companies in the world, was hacked by a group of people called the Arab Youth Group. On Wednesday Aug. 15th 2012, a Saudi Aramco official confirmed that the company had isolated all of its electronic systems from outside access due to the disruption of a virus that infected personal workstations but not the primary component of the network, (Vijayan, 2012).

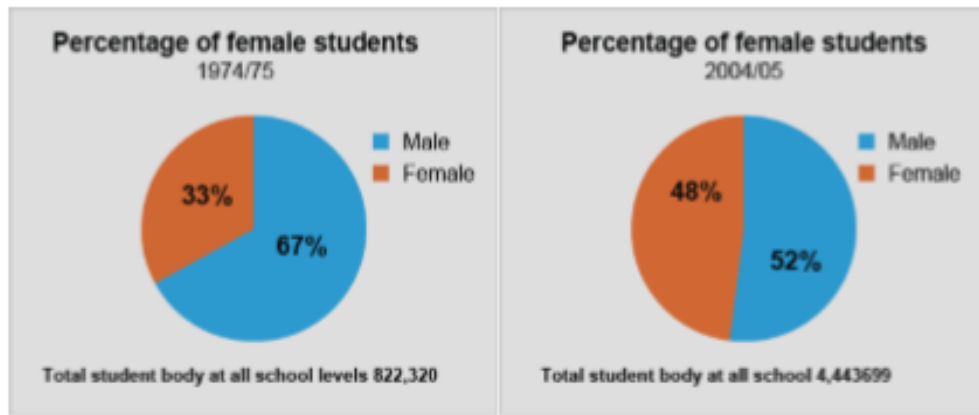
It can be concluded that, as the use of computer technology in Saudi Arabia increases and as more governments implement their own websites, the attack on their systems and websites will increase as well. Also, the level of information security awareness in most Saudi Arabia government departments is low compared to other countries such as the USA and the UK (Al-Gahtani, 2003).

2.8.3 Saudi Arabia cultural effect in information security

The Saudi Arabia government has achieved gender equality in education where males and females get equal access to basic education. The number of female students jumped from 33% compared to 67% male in the year 1974 to 48% female and 52% male by the year 2004 (Figure 2.7). Also, the Saudi Arabia government has encouraged young women to continue their education and enrol at all levels of higher education. Moreover, the labour and working law in Saudi Arabia treats man and woman equally in salary and employment (Almunajjed, 2009). However, there is an educational gender gap between males and females in Saudi Arabia because of the structure of the education system. Fields of specialization for wom-

en at university level is limited to education and teaching, human sciences, natural sciences, and Islamic studies (Figure 2.8).

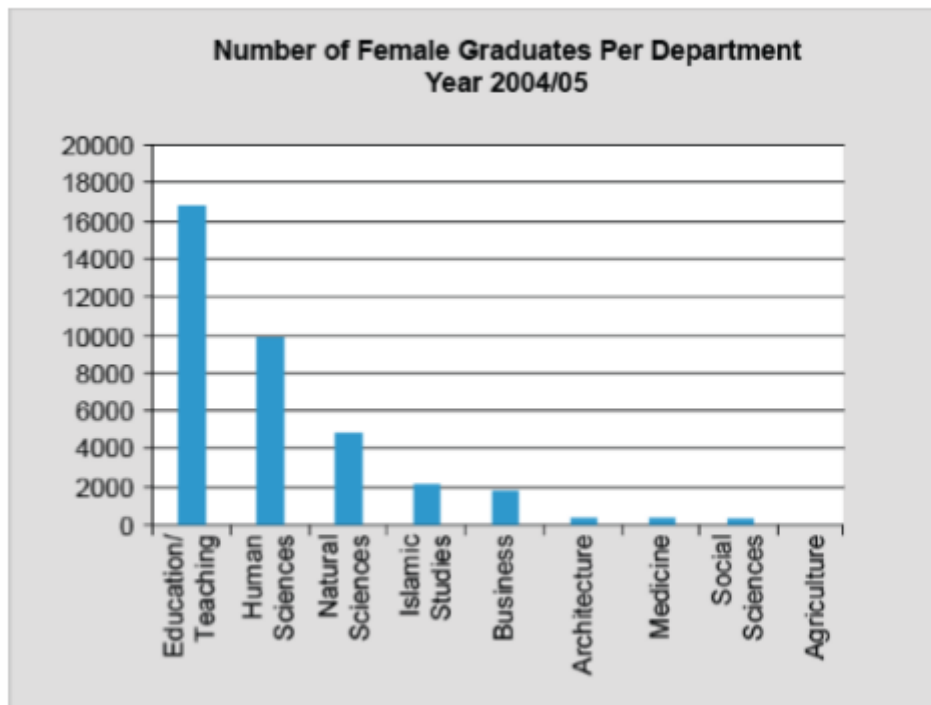
Percentage of Female Students at All School Levels (1974–75 and 2004–05)



Source: SAMA, 2008, Ministry of Education, p. 374

Figure 2.7: Percentage of Female Students at All School Levels (1974–75 and 2004–05)

Female Graduate Degrees by Department (2004–05)



Source: Al Hamed, M., Ziadeh, M., Al Oteibi, B., and Mutawalli, N., *Al Taa'im fi AlMamlaka al Arabiya AlSaudiya: Rouyat al Hader wa Istishraf al Mustakbal*, 4th ed., Al Rushd Library, Beirut, Lebanon, 1428/2007

Figure 2.8: Female Graduate Degrees by Department (2004–05)

As shown in Figure 2.8, almost all female university graduates have degrees in either education and teaching or human sciences and there are few female university graduates in the fields of science and technology. This is one of the major reasons women have unequal opportunity in the labour market (Almunajjed, 2009). Almost all female graduates take jobs as teachers in the labour market. This creates a gender labour market inequality.

Saudi Arabian basic law is Shari'a law which requires segregation of males and females in the work environment. The education system in Saudi Arabia enforces gender segregation, therefore, women's working roles are highly concentrated in teaching. Jobs that need a mixed work environment are rarely available for females, even fields such as medicine and agriculture are sometimes restricted. Therefore, most young women take jobs teaching in a girl's school (figure 2.8). Saudi women are not engaged in decision making in organisations' policies. Most major administration jobs in the Ministry of Education are held by men. Each province and district in Saudi Arabia has an all female Supervisory Bureau for Women's Education which reports to the general male manager of Educational Affairs. Most major decisions about women's education and work environment are made by males (Almunajjed, 2009). Communications between males and females are slow and not as frequent as they should be (Almunajjed, 2009).

2.9 Conclusion

The previous studies in the literature provide evidence that protecting information is not a simple task. Information cannot be secure unless serious actions, process, controls and policies are applied. The literature review identifies the meaning of information and information systems and the need to protect these systems through the use of technology, processes and policies that help safeguard the information and information systems. These techniques can be used to meet the aim of this research which is to identify policies and actions to protect information security systems for PNU and other Saudi Arabian universities and organisations. These information systems should be managed and supervised by an Information System Security Officer.

Some potential threats, risks and attacks that could threaten the security of information systems were identified in this chapter. The research considers these as potential threats to the information security systems of most universities in Saudi Arabia. Laws and regulation are legal measures that could regulate the action of Saudi Arabia citizens in relation to information security and the use of the law could, therefore, contribute to a successful implementation of a strong information security system.

Human compliance can be a potential barrier to a successful implementation of a university information security system and policy in Saudi Arabia. Approaches and techniques are presented in this chapter, such as the use of an annual personnel performance review to ensure and enforce employee compliance at PNU and other universities in Saudi Arabia.

Methods of implementing a successful information security system and policy are identified from the literature and presented in this chapter that could be used as a guideline to implement a university information systems security policy that minimises and overcomes threats and dangers in Saudi Arabia. However, the success of these methods and policy requires the endorsement and involvement of the senior management where it is implemented.

Much of the information collected about Saudi Arabian information systems is related to the effect of culture on the information systems security. The next chapter covers the impact of culture on Saudi Arabian information systems security.

Chapter 3: The Impact of Culture on Saudi Arabian Information Systems Security

Culture has an extensive influence on Saudi Arabian society and business environment. Saudi Arabia has a collective group oriented culture with close relationships between people. The Islamic religion is part of the Saudi Arabia culture and it plays major roles in Saudis lives. Saudi Arabian culture factors, including language barriers, hierarchy, gender communication, fear of losing face, nepotism and wealth, affect the performance of the organisations and their security. This chapter focuses on the impact of the environment and culture of Saudi Arabia on information security and makes some suggestions on how these problems may be overcome.

3.1 Introduction

The word culture derives from the Latin word “cultura”, which means that culture is part of people’s actions (Dadfar et al., 2003). Culture is a complex system of adopted social behaviour based on the way people live and work. Adeyemi-Bello and Kincaid (2012) define culture as “a system of values and norms that are collectively shared between groups of people”. Culture is combination of people’s thinking, saying, and making, their costumes, traditions, language, art, literature, common accepted attitudes, feelings and values. Culture is adopted, obtained, and carried from one generation to another (Rabe, 1992). According to Ferraro, culture is what people have, think, and do in their society (Ferraro, quoted in Dadfar, 1990). Culture covers traditions, customs and values, written and non-written rules (Simon & Yaras, 2000). Culture can be defined as an interlaced system of shared values and rules which form a foundation for the way of life of a particular group. Similar cultures would be those who share similar ideas, customs and values.

Every country or region has its own culture and therefore its own way of living. Saudi Arabian culture has been influenced by the religion of Islam, the role of history, and its tradition which makes it different from other cultures. Culture in Saudi Arabia has an impact on management styles, management decisions and management behaviour (Hill, 2009).

Understanding Saudi Arabian cultural differences, such as language, text direction, hierarchy, gender communication, fear of losing face, and nepotism, can have strong impacts on the success and security of an organisation. This is illustrated at a high level of abstraction by Figure 3.1.

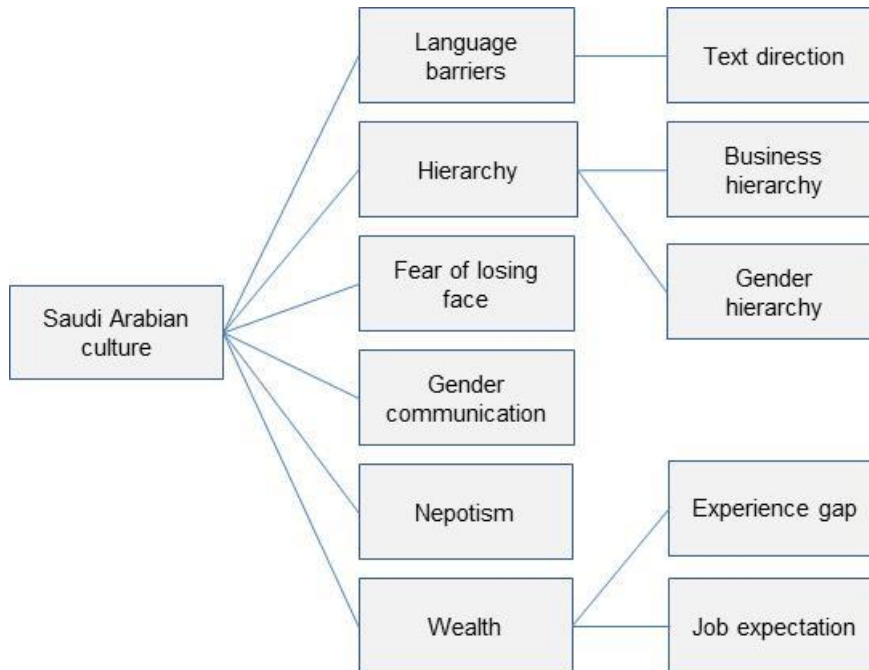


Figure 3.1: Cultural problems in a Saudi Arabian organisation

The following sections analyse the cultural aspects identified in Figure 3.1. This is based on research based on published literature and also on the experience of the author, who, as an employee of an all-female university in Saudi Arabia and a student at Loughborough University in the UK, has direct experience of the different culture in Saudi Arabia and the problems that arise from this.

3.2 Language Barriers

A barrier, as defined in the Oxford Dictionary (2013), is “a circumstance or obstacle that keep people or things apart or prevents communication or progress”. Language barriers can cause communication barriers when people speak different languages. The Arabic language can cause clear communication problems as it is not related to any other language and is very

different to Western European languages such as English, used by most technology suppliers. A language barrier between two cultures such as Arabic and English can be a cause of frustration and misinformation (Nikzad, 2013).

Frustration caused by a language barrier is a result of not being understood by someone else and this can create an unfriendly atmosphere between two communicating parties. Another risk that is when the language is not translated completely accurately, as this can give misinformation due to the word for word translations that come from dictionaries or online language programs. The problem is particularly bad for IT security as nearly all IT suppliers are English speaking and the IT code comments, documentation and help is therefore also in English. Even if documentation is supplied in Arabic, the differences in the language means the translation may not be totally accurate. According to Nikzad, 2013, when it comes to legal translation services, interpretations of manuals and instructions, or international conferences, a simple mistake or a well-meaning attempt at an equivalent in an Arabic/English dictionary could create an even bigger misunderstanding between the two communicating parties.

3.3 Text direction

Most Asian languages such as Arabic and Mongolian have different text direction than Latin languages. Mongolian languages spoken by many East Asian countries such as China and Japan used vertical directional script. The Arabic language is “bi-directional” (BiDi) as it uses right-to-left (RTL) script with Left-to-Right (LTR) elements, such as numbers. Hebrew, Farsi, Kurdish, Yiddish and Urdu are also considered BiDi languages. To reach the Arabic and Mongolian speaking market, software products, mostly written in the English language, must be translated into Arabic and Mongolian languages.

Arabic localization, the process of translating a product, content or application from one language to another, needs careful thought and resource planning when undertaken for the first time (ENLASO, 2011). Software application translation into Arabic is challenging because of the linguistic differences. Date, number, and currency are considered sensitive data and translating from Latin alphabet based languages to BiDi languages such as Arabic

language is challenging. The Arabic language uses Hindi digits. Numbers are laid out in Left to Right order (LTR) in all BiDi languages. Therefore the physical display of the text in Arabic will be a mixture of RTL order for characters and LTR order for numbers and dates, unlike Latin alphabet based languages where character and numbers are both displayed in a consistent, LTR order.

Educational Software translated into Arabic language commonly suffers flow of translation of all Arabic words. For example, most help sections in university software such as Microsoft Office and Banner collection are still in English. Also some university information system programs that are translated into Arabic face major problems because of the differences in the order of the texts. For example, in Arabic, a list of students' names starts with the first name, then the middle name and the last name. While in English it usually starts with the last name, then the first name and any middle name. Most of the university applications that are translated in Arabic present the Arabic list of students in English order which is very confusing.

3.4 Hierarchy

Saudi Arabia business culture is mostly a hierarchical culture. Saudi Arabian workers tend not to use their initiative to take action, but wait for their manager to direct them (Ali, 1986). Therefore, the organizational structure in Saudi Arabian companies is a strong hierarchical structure. In this structure, the manager's job is to make decisions which would be implemented down the chain of command by subordinates. Saudi organizational structure is a strict hierarchical approach in which subordinates are followers and managers are leaders. If superiors do not tell their subordinates what to do, jobs do not get accomplished. A manager who makes no specific job requests to be performed by subordinates would face a problem (Ali, 1986). Most Saudi superiors spend most of their time outside of their offices and request subordinates to perform their jobs either by phone conversation or via email.

It is of great importance for subordinates to show respect to managers and to not question their authority. Saudi managers are authoritarian leaders. They are expected to provide clear instructions about what needs to be done and how to do it. That is why there exists a wide

gap in power between employees and managers in Saudi Arabian firms. Managers who have the most authority should provide complete and specific directives to others. This can be problematic for the organization because it stifles creative thinking and dictates that employees wait to be told what to do rather than making decisions on their own. This impacts the challenges managers face when trying to improve productive behaviours.

The PNU information organisation structure, for example, consists of general Director on top of the hierarchy structure leading counsellors (expert IT consultants), and 11 administration departments, as shown in figure 3.2.

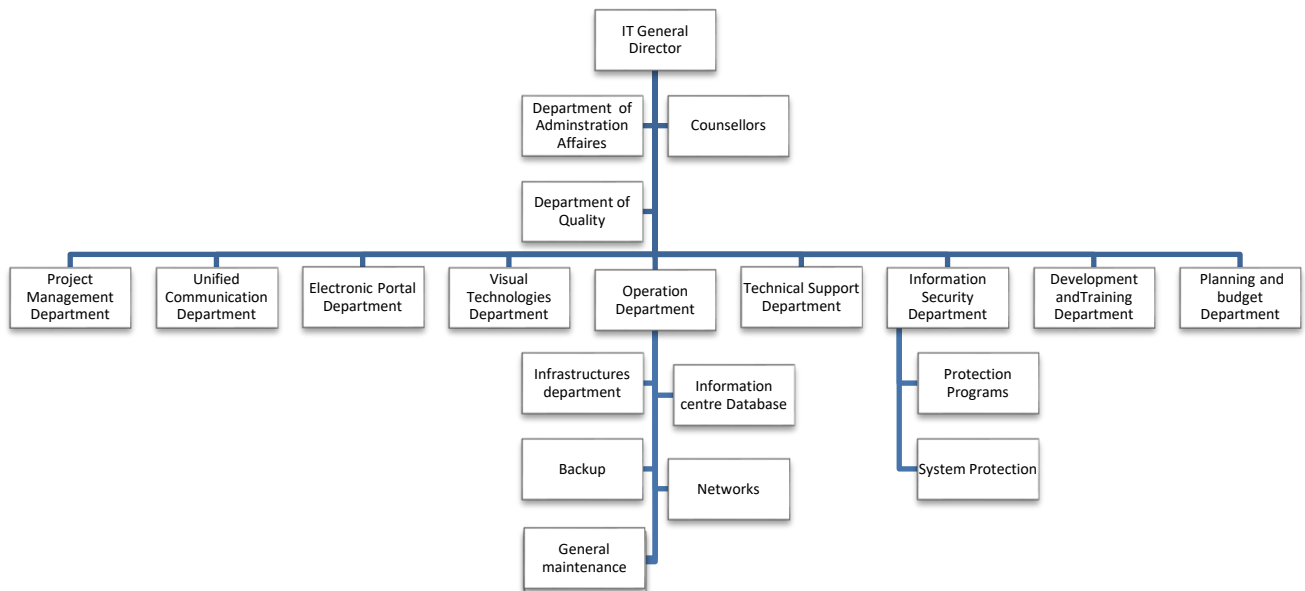


Figure 3.2: PNU Information technology structure (PNU website 2013)

In addition to the business hierarchy, there is also a gender hierarchy. The male gender dominates the female gender in Saudi Arabian culture. Men typically do not listen to women and they expect women to do as they say. A Saudi man would be very reluctant to have a female as their manager and would consider it to be embarrassing. This means that talented female staff can be severely inhibited from getting any promotion except within an all-

female environment. The knowledge and experience of many intelligent females in Saudi Arabia is not used to the best effect.

3.5 Gender communication

In addition to the gender hierarchy issue, according to the interpretation of the Islamic religion in Saudi Arabia, gender segregation in society and organisations is essential. This means that males and females who are not related should not have direct contact with each other. Women in Saudi Arabia can work in male/female organisations but they must not interact with men. Most women work in all female settings where they do not have to interact with men. Women tend to work in girls' schools, women's sections of universities and banks catering for female clients, social work and development programmes for women, medicine and nursing for women, television and radio programming, and computer and library work (Sabbagh, 1996).

Although PNU is an all-female university, some of the high level operational management is handled by men. As a result of the non-communication culture, even senior women employees usually struggle to communicate with men. Most of the communication is done either online, via email or voice communication via phones and mobiles. Because of Saudi culture, direct communication is forbidden, not by the PNU management, but by the female's spouses. Poor communication between women employees and male employees who control the information systems at PNU could jeopardize the security of the information held.

3.6 Fear of losing face

'Losing face' means not maintaining the dignity and the respect of others. In Saudi Arabia culture avoiding confrontation and conflict is preferable and dignity and respect are qualities that are key factors affecting behaviour. Dignity and respect are maintained in Saudi Arabia by saving face which is done by the use of compromise, patience and self-control (Communicaid Group, 2013). Arabian culture utilises the concept of face to solve conflicts and to avoid embarrassing or discomforting others.

In a Saudi Arabian business context, avoiding loss of face is important. In fact, saving face is more important than imposing pressure to meet deadlines or improve productivity. It is important for management to show recognition and appreciation of subordinates for their contributions. It is disrespectful for managers to fail to express their appreciation on a continual basis to subordinates. Unfortunately, the fear of losing face means that Saudis have:

1. An inability to accept criticism.
2. An inability to admit that anything can be wrong

These inability means that any security problems tend to be ignored and 'brushed under the carpet' as to admit to any vulnerability would amount to accepting a criticism and losing face.

3.7 Nepotism

Nepotism is the favouritism of a relative or a friend by those with power in business. Arab people highly value and respect friendship and family relationships. In a business setting, favours based on mutual benefit and trust are ways of enhancing these cultural values. Family and personal relationships take precedence over other governing factors. According to Atiyyah (1993), family and personal connections are more influential than other governing factors in the Saudi Arabian business environment. That is why Saudis like to develop a strong social network which can provide help for their families if it is needed. Business in Saudi Arabia is based upon personal connection, so establishing a social network is essential to be successful. Saudi employers like to hire those who they know and trust; therefore it is encouraged and accepted for managers to hire and promote family members or friends (Fischer, A.H. and Manstead, 2000) and managerial decisions are often affected by the desires of the family (Atiyyah, 1993).

According to Atiyyah (1993), as family and personal relationships are important and common in Saudi Arabian businesses, favouritism of a subordinate who has developed a strong relationship with their managers is common and accepted. It is also common for

subordinates to replace their current manager because of their strong relationships with higher management.

Atiyah (1991) believes that this type of business practice has both negative and positive aspects. It can serve as a catalyst for building strong relationships with employees up and down the chain of command. However, this could lead to unproductive employees' problems (Ali and Schaupp, 1992). It could also weaken the value of performance. In this type of environment, the employees may consider that getting a better position is not necessarily a result of working harder but by having a good relationship with organizational leaders. This can lead to resentment amongst other employees and reduce the efficiency of the organization performance (Atiyah, 1991). This could also lead to the hiring of unqualified people in sensitive positions, such as in the information security monitoring department, which then puts the security of information at risk.

3.8 Wealth

The oil wealth of the state of Saudi Arabia is well known. This has had two significant effects on IT systems and on the security of these systems.

Saudi Arabia is a newly developed country with an economy which has expanded rapidly with its oil revenues. This expansion has been reflected in the rapid expansion in IT with companies and organisations starting to use interconnected computer networks and most of the organisations in Saudi Arabia are putting the country's new found oil wealth into investment in IT systems to digitalise their information. However, this rapid expansion has meant that there are very few people in Saudi Arabia with sufficient experience and expertise in IT systems and security. People are generally unaware of the problems of IT security, let alone any solutions to the problems. This is made worse by the fact that, generally, the Saudi people have a very trusting nature and an inability to believe that anyone would want to do any harm to them and their systems.

The Saudi Arabian people are rightly proud of their very successful, expanding economy, and they expect to be part of the business it generates. However, this leads to an expectation

that they will always have a senior position within any organisation. Most Saudis prefer managerial positions because of the status and position. For example, jobs involving manual labour would not be accepted by most Saudis and as they consider these to be embarrassing positions (Curry and Kadash, 2002). Unfortunately, this attitude prevails regardless of whether they are suitably qualified and so, with the shortage of experience and expertise in the country and with jobs being granted through nepotism, many of the senior managers in Saudi Arabia are unqualified and inexperienced. Furthermore, because of the fear of losing face, there is an inability to address this problem or even admit to it. Clearly, this will have a negative effect on IT management and security.

3.9 Conclusions

Saudi Arabia has seen a rapid expansion of information systems. However, the culture in Saudi Arabia has the effect of making the security of this information very vulnerable which, in turn, can have an effect on the success of Saudi organizations. This chapter has shown that Saudi Arabia culture adds an additional layer of complexity to the security of any information system. A number of problems specific to Saudi Arabian culture have been identified.

Information systems security should be a concern of every company and organisation. However, this chapter has highlighted additional problems created by the culture in Saudi Arabia. It is believed that any organisation working in Saudi Arabia should note the potential risks to IT security reported in this chapter and should address the problems with care and sensitivity to take the culture into account. This chapter has made some suggestions on ways forward for investigation to resolve the problems identified. Other problems in Saudi Arabian information system security will be difficult to solve. However, IT itself is already helping to overcome some problems, such as the use of email to enable male-female communication. The next chapter covers the methodology used to collect and analyse data for this research. It also covers some research types, philosophies and methodologies and then the researcher choice of the research type, philosophy and methodology.

Chapter 4: Methodology

This chapter presents the research approach, philosophy and methodology adopted for this study that helps achieve the research objectives outlined in chapter 1. It starts by describing some research types, philosophies and methodologies and then the researcher choice of the research type, philosophy and methodology.

4.1 Research Methodology

Research is a consistent effort of gathering, analysing, and interpreting information to find an answer to a question, a solution to a problem, or establish facts (Oxford dictionary 2014; Neuman, 2006). Research methodology is a systematic way to find an answer for questions, solve a problem, find a solution or gain knowledge. Rajasekar, et al. (2013) defines research methodology as “The procedures by which researchers go about their work of describing and predicting phenomena.” According to Kagioglou et al., (1998), research methods are divided into three themes, research philosophy, research approach and research techniques. See figure 4.1.

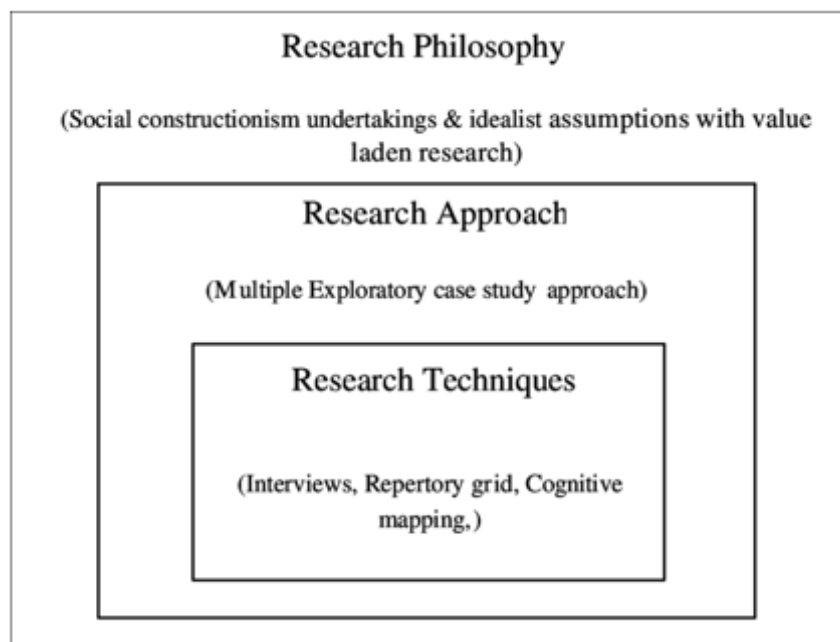


Figure 4.1 Nested Approach (Kagioglou et al, 1998)

4.2 Research Philosophy

Research philosophy is defined as a development of new knowledge and nature of knowledge (Collins, 2010; Saunders, et al., 2007). Research philosophy has an influence in the researcher's selection of methodologies in a research project. It has an impact on the researcher's choice of data collection and analysis methods (Crossan, 2003). The two main information system research philosophies are positivistic and phenomenological (interpretivist) (Orlikowski and Baroudi, 1991). Research can have a positivistic philosophy and/or a phenomenological philosophy.

4.2.1 Positivistic

Collis and Hussey (2003) define positivistic philosophy as "approaches that are founded on a belief that the study of human behaviour should be conducted in the same way as studies conducted in the natural science." Bandaranayake (2012) defines positivistic as a "reality" to find the reality of things. Natural science research, such as chemistry, geology and physics, usually uses this kind of philosophy. Methods used for positivistic philosophy are experimental studies, longitudinal studies and cross-sectional studies. Positivistic philosophy is an approach that uses consistent techniques such as hypothesis, measurement and evaluation to look for the facts or proof of any social phenomena (Neville, 2007).

4.2.2 Interpretivist/Phenomenological

Also known as interpretivist, phenomenological philosophy is to know the true meaning of social world experience (Katadae, 2000). Phenomenological philosophy can be referred as "social constructionism: *constructing knowledge about reality, not constructing reality itself*" (Shadish, 1995), especially in management research. Titchen and Hobson (2005) define phenomenological philosophy as "the study of lived human phenomena within the everyday social contexts in which the phenomena occur from the perspective of those who

experience them” This type of philosophy is based on observation, understanding and investigation and then analysis and construction of a social cases (Badewi, 2013). This philosophy can help the researcher point out the research issues by using and evaluating in detail small samples (Kasi, 2009). Easterby-Smith et al., (2006) argue that in phenomenological philosophy, the researchers focus on their beliefs and values to reach an acceptable solution for the research problem. Methods used for this philosophy are (Katadae, 2000):

- Case studies
- Action research
- Ethnography (participant observation)
- Participative enquiry
- Feminist participative
- Grounded theory

Table 4.1 presents a comparison between the two philosophies in terms of their beliefs, what should the researcher do when choosing one of these philosophies and the methods used.

Table 4.1: Positivism Vs Phenomenology Research Philosophy

	Positivist paradigm	Phenomenological paradigm
Basic beliefs	<ul style="list-style-type: none"> - The world is external and objective - The observer is independent - Science is value-free 	<ul style="list-style-type: none"> - The world is socially constructed and subjective - The observer is a party to what is being observed - Science is driven by human interests
The researcher should	<ul style="list-style-type: none"> - Focus on facts - Locate causality between variables - Formulate and test hypotheses (deductive approach) 	<ul style="list-style-type: none"> - Focus on meaning - Try to understand what is happening - Construct theories and models from the data (inductive approach)
Methods include	<ul style="list-style-type: none"> - Operationalizing concepts so that they can be measured - Using large samples from which to generalise to the population - Quantitative methods 	<ul style="list-style-type: none"> - Using multiple methods to establish different views of a phenomena - Using small samples researched in depth or over time - Qualitative methods

(Source: Easterby-Smith *et al.*, 1991)

Research can be a positivistic, phenomenological or both, with overlaps between the two (Neville, 2007). However, Knox (2004) argues that it is acceptable to use only one philosophy and multiple methodologies in research.

4.2.3 Choice of Philosophy

This research is based on the observation of people's understanding of information security in relation to their culture and experience. Therefore, it is more suited to an interpretivist philosophy.

This project is analytical research in which the researcher analyses existing information security and makes a critical evaluation of it by asking 'why' and 'how' an event is happening. The research approaches that are fit for this research are empirical and non-empirical. The techniques used for this study are:

- A case study is used in this research for the purpose of understanding the information security system. This is descriptive research in which the researcher relies on observation and examination of collecting data related to the information security system.
- The researcher studied in depth the PNU information security system. The methods used to collect data were surveys, interviews, participation and investigation.
- An action research approach is used for ethnography (participant observation), in which the researcher was a participant in the auditing process to observe the information security weaknesses and also to observe the effect of employees' experiences and university culture on the security of the information systems.

4.3 Research approach

The research approach describes the style in which the research is conducted. The researchers can use more than one approach, depending on the type of the research. The type of the research and some of the research approaches such as quantitative vs qualitative, subjective vs objective and deductive vs inductive are explained in the next subsections.

4.3.1 Type of Research

There are different types of research. Neville (2007) differentiates the research into four types:

- **Exploratory research** is when there are no or few previous studies present. It is the development of hypotheses. The techniques employed in this type of a research would be observation and reviews of previous studies and case studies (Neville, 2007).
- **Descriptive research** is the description of the event or elements as it exists at present. The researcher cannot control the changes and can only document what has happened or what is happening. The methods used are quantitative including comparative and correlation methods (Neville, 2007).
- **Analytical research** is the analysing of existing facts and information and make critical evaluation of them by asking why and how this event is happening (Shmueli, 2009).
- **Predictive research** is the prediction of a new event that is most likely to occur, based on new observations and analysing available facts (Shmueli, 2009).

This research is analytical research in which the researcher analyses an existing information security system to identify the issues and their causes and effects in a critical evaluation.

4.3.2 Quantitative and Qualitative

The quantitative approach uses a different methodology to the qualitative approach. The quantitative approach is based on measurement and analysis of relationships between variables. Berg (2001) defined the qualitative approach as “the meanings, concepts, definitions, characteristics, metaphors, symbols and descriptions of things.” Table 4.2 shows the relationships between quantitative and qualitative approaches.

Table 4.2: Quantitative and qualitative approaches adopted from Neville (2007)

Quantitative	Qualitative
<p>The emphasis of Quantitative research is on collecting and analysing numerical data; it concentrates on measuring the scale, range, frequency etc. of phenomena.</p> <p>This type of research, although harder to design initially, is usually highly detailed and structured and results can be easily collated and presented statistically.</p>	<p>Qualitative research is more subjective in nature than Quantitative research and involves examining and reflecting on the less tangible aspects of a research subject, e.g. values, attitudes, perceptions.</p> <p>Although this type of research can be easier to start, it can be often difficult to interpret and present the findings; the findings can also be challenged more easily.</p>

4.3.3 Subjective and Objective

The subjective approach is based on individual opinion, interpretations and points of view. Subjective research is when a researcher has control of the research outcome and is involved in the subject matter. The objective approach is opposite to the subjective approach as it is based on measurable facts and precise analysis and the researcher tends to remain independent of the subject matter. Remenyi et al. (1998: 33), stated that objective researchers are “Independent of, and neither affect nor is affected by the subject of the research”. Easterby-Smith et al. (1991) expressed subjective and objective approaches as interpretivism and positivism. See Table 4.3.

Table 4.3: Key Research Implications of the Subjective and Objective Perspectives

Positivist Perspective		Subjectivist Perspective	
Independence	The observer is independent of what is being observed.	The observer interacts with subject being observed.	Interaction
Value-freedom	The choice of what to study, and how to study it, can be determined by objective criteria rather than by human beliefs and interests.	Inherent biasness in the choice of what to study, and how to study it as researchers are driven by their own interests, beliefs, skills, and values.	Value-laden
Causality	The aim of social science should be to identify causal explanations and fundamental laws that explain regularities in human social behaviour.	The aim of social science is to try to understand what is happening.	No Cause and Effect
Hypothetico-deductive	Science proceeds through a process of hypothesising fundamental laws and then deducing what kinds of observations will demonstrate the truth or falsity of these hypotheses.	Develop ideas through induction from evidence; mutual simultaneous shaping of factors.	No Hypothetico-deductive reasoning
Operationalisation	Concepts need to be operationalised in a way which enables facts to be measured quantitatively; static design – categories isolated before study.	Qualitative methods – small samples investigated in depth or over time; emerging design – categories identified during research process	Operationalisation
Reductionism	Problems as a whole are better understood if they are reduced into the simplest possible elements.	Problems as a whole are better understood if the totality of the situation is looked at.	No Reductionism
Generalisation	In order to be able to generalise about regularities in human and social behaviour it is necessary to select samples of sufficient size; aim of generalisations is to lead to prediction, explanation and understanding.	Everything is contextual; patterns identified – theories then developed for understanding.	Generalisation
Research Language	Formal, based on set definitions; impersonal voice; use of accepted quantitative words.	Informal, evolving decisions; personal voice; use of accepted qualitative words.	Research Language

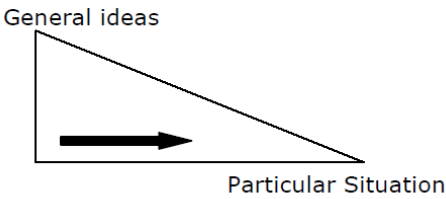
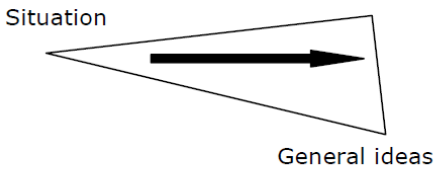
Compiled from: Easterby-Smith et al. (1991), Hussey and Hussey 1997), Creswell (1994), Remenyi et al. (1998)

4.3.4 Deductive and Inductive

The deductive approach is a top-down process that starts with an existing theory or generalisation then tests if it can be used in specific situations (Hyde, 2000).

The inductive approach is a bottom-up process that starts building a theory based on observation of a particular instance (Hyde, 2000). Table 4.4 is Neville's (2007) differentiation of the two approaches.

Table 4.4: Deductive and inductive approaches adopted from Neville (2007)

Deductive	Inductive
 <p data-bbox="416 1317 863 1424">Deductive research moves from general ideas/theories to specific particular & situations: the particular is deduced from the general, e.g. broad theories.</p>	 <p data-bbox="901 1317 1348 1397">Inductive research moves from particular situations to make or infer broad general ideas/theories.</p>

4.3.5 Choice of Approach

This research uses both quantitative and qualitative approaches to analyse the collected data from the conducted surveys and interviews questionnaires. Creswell (2003), explained that research can use both quantitative and qualitative approaches. It could start with quantitative approaches to test and analyse an idea or situation which could be followed by a qualitative approach to support the research with a more detailed explanation from some individuals.

This research is a combination of both a deductive research and inductive approaches. It is deductive, moving from the general idea that the security of information systems needs improvement to the more specific implementation of a framework for information security policy. Also, it moves from the particular situation at one university to make a generic theory or idea about the state of a whole country.

Furthermore, the researcher played a major part in the implementation of the fieldwork and had a control on the outcome in raising the level of information security awareness level. Therefore, a subjective approach is used to reach the research aim.

4.4 Research Strategy

The research strategy provides the overall actions, methods and steps that direct the researcher thought and effort. The researcher could use multiple methods to help obtain the research conclusion (Creswell, 2003). There are various types of research strategies:

- **Experimental** is finding a relationship between a set of variables by manipulating the independent variable on the dependent variable to maintain a control over the rest of the variables (Keppel,1991).
- **Survey** is a deductive method of collecting data by either the distribution of questionnaires or interviews of a sample of a population and the recording of their responses (Neuman, 2006). Neuman stated that the collected data from the interview is more accurate than the data collected from questionnaires.
- **Grounded theory** is an inductive method with an aim to generate or develop a theory from a collected data. Glaser and Strauss (1967) define grounded theory as “the discovery of theory from data systematically obtained from social research.”
- **Action research** involves solving a problem by engaging the studied population to work together as a team to improve their way of handling issues. According to the

Blumberg et al. (2005), people involved in action research play a major part in monitoring and testing, and they collaborate to identify issues and develop solution.

- **Case study** is an in-depth investigation of a social behavioural of a small geographical area in order to explore and understand complex problems, (Zainal, 2007). Yin (1984) defines a case study as “an empirical inquiry that investigates a contemporary phenomenon within its real-life context; when the boundaries between phenomenon and context are not clearly evident; and in which multiple sources of evidence are used.” Yin (1994) states that there are three types of case studies, exploratory (what), descriptive (how) and explanatory (why).

4.4.1 Choice of strategy

Choosing the appropriate research strategy approach depends on the type of research questions, the focus is on the contemporary against historical phenomena and the investigator control over the actual behaviour event (Jait, 2011). According to Saunders et al. (2007), the research strategy provides the required plan for answering the research questions and achieving the research objectives.

According to Yin (1994), a case study is an investigation of a phenomenon in reality context. The case study is the most common research strategy in the information system field (Scott and Ives, 1982). Information systems case studies can be classified, according to the adopted epistemological and ontological assumptions, as positivist, critical or interpretive (Yin, 1993).

The appropriate research strategy approach to achieve the research objectives outlined in chapter 1 is mainly a case study of the people culture that affects the information security awareness when using an information system (See Table 4.5).

Table 4.5: Research strategies used for each research objective

Objectives	Strategies used
Objective 1: to carry out a literature review on previous work in the research area.	The literature review
Objective 2: By means of interviews, surveys and experiments, determine the current state of IT security Saudi Arabian knowledge-intensive organisations.	Survey strategies which include questionnaires and face to face and voice interviews
Objective 3: Analyse the findings from Objective 2 to formulate a practical and effective policy and action plan for any Saudi Arabian knowledge-intensive organisations to improve their IT security, with particular emphasis on overcoming the awareness, cultural specific and legal barriers to IT security at Saudi Arabian knowledge-intensive organisations.	Quantitative methods using the tools, Excel and SPSS, were applied to analyse the initial survey finding to identify the users overall ideas of the organisation, the information system security and factors behind the lack of information security system awareness and poor communication between the users and the IS department.
Objective 4: By conducting interviews and/or surveys at other organisations, determine how common are the dangers and barriers to information system security in other service organisations in Saudi Arabia and how much of the plan for PNU would be applicable to other organisations in Saudi Arabia.	Grounded theory was applied to analyse the collected data to identify factors that affect the information security awareness level and the main causes of them and the need to develop an information security framework. The finding showed that the most common factor was caused by the field culture. A survey was conducted at the case study university and a second university and the collected data was compared.
Objective 4: By analysing the results from Objective 5, produce a generic framework of recommendations for policy and action to improve information system security in Saudi Arabian organisations.	Action research was used to develop and evaluate the culturally aware information security framework, although there was a lack of support from the people involved to bring the framework into action
Objective 6: Test the framework.	A quantitative approach was used to test the developed culturally aware information security framework by mean of survey questionnaires.

4.5 Data Collection Methods for the Research

Any research requires two types of methods to collect data either counting things and/ or interviewing people as in quantitative and qualitative methods (MacDonald *et al.*, 2011), see Table 4.6.

Table 4.6: Research methods: Quantitative and Qualitative

	Quantitative	Qualitative
Aim	The aim is to count things in an attempt to explain what is observed.	The aim is a complete, detailed description of what is observed.
Purpose	Generalisability, prediction, causal explanations	Contextualisation, interpretation, understanding perspectives
Tools	Researcher uses tools, such as surveys, to collect numerical data.	Researcher is the data gathering instrument.
Data collection	Structured	Unstructured
Output	Data is in the form of numbers and statistics.	Data is in the form of words, pictures or objects.
Sample	Usually a large number of cases representing the population of interest. Randomly selected respondents	Usually a small number of non-representative cases. Respondents selected on their experience.
Objective/ Subjective	Objective – seeks precise measurement & analysis	Subjective - individuals' interpretation of events is important
Researcher role	Researcher tends to remain objectively separated from the subject matter.	Researcher tends to become subjectively immersed in the subject matter.
Analysis	Statistical	Interpretive

(Source: MacDonald *et al.*, 2011)

Table 4.6 summarises the key features of the two different ways to collect data used in the quantitative and qualitative methods including the tools and types used to collect data, the type of output data, the sampling size, each method approach, the research role and the type of analysis used for each method.

In order to achieve the objectives and aim of the research, the research design and methods should be planned with care (Bouma *et al.*, 1996). According to Yin (1994), the research design is “the logical sequence” that act as a connection between the data collected and the research conclusion.

This research starts with quantitative methods applied through questionnaires and qualitative methods applied through interviews. The research is used to achieve research objectives. The next subsections are an explanation of each method used in this research. The research stages are described in Figure 4.2.

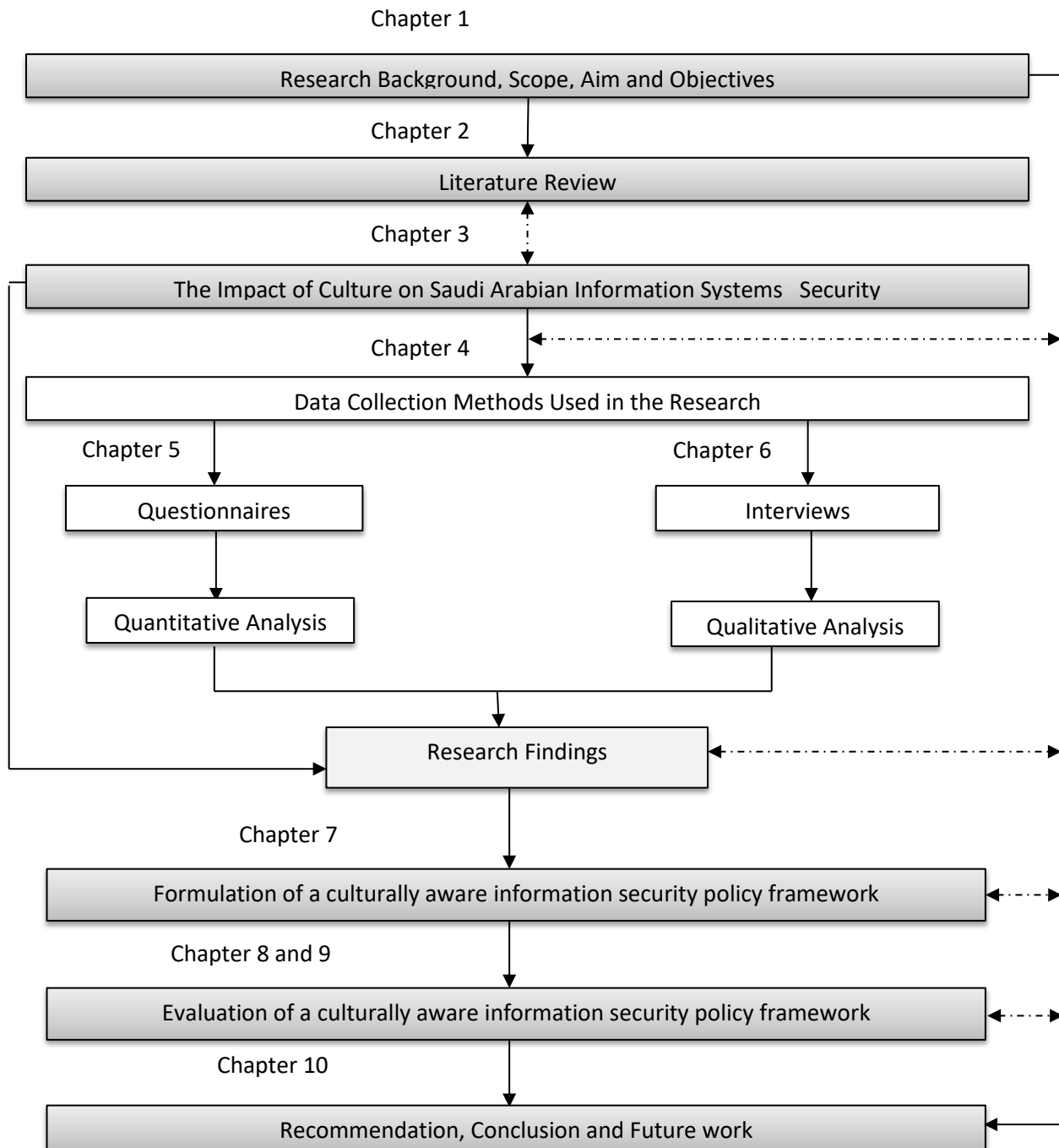


Figure 4.2: Research Stages

4.5.1 Literature Review

The literature review process was undertaken to review all published work in the area of specific interest of the researcher (Mohamed, 2006). This research process concentrated on previous literature studies that have been conducted in the following areas: information security, implementation of information security, management of information security, information security policy, human compliance to information security policy and information security in Saudi Arabia (see Chapter 2).

The finding of the literature review helps to define and refine the researcher's aims and research objectives described in chapter 1. The literature review process continuously assists the research and contributes in all the research phases (Figure 4.2). The literature review findings from previous information collected about Saudi Arabian information system led to identifying issues related to the effect of culture in information systems security.

The need to implement a culturally aware information security policy framework was identified in the findings of the literature review. This framework could be used as a guideline to implement a university information system and policy that raise the level of information security awareness among users and minimise and overcome threats and dangers at Saudi Arabia.

4.5.2 Survey

The most common method of data collection is a questionnaire, which can provide researchers with quantitative data (Dornyei, 2001 cited in Alshumaim and Alhuassan, 2010). This research employed a survey questionnaire strategy on two occasions. The initial questionnaires were developed to identify the information system users overall idea about the security of the system and the second set of questionnaires was developed to measure the level of users information security awareness before and after the implementation of the developed security awareness framework.

4.5.2.1 Initial Questionnaires

For the initial questionnaires, statistical techniques were used to explore correlations between factors. Moreover, the technique of hypothesis was used to help determine whether a potential relationship is real or just by chance where:

The null hypothesis H₀ = There is no relationship between two questionnaire responses.

The alternative hypothesis H₁ = There is a relationship between two questionnaire responses.

Pearson's coefficient is the most common measure of correlation (Price 2000). The two-tailed test is used to measure the significance levels of Pearson's correlation, to confirm the existence of a real relationship. According to Price (2000):

*“A very important part of statistics is describing the relationship between two (or more) variables. One of the most fundamental concepts in research is the concept of **correlation**. If two variables are correlated, this means that you can use information about one variable to predict the values of the other variable.”*

Correlation (r) is single number that shows the strength of the relationship between two variables (X, Y). The formula for the correlation (r) is:

$$r = \frac{N\sum XY - (\sum X)(\sum Y)}{\sqrt{[N\sum X^2 - (\sum X)^2][N\sum Y^2 - (\sum Y)^2]}}$$

Where: N is the sample size

$\sum XY$ is the sum of the product of the two variables

$\sum X$ sum of variable X

$\sum Y$ sum of variable Y

$\sum X^2$ sum of squared variable X

This correlation value will always be between -1.0 and +1.0. If it is close to 1.0 or -1.0, then this means that there is a strong relationship between the two variables (X, Y). However, if

the correlation number is far from 1.0 or -1.0, then the relationship between the two variables(X,Y) is not highly correlated, but there is still a relationship between variables(X,Y). If the correlation number is equal to zero, then there is no relationship between the two variables. Moreover, if the correlation number is positive, then it means that as one variable (X) increases so does the other one (Y), or as variable(X) decreases then variable(Y) decreases as well. On the other hand, if the correlation number is negative, then this means that as one variable (X) increases the other variable (Y) decreases, or as variable(X) decreases then variable(Y) increases. SPSS was used in this study to calculate the correlation between two variables.

4.5.2.2 Second Questionnaires

The questionnaires used on the second occasion used a method to analyse the data adopted from Bond (2012). A survey was distributed to all types of users and the responses were used as an indicator of the level of the overall participants' information security awareness levels. For each question, multiple choice responses in the survey were given a number from (1-5) according to the question's answer in a Likert Scale approach (Bond, 2013). The collected results indicate the overall classification of the risk level of the surveyed university. The question responses in this survey (except for the first question) were each assigned a risk value (1-5). The highest risk (5) indicates weak awareness, negligent behaviour, or high risk activities, and the lowest risk (1) indicates strong awareness and good security practices (Bond, 2013). The collected survey can be used to determine the overall risk score or risk level of the organization as follows:

- a. For each question, the risk value was multiplied for each question by the number of times it was chosen by the survey participant.
- b. The average of the response totals for all survey response totals was calculated by dividing the survey cumulative response total by the number of survey participants to calculate the participants overall risk level.

This research used two different software applications to analyse the data collected from the two developed surveys. SPSS was used to analyse the data collected from the initial survey and Microsoft Excel was used in second survey to analyse the collected data.

4.5.2.3 The interviews

In this study three types of interview techniques were used to collect data: structured, unstructured, and semi-structured interviews. According to Mohamed (2006), in a structured interview, the interviewer has prepared a questionnaire in which they ask the questions and record the answers without getting any further detail. Whereas semi-structured interviews can gain more detailed information by turning the interview into a conversation which can lead the interviewers to add more questions to clarify the interviewee's point of view (Lindlof and Tylor, 2002). An unstructured interview is when the interviewer introduces the scope of the interview, asks as many questions as needed and records the replies (Lindlof and Tylor, 2002). Three types of interview have been used in this study, telephone interviews, face-to-face interviews and group interviews. Table 4.7 differentiates between face-to-face and telephone interviews.

Table 4.7: Face-to-face vs Telephone

	Pros	Cons
Face to Face	People can be very generous with their time and expertise	Appropriateness of setting
	Interpersonal dynamics and establishing trust may yield insights	Balance responsibility to your interviewees and needs of investigation
Telephone	In-depth examination of topic possible	Can be time intensive
	Can do more without travel-time, from your desk	Less opportunity to establish rapport

(Source: MacDonald *et al.*, 2011)

This research interview questionnaire consists of three parts that covers three areas, the vulnerability of PNU information security, employee and user awareness and training programmes. Telephone interviews were conducted with the male managers. Face-to-face interviews were conducted with all the females who had agreed to be interviewed, and a group interview was conducted with students. Because of the poor level of English of most the interviewees, the interview questionnaire was presented in the Arabic language so everyone could understand it.

4.6 Summary

This chapter covered the philosophy, the approach, the strategy and the methodology adopted in this research. Several techniques and methods have been used to reach the objectives of the research. Data was collected using survey and interview questionnaire methods.

Chapter 5 covers a full description and analysis of the survey questionnaire which was conducted to identify the case study organisation's employees' overall idea of information system security. Chapter 6 covers a full description and analysis of the interviews held to identify the vulnerability of system, employee's awareness and the training program effectiveness.

Chapter 5.0 Data Collection-Survey

This chapter describes the data collection-survey methodology and presents the data collection findings. The following sections relate to the data collection analysis, with separate sections for the two questionnaires distributed, one for the Information Technology (IT) staff and one for the non-IT staff and the faculty members and students who are the end users of the IT system questionnaires. Finally, there is a section listing the problems highlighted by the findings of the two surveys.

5.1 Questionnaires' aim

The aim of these surveys is to get an overall idea of what the employees at a knowledge intensive organisation in a newly developed country, Saudi Arabia, think of the information systems they are using, focusing on their security. This study was conducted to see if the dangers and barriers to information security presented in the literature review exists in Saudi Arabian organisations and to identify new threats and barriers not covered in the literature review.

5.2 Data collection-Survey process

The process of the survey starts with the distribution of the questionnaires, the result of the distribution and the questionnaires design is explained in the next subsections.

5.2.1 Distribution of Questionnaires

The survey questionnaires were conducted at Princess Nora bint Abdul Rahman University (PNU). An Arabic version of each questionnaire was submitted to the PNU Department of Scientific Research for approval before distribution at PNU. After the questionnaires were approved, they were submitted to the Heads of Departments and Deans of the colleges of the PNU. The PNU Department of Scientific Research distributed the questionnaires to all employees at PNU. Also included with the questionnaires was a formal letter, which stated the importance of participating in these surveys and specified to whom they should be distributed. The questionnaires were collected from the same department, the Department

of Scientific Research, after two weeks. This type of distribution method may lead to bias in the results as the respondents' answers may be affected once they know that the management would collect them. However, no other methods could be used to distribute these questionnaires because of the limited time and lack of any other electronic means.

5.2.2 Questionnaire distribution results

450 copies of the questionnaires were distributed and 154 were collected. The overall response rate was therefore 34%. Of those, 300 copies of a non-IT staff questionnaire were distributed with 109 collected, giving a response rate of 36%. In addition, 150 copies of IT staff questionnaires were also distributed and 45 participated in this survey giving a response rate of 30%.

5.2.3 Questionnaire Design

Two types of questionnaire were distributed, one for Information Technology (IT) staff and one for non-IT staff, faculty members and students who are the end users of the IT system. The purpose of having two types of questionnaire is to avoid confusing the majority of the participants with technical questions and get accurate responses from participants. The non-IT staff questionnaire consisted of 16 questions, most of which were yes/no and multiple-choice questions, with a few open-ended questions. The second questionnaire was for those who know more about the structure of the system, the IT employees. This questionnaire consisted of 20 questions, which were mostly yes/no and multiple-choice questions, and some more IT security related open-ended questions. The participants were male and female staff, faculty members, and students. See Appendix A.

5.3 Data collection analysis process

This study uses quantitative approach for the two surveys, one questionnaire for non-IT staff, faculty members and students and one questionnaire for IT specialists. This section presents the analysis of the questionnaires on the non-IT staff and Section 5.4 presents the analysis of the questionnaire for IT staff.

300 copies of the non-IT staff questionnaire were distributed and 109 participated in this survey. The non-IT staff questionnaire consisted of 16 questions, with the results given in the following subsections.

5.3.1 Q1: Gender (male/female)

The gender balance at PNU is predominantly female, with, at the time of writing, 5368 female staff and only 496 male staff. As seen in Figure (5.1), few males took part in the survey. The male staff represent around 10% of the population of PNU employees and work mostly as either faculty members or in the IT management department. Based on Islamic tradition, the male employees are located in buildings far from the female departments. Having only a manual distribution method, via their managers, made it difficult to distribute the survey to males (the distribution of the questionnaires from managers to staff was not controlled by the researcher). Although female participation is very important, male employees may know more of the technical structure of the IT system at PNU, on the basis that more men work in this field than women. Moreover, technical jobs have traditionally been male oriented in Saudi Arabia. According to Almunajjed (2009), a global consulting firm, women in Saudi Arabia are typically restricted to working only in the field of education, either teaching or in administrative positions. Factors like social, legal, educational and occupational culture keep Saudi women from fully participating in the labour market.

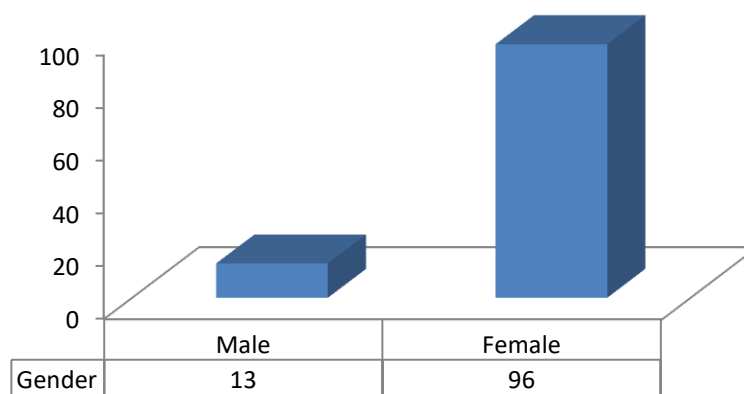


Figure 5.1 Gender

5.3.2 Q2: Age Group

The majority of the respondents were aged between the ages of 21 and 40. The older generation, 50 and over, did not participate to the same extent. This group may know less and may be unaware of the usability and security of the IT system at PNU (see Figure 5.2). The reason for only a few of the older generation, 5 participants, responding could be that:

- They did not understand the questionnaire due to the lack of knowledge in the field of information systems.
- They were not interested in doing it.

According to Alshumaim and Alhuassan (2010), computers were introduced to all secondary schools in 2001, when the Ministry of Education in Saudi Arabia recognized a need to eliminate computer illiteracy. Therefore, it is possible that the older group, aged 50+, may not have been formally educated in computer use. This could be a relevant factor in the response rate from this demographic. Effectively, either the respondents are embarrassed to admit their problems or they do not make use of computers on a regular basis. It is also possible that the terminology used in the questionnaire may inadvertently have been at too technical a level for those without any formal education in this area. According to a survey of graduate students, the limiting factor in the use of electronic technology is the limited proficiency of English language among females compared to males (Al-saleh, 2004). Also, the younger generation, who represent the majority of the end users, are mostly students (numbering approximately 40000 according to the Information and Statistics Department at PNU), and therefore should be able to contribute more to the questionnaire since they utilise the systems more frequently, mainly the Banner system which is the computer information system that has information about courses, students, faculty and staff.

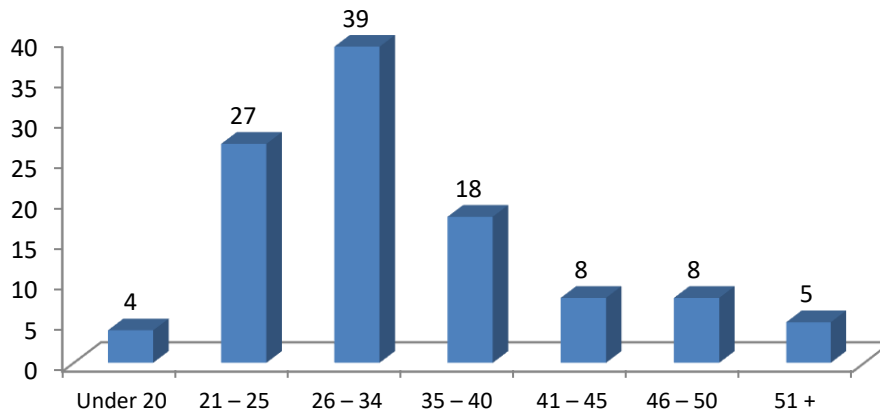


Figure 5.2 Age group

5.3.3 Q3: What is your highest qualification?

This question covers the qualification level of the participants. The reason for asking this question was to ascertain the education level of the respondents. Based on the age group analysis, the older group are more likely to hold a PhD or a master degree and were seen to participate less than those of the younger generation (38 out of 112) in this survey. Moreover, relatively few participants (20 out of 112) of the younger generation represented those with only high school qualifications, who were mainly students at PNU. Most of the group (51 out of 112) that completed the questionnaires had bachelor degrees as their highest qualification (Figure 5.3).

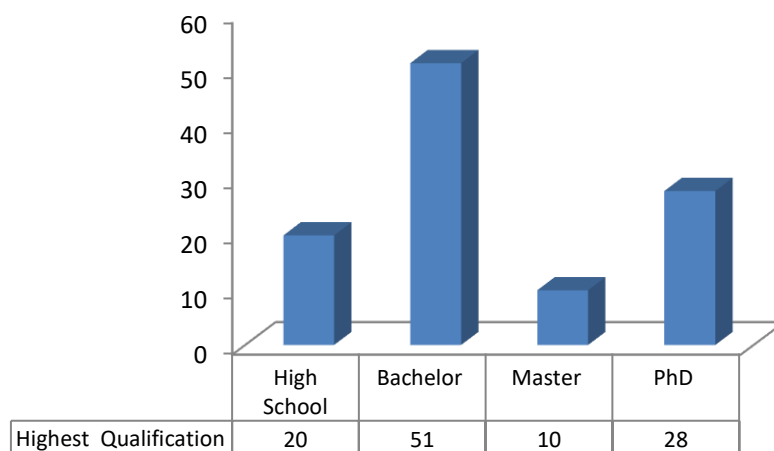


Figure 5.3 Qualification

There is a positive correlation (0.669) between age and qualification. As age increases, the qualification level also increases (Table 5.1).

Table 5.1: Correlations between age group and qualification (as presented by SPSS)

		Age	Qualification
Age	Pearson Correlation	1	.669**
	Sig. (2-tailed)		.000
	N	109	109
Qualification	Pearson Correlation	.669**	1
	Sig. (2-tailed)	.000	
	N	109	109

** . Correlation is significant at the 0.01 level (2-tailed).

The correlation ($r=0.669$) is significant at the ($p<0.01$) level (2-tailed). The Sig. (2-tailed) is equal to (.000) which does not actually mean zero. SSPS, the statistical package used for this analysis, rounds the number to the nearest 3 decimal places only.

5.3.4 Q4: Do you have any IT related qualification at undergraduate / postgraduate level?

The aim of this question was to find out if any of the non-IT employees who use the IT systems have any kind of IT related qualification. Almost all the group that completed the questionnaire for non-IT staff (94 out 112 participants) have no IT-related qualification from their undergraduate or postgraduate study. Only 15 participants have an IT related qualification.

5.3.5 Q5: Have you attended any IT related training courses?

This question focuses on the amount of training given to the user to prove that the more training taken the easier the IT system will be. Even though non-IT employees who are the end users of the IT system need extensive IT training because they have no IT related education, most of them (55 out of 112 respondents) reported that they had never

attended any training course. 27 respondents had only taken one training course (Figure 5.4).

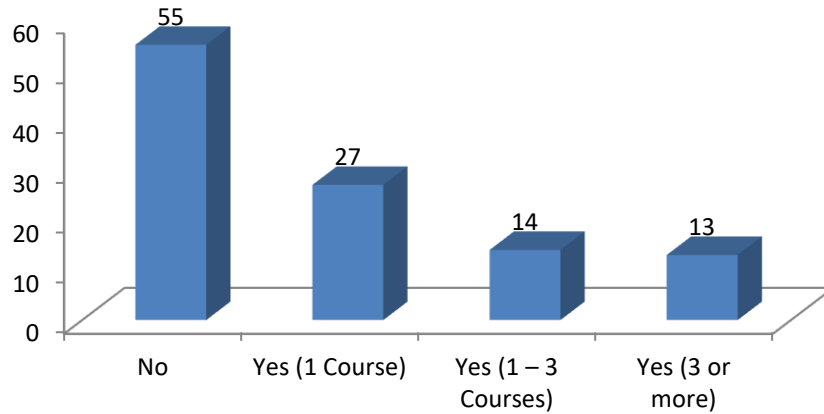


Figure 5.4 Training courses

5.3.6 Q6: Position held at PNU:

Most of the respondents have either held a management position or an academic/lecturer position (43 and 47 out of 112). A small number of students had also participated. The limited involvement of the students is likely to have been a result of the distribution method through the Heads of Departments and Deans of the colleges who tended to focus on staff only. Also, the small number of IT supporting staff involved (3 out of 112) is because most were given the other questionnaire for IT-related staff (Figure 5.5).

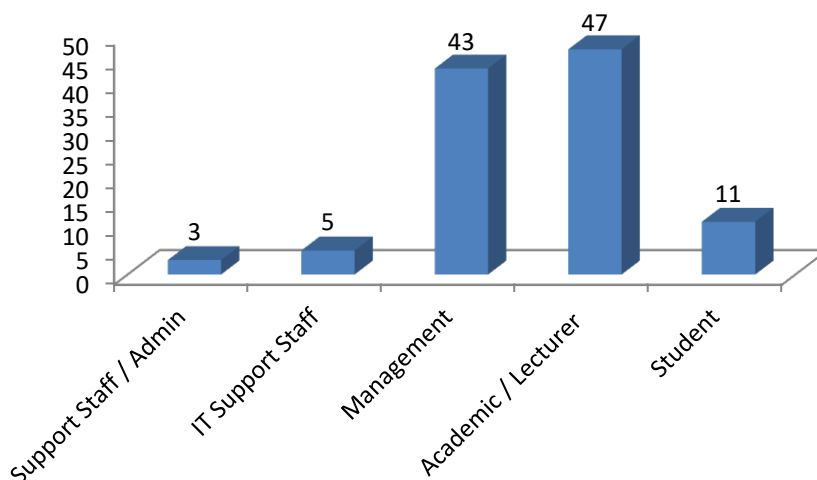


Figure 5.5: Position held at PNU

5.3.7 Q7: Which of the University's computer systems do you use?

The majority of the group do not know which system they are using. The rest use the Banner system, which is a computer information system that has information about courses, students, faculty, and staff (Figure 5.6).

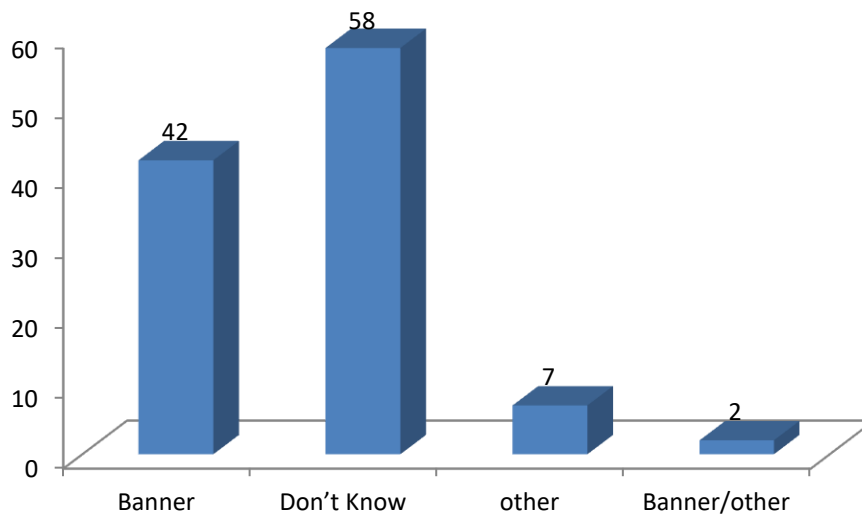


Figure 5.6: Computer systems used at PNU

It is possible that most of the participant (figure5.6) who chose 'don't know' are using the Banner system but don't know the name of the information system they are using because it is the system used by all academic and most management members. According to an interview with Kholud Aljadawi, an IT worker who works for the IT outsource company called Wipro, there is another information system which is used for hardware maintenance, software support and updating the system. This system is used mainly by specialist IT staff as it does not support the Arabic language. The future plan is to translate it in to Arabic and it will then be made available to everyone in the PNU organisation. Employees will be able to submit their technical problems (hardware/software) to IT staff through this new software instead of telephoning.

5.3.8 Q8: Do you often face problems when using the University's computer systems?

52% of the respondents have not faced any problem when using the system. These are mostly from the same group who have had no training courses and no IT related education, which could mean that they use the system less. It could be that they may think the issues they encounter are just a result of their lack of training rather than a system failure. 44% of the respondents reported that they did face problems when using the IT computer system (Figure 5.7).

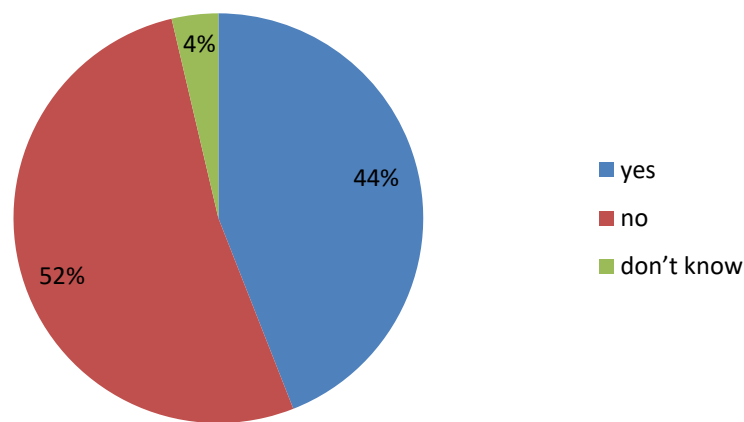


Figure 5.7: Computer system problem faced

Out of 52% of the respondents that believed they face no problem with the computer system, it is a possibility that the respondents would not recognise a problem due to their lack of knowledge of how the system normally performs.

5.3.9 Q9: When dealing with IT related tasks, do you consider yourself someone more likely to have to help others, or to ask for help yourself?

Although they may know little about the system, have no IT related education and have had little training, 45 out of 112 respondents report that they help others with their IT. Helping each other and working as a team could enhance the quality of the work environment, however, this kind of unprofessional help may cause more problems for the security of the IT system. Herold (2010) stated that an employee with no knowledge or understanding of how to ensure security and confidentiality of information would risk the most valuable

business assets and information being mishandled or misused. 30 out of 112 respondents had asked others for help and 22 both ask for help when they need help with their IT and also provide IT help for others (Figure 5.8).

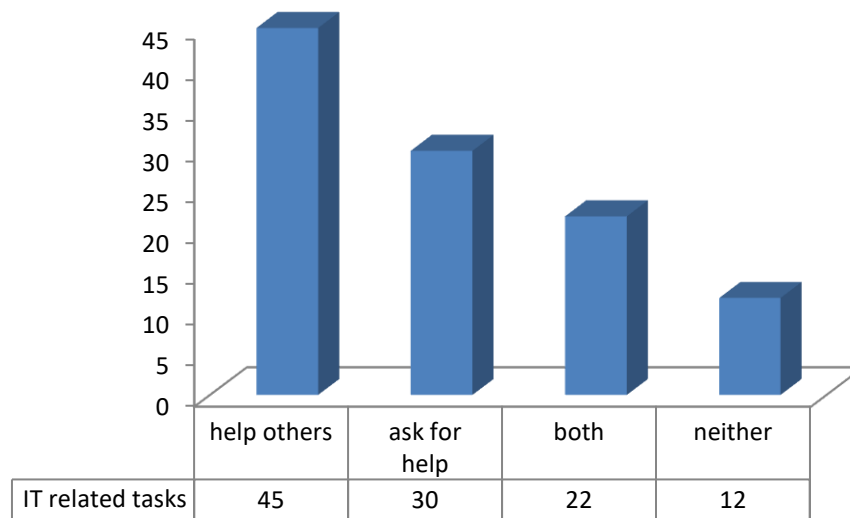


Figure 5.8: IT related tasks

According to Figure 5.8, the majority of employees help each other so this could be one of the reasons that they don't seek help from the people with more IT knowledge, such as IT-technicians. This could also be due to communication issues.

5.3.10 Q10: Please list and rate (1-5) any problems that you have faced in the past month:

The respondents were asked to rate any problems they had faced in the month the questionnaires were submitted and most of them reported significant problems. According to the respondents, the most significant problem faced was having no network coverage. They also complained about the network and about the Internet being slow. Some of them experienced difficulties accessing their account and email. Other respondents complained about their password being changed without their knowledge. Kholud Aljadawi explained that for security reasons, they sometimes change employees' passwords and they would

inform employees by sending emails containing the new passwords. Some participants have experienced problems related to versions of application software not being updated. Some respondents reported problems with the usability of the system (Banner), as they were unable to see all the names in the students list. Some respondents could not use the computer whenever they needed it because they didn't have access to a computer. Students can use University computers only if they have computer related classes. Other respondents complained about not having good antivirus programs available on their University computers.

5.3.11 Q 11: On a scale of 1 – 5 how computer literate do you see yourself?

(1 illiterate /5 very literate)

This question was asked in order to know how computer literate the respondents believed they are. The majority of respondents believed they are computer literate and gave themselves high scores for computer knowledge; their score falls between 3 (semi-literate) and 5 (literate) out of 5 (very literate) (Figure 5.9).

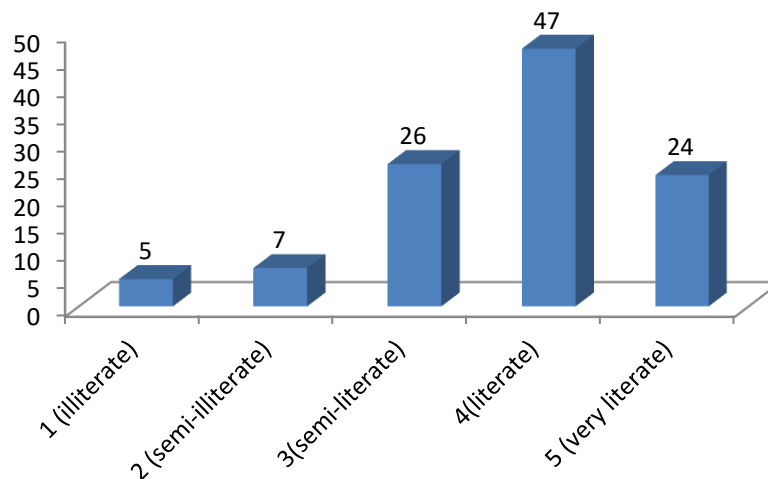


Figure 5.9: Computer Literacy

Table 5.2: The Relationship Between academic qualification, number of training courses attended and the participants view of their own computer literacy

Qualification	Number of training courses attended	Computer literacy
High school /IT related education	1	1
High school /no IT related education	1	0-3
	2	0-3
	3	0
Bachelor/ IT related education	1	1
	2	1-3
	3	1
Bachelor/no IT related education	1	0-3
	2	0-3
	3	1-3
	4	2
Master/ IT related education	4	2
Master / no IT related education	1	1-3
	2	3
	3	2
	4	2
PhD/ IT related education	1	1
	2	2
	3	1
	4	1-3
PhD/ no IT related education	1	1-3
	2	1
	3	1-3
	4	0-3

As shown in table 5.2 the number of training programmes attended has little effect in raising the level of computer literacy among all types of employee with different level of qualifications. This shows that the training programmes given to the employees need to be modified to raise their computer qualification skills.

5.3.12 Q12: Do you feel the IT systems at PNU are difficult to use?

This question is about the difficulty in using IT systems at PNU. The respondents appear to have mixed feelings about the system difficulty. They think that the system is neither easy nor difficult (See Figure 5.10).

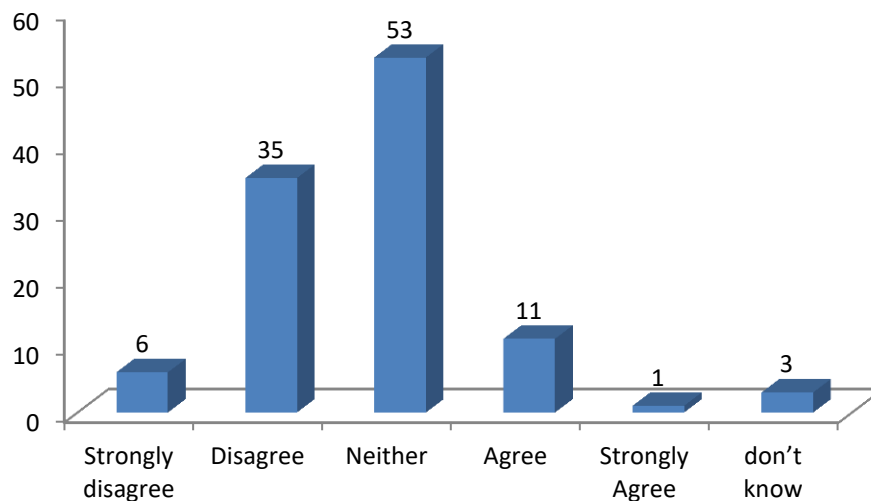


Figure 5.10: IT systems difficulty of use at PNU

35 out of the 112 respondents thought that the IT system is easy to use. It likely included many of the 14 out of 112 respondents who reported having attended more than one training course. Frost (2013) showed that training could improve employees with the weakest skills, which also develops employees' confidence. If this is true, then this means that training courses have positive effects on the respondents and the employees in general. Employees of any organisation should find their own organisation's system easy to use.

5.3.13 Q13: How many passwords do you use to access the various IT systems at PNU?

The majority of the respondents (42 out of 112) revealed that they use only one password. According to Hunt (2011), it is very risky for Internet users, who usually have more than 22 protected accounts, to use one password and the same login details. Moreover, Hunt (2011) thinks that it is nearly impossible to have 10 or more Internet accounts with unique strong passwords that can be remembered. In addition, Burkeman (2012) believed that having a number of passwords could lead to confusion. Furthermore, it takes a penetrator only a few minutes to find a short password, 3-6 characters in length, or words in dictionaries (Pfleeger and Pfleeger, 2007). Some were not sure how many passwords they have been using. Some of the respondents may have included all their Internet accounts' passwords - for this they picked five passwords, see Figure (5.11).

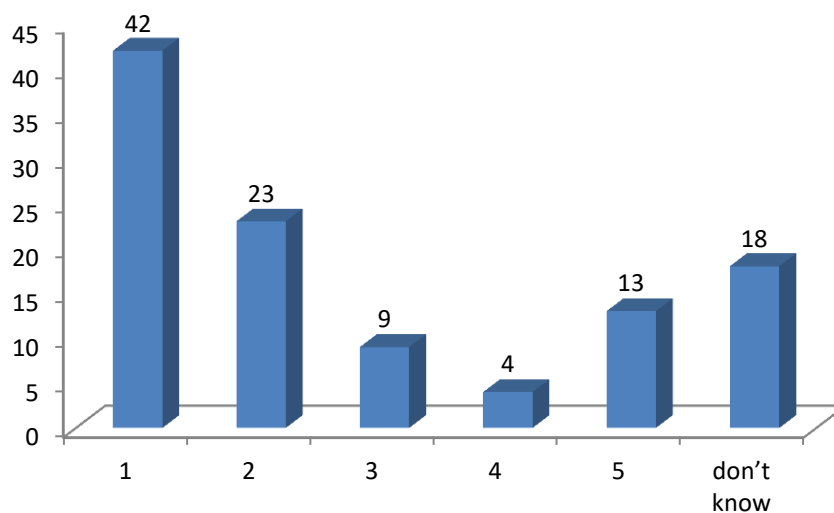


Figure 5.11: Number of passwords used

Figure 5.11 shows that most employees have only one password. The end user using their organisation's computer work station generally has two types of passwords one local password for each work computer that is authenticated on each work station (Locke et al., 2009). The other password is an individual unique password for use of university application systems such as the email system and the Banner system.

5.3.14 Q14: Which parts of the current IT systems do you find the most difficulty with?

When the group were asked about the aspects of the current IT systems they find the most difficult, most of the respondents thought that the Banner system was very difficult to use. Furthermore, the respondents reported that the Banner system was very difficult to access and it seems that nothing has been done to improve the application since its introduction. The respondents also complained about communication between themselves, as system users, and the IT staff. The users complained about not getting any response back and the IT staff complained about the user not understanding the system. Therefore, most of the respondents wanted more training programmes to help them understand the Banner system. One of the recommendations was training employees to ensure that they understand the importance of securing information they access (Pfleeger and Pfleeger, 2007). Some of the respondents complained about the lack of training programs for using new hardware devices. According to Frost (2013), training is important to increase employee knowledge and satisfaction, and to improve employee performance. Finally, some of the respondents wanted to know the location of the information storage as they wanted to make sure it is safe.

5.3.15 Q15: If you would like to add any additional information in relation to using the IT facilities at PNU please write it below:

The respondents indicated they would like to add additional information in relation to using the IT facilities at PNU, as follows:

- Two of the respondents asked for more training programmes.
- One of the respondents asked for more tasks to be done electronically.
- Two of the respondents asked for frequent updates to the programs
- At least one respondent asked for an upgrade of the computer's hard disk.
- At least one respondent asked for maintenance to be done by females.
- Two of the respondents asked for an update of the information system Banner.
- At least one respondent asked for better communication with people in charge since they mostly get IT help from their colleagues (See Q9).

- At least one respondent requested a special, help-desk department just for answering any questions. They suggested this would be a solution for the communication issue with IT-staff, who they said rarely come when needed (See Q9).

The above data collected revealed issues related to segregation and communication, for example, the respondent's request for maintenance to be undertaken by female shows lack of communication between the female users and male IT staff. Moreover, there is an issue to communication in general even between female employees, such as the poor communication with female help desk operatives.

5.3.16 Non-IT staff survey analysis conclusion

Based on their responses, it can be concluded that the respondents were using a new and, for them, an unfamiliar IT system, Banner. Although almost all of them have no IT related education, most of them have had training courses on this particular IT system, making it easier to use. The respondents asked for training courses to familiarise themselves with any new system they may use. There does also seem to be a substantial problem with network coverage. The network is either slow or there is no network coverage at all in places. There is also a lack of communication between end users and the IT staff, which emphasises the need to make the IT systems easier to use, especially the Banner system, by updating or replacing it. It also highlights the need for in more training courses.

5.4 IT-employee survey analysis

This questionnaire for IT staff consisted of 20 questions, which were mostly yes/no and multiple-choice questions, and some more IT security related open-ended questions. 150 copies of the questionnaires were distributed and 45 participated with a respond rate of 30%.

5.4.1 Q1: Gender

Although PNU is a female university with few male staff, males play a major role in this organisation, especially in the IT management department. Therefore, it would have been better if males had participated in this survey and it is disappointing that only females did so.

5.4.2 Q2: Age group

The majority of the respondents, 80%, were between the ages of 21 and 34. There was no participation of those older than 50 or under 20. 20% of the respondents are between the ages of 35-50 (Figure 5.12). The poor response from younger (under 20) and older (51+) employees, who form about 15% of the PNU population, may be because they know less or are not interested in IT security.

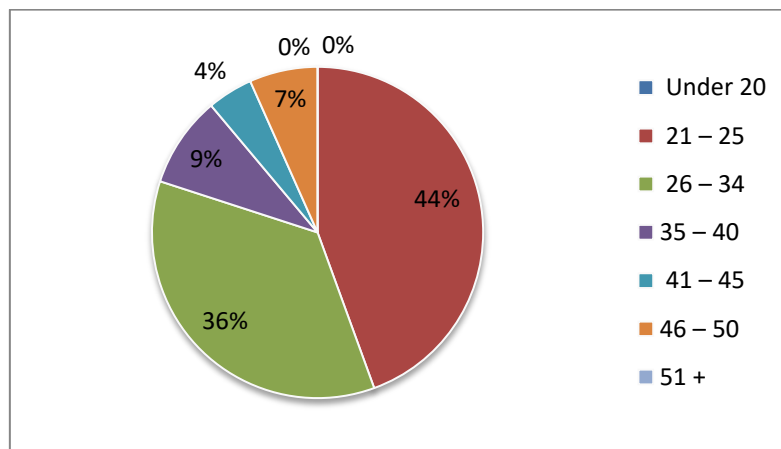


Figure 5.12: Age group

5.4.3 Q3: What is your highest qualification?

Of the respondents that completed the IT staff questionnaire about the qualification level, 76% have a bachelor degree as their highest qualification. Only 4% have a PhD degree and 20% have a high school degree qualification (Figure 5.13). None had a Master's degree as their highest qualification.

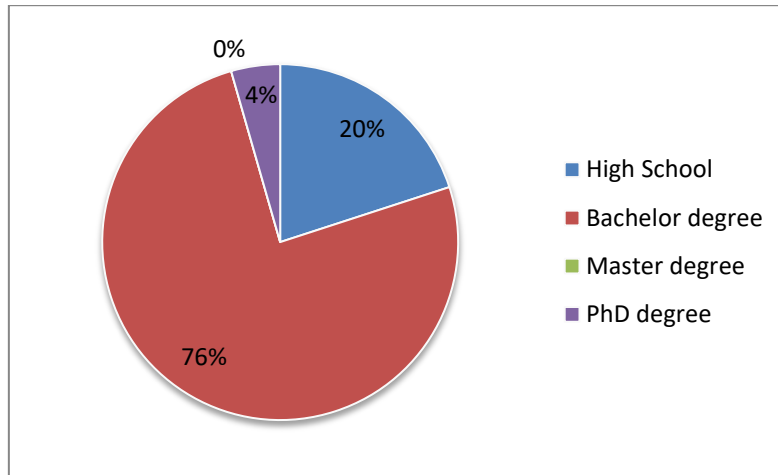


Figure 5.13: Qualification

5.4.4 Q4: Is your education IT related?

Since this questionnaire was designed specifically for IT employees, the majority of the respondents, 62%, held an IT related qualification at undergraduate or postgraduate level. However, a significant percentage (38%) of the respondents did not have an IT related degree. This suggests that PNU may have relatively under-qualified employees doing IT related tasks and this could negatively affect the security of the IT system there. As Herold (2010) stated, an unprofessional IT employee could mishandle or misuse and put at risk the most valuable organization asset of information (Figure 5.14).

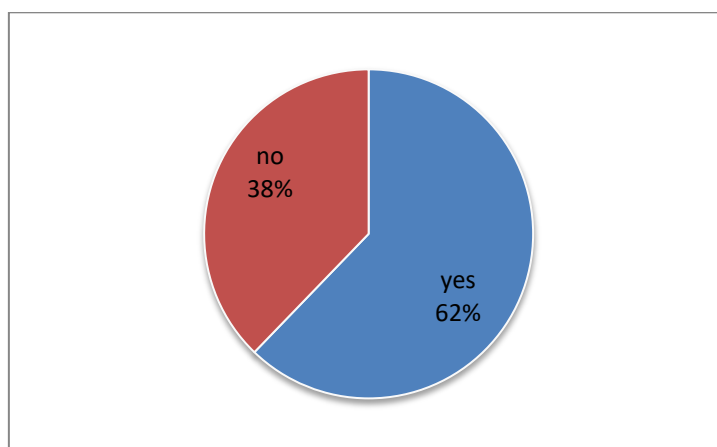


Figure 5.14: IT related education

5.4.5 Q5: Have you attended any IT related training courses?

Although most of the respondents have IT related qualifications, they would normally need to have more than one training course before using any new IT system. 33% of the respondents reported that they had not had any IT related training and asked for more training courses. 21 % of the respondents had only had one training course, which may not be enough (Figure 5.15). Since PNU is a newly developed university, most of its application software and hardware has been newly developed as well. Employees should have effective training programmes in order to achieve organisation goals and mission. Herold (2010) expressed that employees accessing or influencing the accessing of organisation assets, such as information, should receive more training and refresh their training every year or more often, depending on the nature of the organisation.

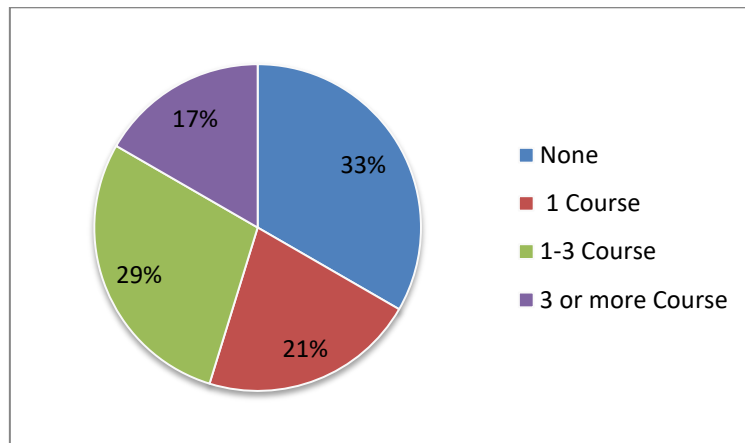


Figure 5.15: IT related training courses

5.4.6 Q6: Position held at PNU:

Eight of the 45 respondents held IT management positions at PNU. 16 of the 45 respondents are IT support staff, most of whom perform computer maintenance. 11 held other positions and seven held more than one job within the University. The lack of students' involvement in the questionnaire is likely to be a result of the distribution method through the Heads of Departments and Deans of the colleges who tended to focus on staff only (Figure 5.16).

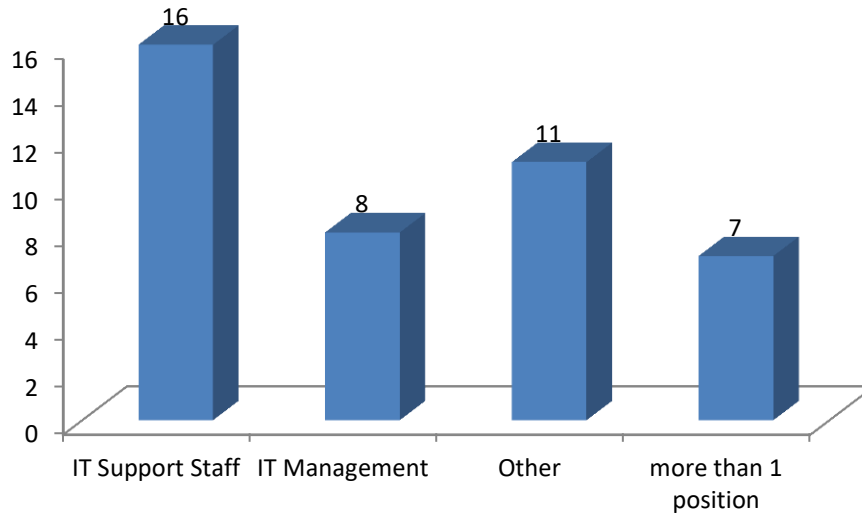


Figure 5.16: Position held at PNU

5.4.7 Q7: Which of the tasks below do you perform whilst at the University? Tick where appropriate:

Figure 5.17 shows the tasks performed at the University. Five of the respondents perform data entry. Three of the respondents do IT management and eleven of the respondents perform computer maintenance. Four responses came from the data manager or system developer/programmer. Those employees should be the targets for this research, since they are the ones who use the system the most and know more about the problems of the IT system security. The majority of the respondents undertake tasks other than the ones listed in the questionnaire.

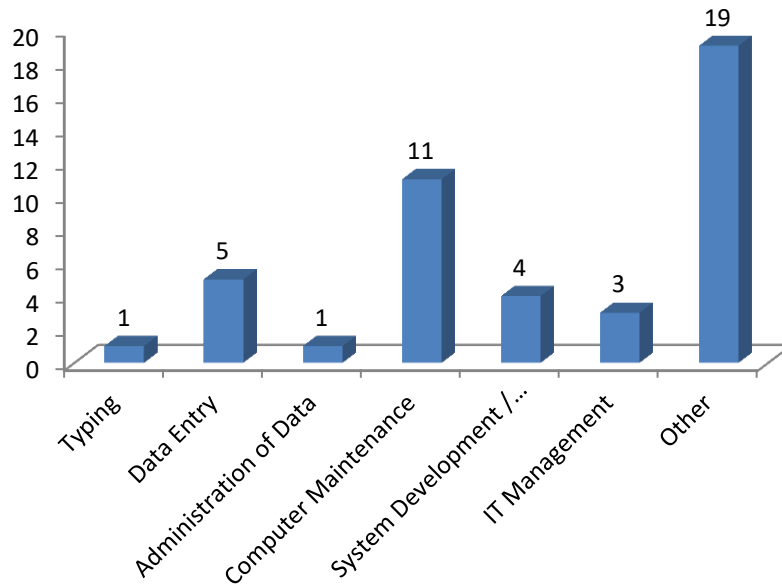


Figure 5.17: Tasks performed

5.4.8 Q8: Which of the University's computer systems do you use?

The Banner system is the IT system that most non-IT employees and IT employees use. 13 out of 45 of the IT respondents reported that they worked with the Banner system; some use Microsoft Office programs. It is surprising to note that the majority of the IT employees did not know what system they are using or did not give any answer. It could be assumed that if they took any training courses for a given system they should, at least, know the name of that system (Figure 5.18).

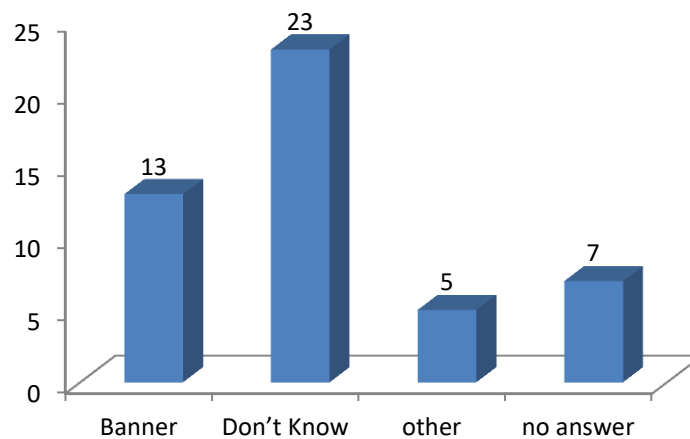


Figure 5.18: Computer system used at PNU

5.4.9 Q9: Do you often face problems when using the University's computer systems?

Most the respondents (60%) reported that they did not face any problems with the system. 29% of the respondents had faced problems with the system and some respondents did not know. It is nearly impossible with a new computerised and networked university to encounter no problems with the system internally or externally (Figure 5.19).

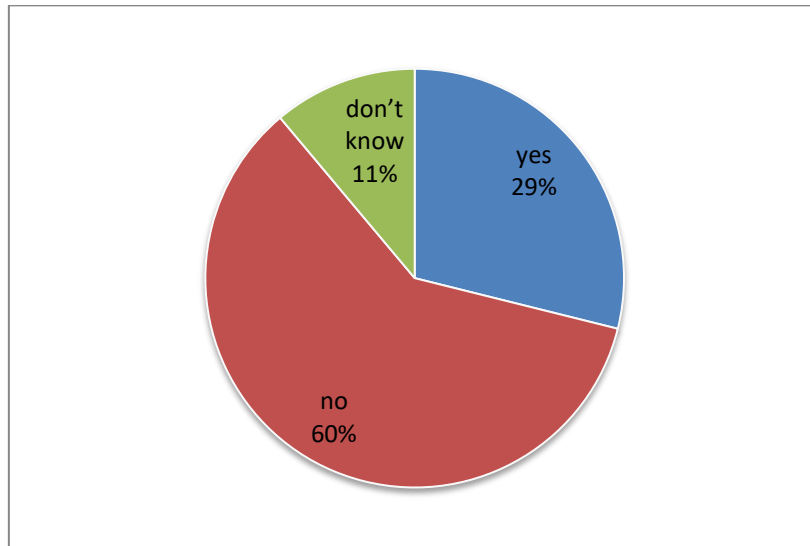


Figure 5.19: Problems faces with computer system

5.4.10 Q10: Do you find yourself asking others for help, or helping others?

It is interesting to note that while the majority of respondents reported that they faced no problems with the system, 22% have at some point asked for help when using an IT system. If people need to ask for help, then it could be an indication that the system is not user friendly. 36% of the respondents had both asked for and given help (Figure 5.20).

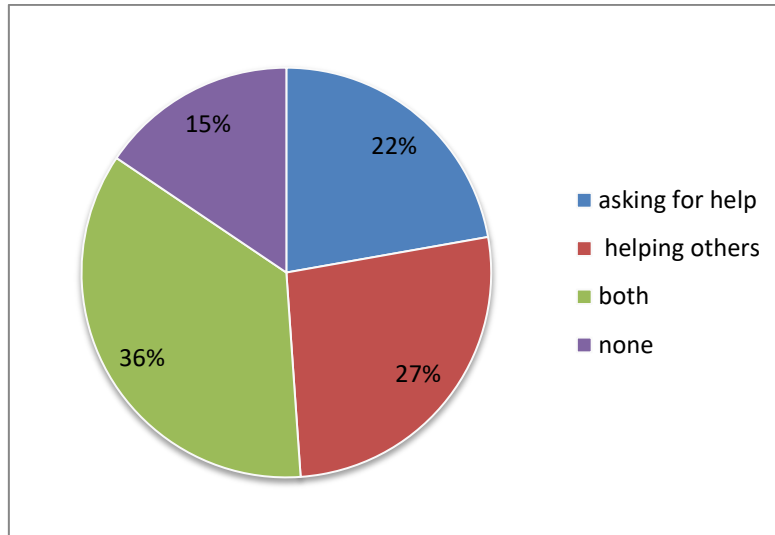


Figure 5.20: asking for help/helping others

5.4.11 Q11: Please list and rate (1-5) any problems that you have faced in the past month:

This question was asked to know the common problems faced by PNU employees. The respondents had faced three major network problems in the past month; six of the respondents face either slow network, no network coverage or limited network time.

5.4.12 Q12: On a scale of 1 – 5 how computer literate do you see yourself?

The aim of having this question is to know the computer qualification and experience level of PNU employees in their own opinion. Considering the respondents in this survey are the ones who have IT jobs and IT qualifications, it is surprising that when asked, on a scale of one (illiterate) to five (very literate) how computer-literate they saw themselves, most of them submitted a low point two (semi-illiterate) or less. Twelve of the forty-five respondents considered themselves as very literate (Figure 5.21). The zero indicates no response to the question. This suggests that they are not qualified to handle an IT system.

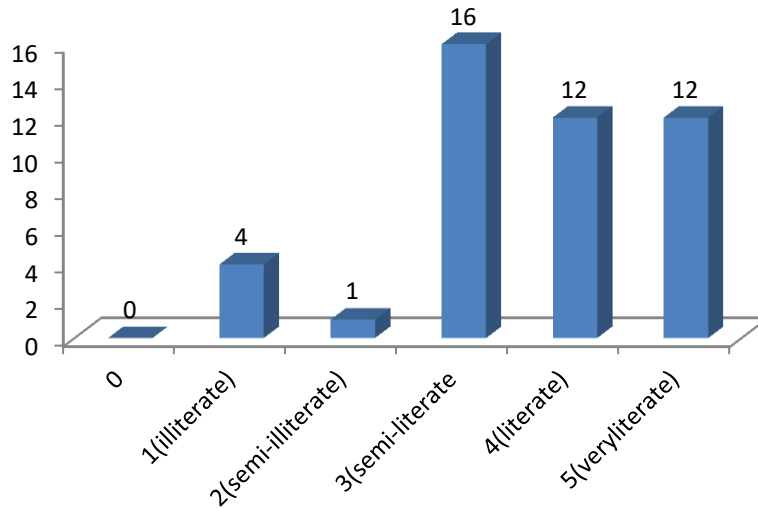


Figure 5.21 Computer literate

As shown in table 5.3, the result is the same as Table 5.2 in that the numbers of training programmes undertaken has little effect in the level of computer literacy among IT employees with different levels of qualification. The respondents for example, with high school degree and IT related education with three training programmes consider themselves between computer semi-literate to computer literate, whereas some with high school degree and IT related education with four training programmes consider themselves to be between computer illiterate to semi-literate. This also shows that the training programmes given to the employees has little effect in raising the level of employees computer skills and this training needs to be modified to get more benefit from them.

Table 5.3: the relationship between: Qualification, Number of training and Computer literate

Qualification	Number of training	Computer literate
High school /IT related education	3	3-4
	4	1-3
High school /no IT related education	1	3-4
Bachelor/ IT related education	0	5
	1	3-5
	2	1-5
	3	3-5
	4	2-5
Bachelor/no IT related education	0	1-4
	2	1-4
	3	3-4
	4	3
PhD/ no IT related education	1	3-4

5.4.13 Q13: Do you feel the IT systems at PNU are difficult to use?

This question is focused on how PNU end users evaluate the IT system difficulty of use. Interesting results were gathered concerning the ease of use of the Banner IT system. 7% of the respondents thought that the system is very easy to use and 35% of the respondents thought it was a fairly easy system, disagreeing with those who found it difficult to use. Those who found it easy to use are more likely to be the employees who attended training courses on the IT system. 41% thought that the system was neither easy nor difficult (Figure 5.22). Table 5.4 shows that there is a positive relationship, correlation = 0.525, between IT qualification and perceived system difficulty of use.

Table 5.4 : Correlations between System difficulty and IT qualification (as presented by SPSS)

		Sys Difficulty	IT qualification
Sys Difficulty	Pearson Correlation	1	.525**
	Sig. (2-tailed)		.000
	N	45	45
IT qualification	Pearson Correlation	.525**	1
	Sig. (2-tailed)	.000	
	N	45	45

** . Correlation is significant at the 0.01 level (2-tailed).

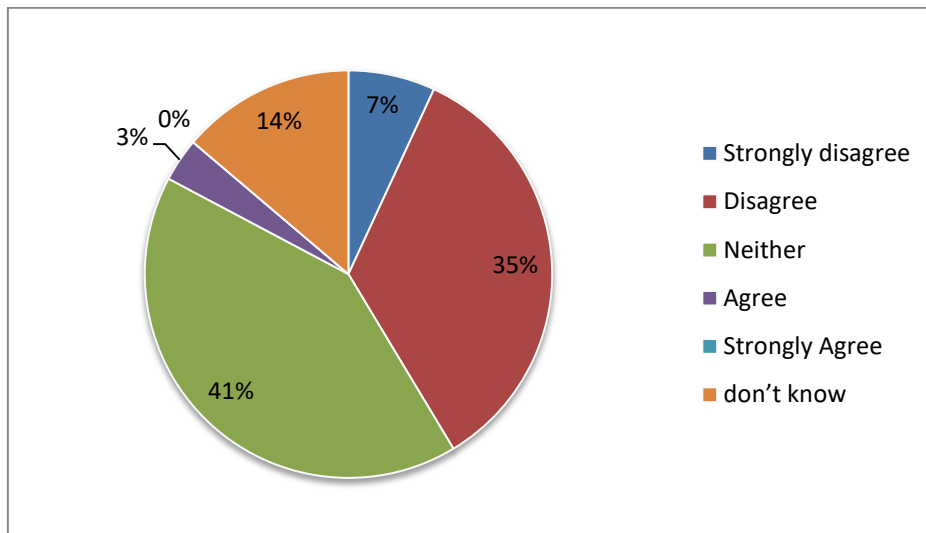


Figure 5.22 Perceived IT system difficulty of use

5.4.14 Q14: How many passwords do you use to access the various IT systems at PNU?

This question was asked about the number of passwords the respondents use. The reason for asking this question is to see, based on the number of the passwords, if the employee knows the true reason for using a password and the importance of it to the security of the information. It also shows how aware the employee is of the security of importance of information. 16 of the 45 respondents use one password to access various IT systems at PNU (Figure 5.23). This is unsurprising, as almost all the employees access only one IT

system, Banner, at PNU. Those who answered otherwise were the ones who may not understand the question since there is, at most, two access password to PNU systems and it is likely that, like the non-IT staff their responses referred to their use of passwords for non-work internet access. Therefore, any further use of this survey would need to clarify the question so it is not ambiguous.

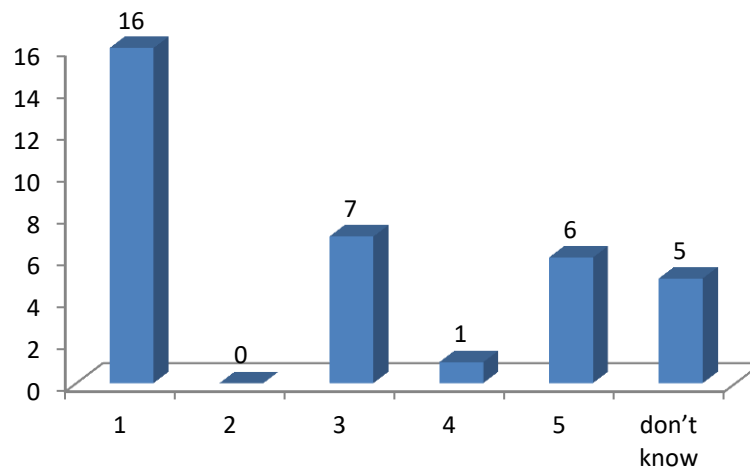


Figure 5.23: Number of passwords used

5.4.15 Q15: How much training on the Banner systems have you received?

The reason for this question is to see if the employees get enough training before they use any PNU system. The lack of training on the Banner system received explains why most of the respondents found the Banner system difficult to use. According to Frost (2013), employees who receive enough training will be able to perform their job better. The lack of training could also cause misuse of the IT system. Most of the respondents (39 out of 45) either received no or little training on the Banner system (Figure 5.24).

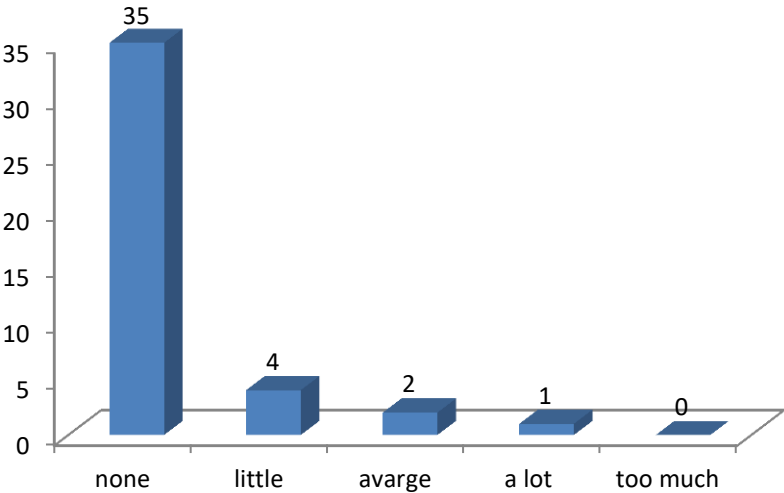


Figure 5.24: Training on the Banner System

5.4.16 Q16: What do you see the solution being to improve the computer systems at PNU?

To improve the IT system at PNU, the majority of the respondents reported that they should have more training courses. Some respondents thought that increasing the number of IT staff could help improve the performance of the IT system. Some respondents thought that the entire system should either be modified or replaced (Figure 5.25).

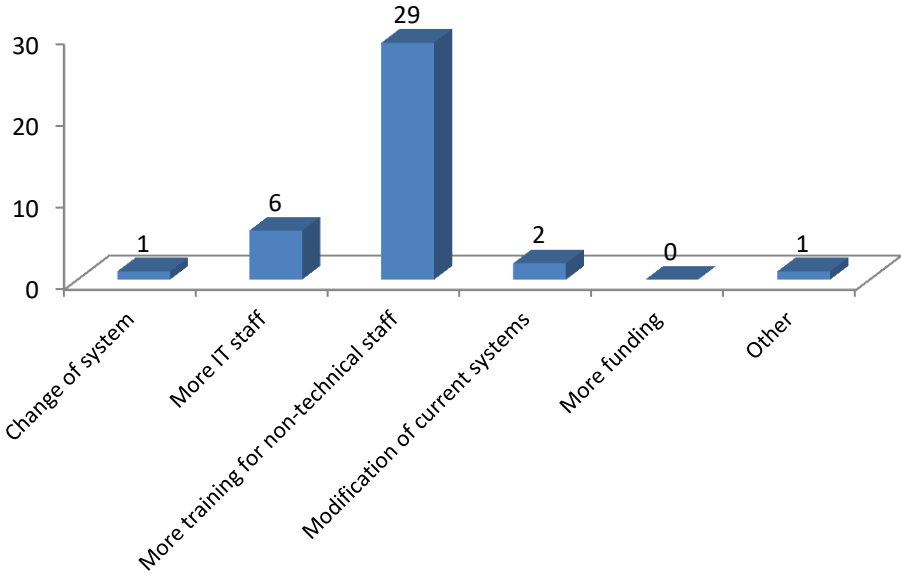


Figure 5.25: Solutions to improve the computer system

5.4.17 Q17: How much external support does PNU currently utilise for the current information systems?

This question was asked to see if PNU IT is still depending on external support. From the respondents' point of view, PNU needs daily external support for the current information systems. Some thought that PNU has weekly or monthly external support. The majority did not know (Figure 5.26).

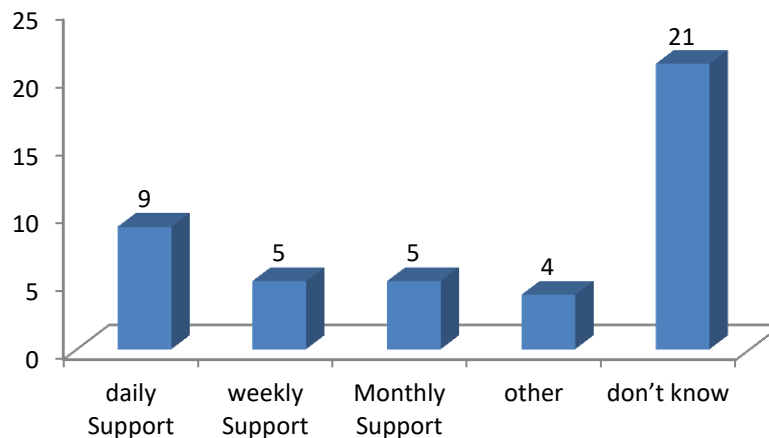


Figure 5.26: External support

5.4.18 Q18: Do you feel the current IT department is managed correctly?

The respondents have mixed feelings about the current management of the IT department. 14 out of 45 of respondents neither agreed nor disagreed that the current management correctly manage the IT department. This is the same as the number of respondents who believed that the current management team correctly manages the IT department (Figure 5.27). Eight of the respondents do not agree that the management team are doing their job correctly even though the PNU working culture is hierarchical with managers directing their employees and the employees tending not to use their initiative to take action. The employees just show respect and not question the managers' authority. However, it is important that management's job is respected by all employees in order to achieve the University's goal and mission in securing its information system. Management should make

sure that all employees agree with the management's decisions, which helps to achieve the organisation's goal to create a good team atmosphere (Smith, 2013).

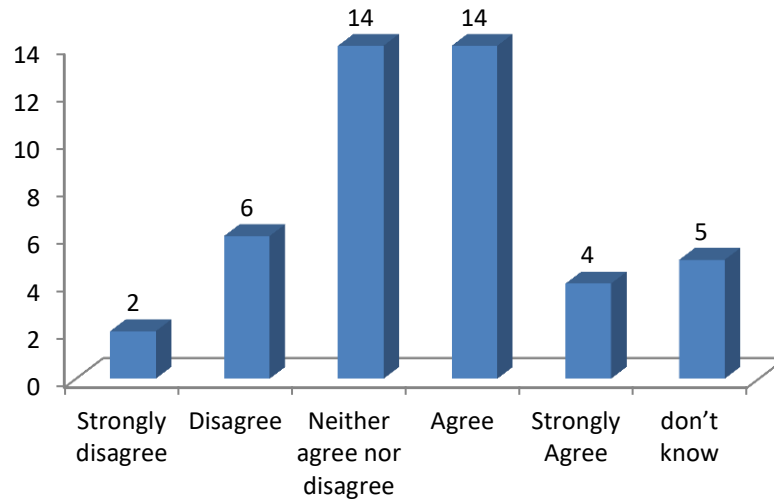


Figure 5.27: The IT department management is managed correctly

5.4.19 Q19: Have you found this training to be beneficial?

Most of the respondents had not taken any training courses, so they did not respond to the question about whether they found the training to be useful. Only one answer was collected, which indicates there were not enough training courses.

5.4.20 Q20: How secure do you feel the current computer systems are at PNU?

Almost all the respondents, 80%, thought that the PNU IT system is, at least, somewhat secure, with 18% believing it to be very secure. 7% thought it is not secure and 13% did not know (Figure 5.28). This indicates that either the system is reasonably secure or, more likely, considering the computer literacy of participants, the IT staff are simply ignorant of the threats to IT security at PNU.

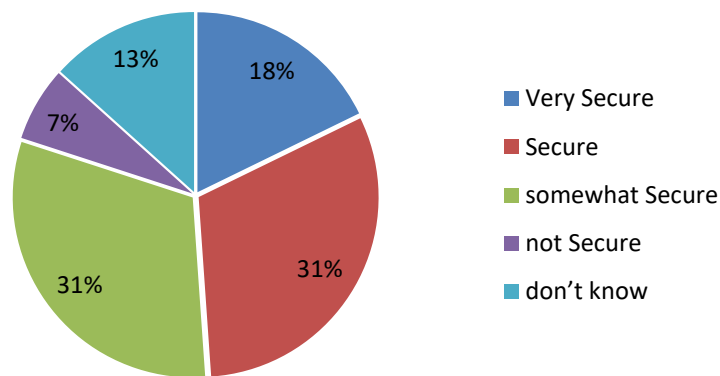


Figure 5.28: Security of the current computer system

5.4.21 IT Staff Survey Conclusion

It can be concluded that the IT employees need more than one training programme to enhance their knowledge of the system they use. Based on their responses, most IT employees did not take any training courses before they used the system for the first time and asked for more training courses to help them understand the system. Untrained PNU IT employees may avoid embarrassment and discomfort by not doing the work required and they may make mistakes that jeopardise systems' security. PNU needs to have very effective organised training programmes that cover all employees to help its employees gain their dignity, respect and safe face (See section 4.6). PNU should also monitor the training programmes and measure the effectiveness of their performance through surveys.

Nepotism, hiring inexperienced, underqualified relatives or friend, could be one of the reasons that some employees are not fit for the work. As a result, most of the respondents are young, relatively inexperienced, and hold a bachelor degree as their highest qualification. Therefore, for the time being, PNU needs to educate the IT employees by forcing them to continue studying. Moreover, human resources at PNU needs pay more attention in assigning the right person for the right job, avoid the traditional favouritism of friends and relatives (See section 4.7).

According to PNU work hierarchy, most IT management jobs are handled by men, even though, it is an all female university. This can cause gender communication issues (see section 4.5). The IT survey result shows there are communication problems between the users of the system and the IT staff. Therefore, PNU needs to pay more attention to this problem and find a way to improve the communication level between its employees.

5.5 Summary of the finding results

The results from both surveys show:

1. Older groups are more likely to be computer illiterate. This is probably because they did not get a chance to study IT early in their life.
2. There is a need to improve the quality of training courses to improve IT employees' qualification.
3. The number of training courses has a significant effect on how easy an IT system is to use for both non-IT staff and IT staff alike. The more training attended, the easier people find the systems to use.
4. Only one IT system is being used at PNU by most people, which is the Banner system. The predominant system in use at PNU is, therefore, the Banner system.
5. Most of the respondents used only one password as they only used one system.
6. When users need help in using the information systems at PNU, respondents mostly sought IT help from their colleagues not the university's IT staff.
7. Staffs are generally unaware of the security threats to the PNU systems.

The above findings reveal the following fundamental problems with IT and information systems security at PNU:

1. One of the problems is that the main data entry software used by PNU employees is the Banner system which seems to have a usability problem. Q14 of non-IT survey indicates that most participants find the IT system that they use that most, the Banner system, is very difficult to use. The difficulty of using of the Banner software could affect the authenticity and reliability of the information it holds. The resolution for the Banner system usability could be to update and improve the system and to introduce good training programmes.

2. There is a problem is the quality and quantity of the training programmes. Q5 of the non-IT survey and Q15 of the IT survey show that the majority of IT system users did not take any training courses. This leads to employees mishandling the systems and not adequately understanding their job. The solution could be to measure the effectiveness of the training programmes by, for example, undertaking random assessments of the trainees before and after the training.
3. There is a possible problem of password selection awareness which could threaten and affect the security of the PNU information system but the ambiguous nature of the question asked means that no definite conclusion can be drawn on this. However, the general level of computer literacy has been found to be low so it is likely that the importance of passwords is not well understood. The resolution could be to educate employees of the true significance of passwords. Automatically checking for a strong password and not accepting a weak one, enforcing periodic password change, and implementing a password awareness programme are all highly recommended.
4. There is problem is the lack of communication between users and IT staff. In Q14 of the non-IT staff survey, respondents complained about communication between themselves, as system users, and the IT staff. This leads to IT staff not knowing the problems the end users face, which in turn can cause breaches and vulnerability to the PNU information system. The solution could be improving all kind of communication such as, face-to-face, voice, mail and email and video, between the end users and IT staff and encourage feedback between them.
5. The last problem is the lack of information security awareness. This can lead to employees unknowingly misusing the information system. The solution could focus on special awareness techniques using all kinds of media and multimedia, the social networks, advertising, workshops and training programmes.

All of the issues found could have a huge effect on the security of the information security system at PNU. A further investigation, interview and observation were made to verify these findings. Chapter 6 describes this in more detail. The collected data in this chapter along with the data collected in the next chapter is then used in the formulation of information security policy framework described in the following chapters.

Chapter 6 Data Collection: Interviews

The purpose of this chapter is to collect issues affecting Information System Networks at knowledge-intensive organisations in Saudi Arabia through the use of observation and data collection interview methodologies. Interviews were conducted for three different purposes, one interview was conducted to determine who manages the knowledge-intensive organisation information systems, how they are managed, what services the IT outsource companies provide and to measure the weaknesses and the defects of the information security systems from an IT management point of view. The second interview was conducted to measure the weaknesses and the defects of the knowledge-intensive organisations' information security systems in Saudi Arabia. The third interview was conducted to gather information in relation to the ISO 27K (information security management and policy) accreditation of current computer information systems at knowledge-intensive organisations in Saudi Arabia. All universities in Saudi Arabia are encouraged by the Ministry of Education to get this accreditation to improve their overall level of education accreditation (SASO, 2015).

6.1 The goal of the Interviews:

The main goal of interviews was to get an overall idea of the information systems available at knowledge-intensive organisations in Saudi Arabia and their weaknesses and defects, which could lead to major breaches in information security. Also, part of the goal was to get a clear idea of who manages the information systems, how they are managed and what services the IT outsources companies provide. Most of the interviews were conducted at Princess Nora University (PNU), the case study used in this research. As stated in chapter 1, the reason for this selection is that PNU is:

- One of the largest universities in Saudi Arabia
- A new university that is just starting to establish its policies.
- An all-female university led by IT male administrators which has a potential gap in the communication between them.

- PNU is new to the concept of IT system security.

PNU used to have no networked IT system and most of the information was stored on standalone PCs or on paper. In 2010 PNU assigned an outsourcing Indian company called Wipro to help design and manage its IT systems. Wipro focusses on the IT services and BPO (Business Process Outsourcing) business. According to the Wipro website (wipro.com, 2012), this company offers a wide range of IT, BPO and R&D services such as:

- Analytics & Information Management
- Business Process Outsourcing
- Consulting Services
- Product Engineering Services
- Mobility
- Business Application Services
- Cloud Services
- Eco Energy
- Infrastructure Management Services

Relatively few employees know that Wipro provides PNU with analytic and information management services. The majority of the employees don't even know that the information technology system management has been outsourced.

The purpose of this investigation was to further investigate issues raised from the results recorded from surveys taken at the beginning of 2013, when the respondents were found to be facing significant problems with:

- Lack of network coverage.
- Slow network and internet.
- Accessing their account.
- Passwords being changed without them knowing.
- Accessing email.
- Application software not being updated.
- Lists of students not showing all names.
- Not being able to use a computer (student).
- Insufficient or inappropriate antivirus software being used.

In particular, the group were found to be facing significant difficulties with:

- Using the Banner system.
- Banner system accessibility.
- Communication with IT staff.
- Accessing appropriate training programmes.
- Software/system maintenance.
- Search functions and data structuring.

Other Issues rose which relate to the investigated issues recorded from surveys including structure, physical location and gender communication of the university IT management. In most knowledge-intensive organisations in Saudi Arabia, male employees handle IT management and security. PNU, for example, has a minority of male employees handling IT management and security, and a majority of females, who are the end users, such as staff, faculty members and students. The structure of the PNU information system security management is shown in Figure 6.1.

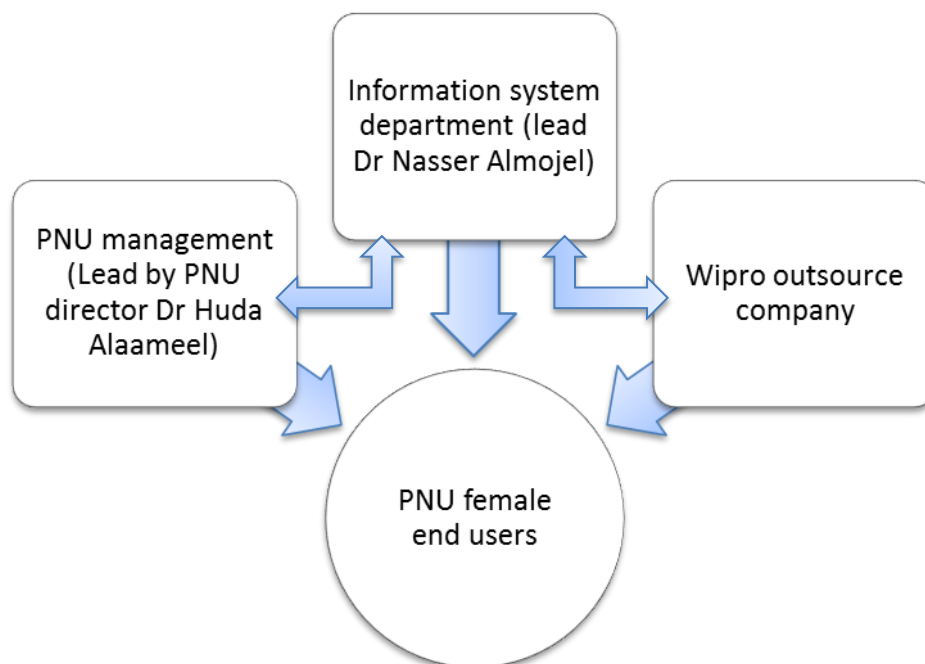


Figure 6.1: The Structure of PNU IT Management.

As seen in the Figure 6.1, there is two-way communication between the IT department and the PNU management and, also, two-way communication between the IT department and the outsource company, Wipro, that manage PNU network and data centre. However, there is only one way communication to the female end users from employees of the IT department, the PNU management or the outsource company Wipro, with very little communication or feedback in the other direction. The IT department, the outsource company and the PNU management do their job without having feedback from their female employees.

In addition, there is a physical communication barrier at PNU. Buildings at PNU are Located far from each other (see Figure 6.2).

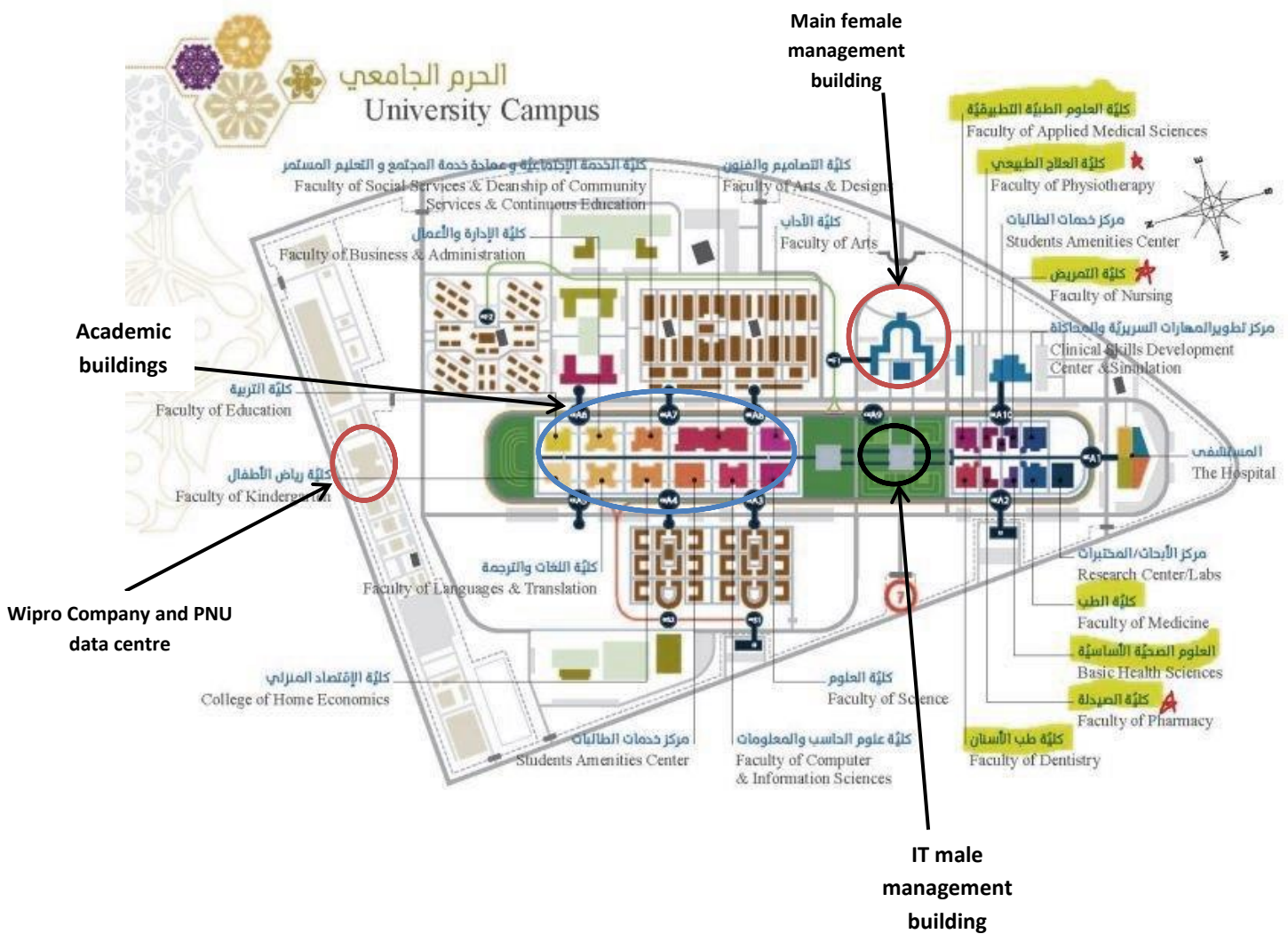


Figure 6.2: PNU campus map
Source PNU website 2013

Figure 6.2 shows that the main management building is far from all academic buildings where most end users are. Either an over-ground metro or car is used to go to the main management building from any college building. The male IT management building is located between the main management building and the academic buildings. The data centre and the outsource company (Wipro) are located at the far end of the university campus. No female employee is allowed to go to the male IT building.

PNU has a culture issue related to gender communication. Therefore, PNU female employees are lost here, not knowing whom to report to if they face any non-technical problem concerning the information system. The management, on the other hand, believe that everything is working fine since no one is complaining. PNU has other culture issues related to the management's strong hierarchical structure, in that the IT management gives orders to the end users without giving their employees a chance to question any decision or command, report their non-technical problems or submit any feedback to them. The huge gap of communication between the two groups could damage the mission of PNU in securing their information system.

6.2 Interview Techniques

In this study, three interview techniques were used to collect data: structured, unstructured, and semi-structured interviews. According to GAO (1991), interviews that gather information by telephone call or face-to-face are structured interviews when the interviewer has a prepared questionnaire, asks the questions and records the answers without getting any further details. Whereas, interviewers using semi-structured interviews have an overall list of questions to ask but allow for more detailed information to be gathered by turning the interview into a conversation which can lead the interviewer to add more questions to clarify their point of view (Lindlof and Tylor, 2002). Unstructured interviewing is when the interviewer introduces the scope of the interview and asks as many questions as needed to the interviewee and records their replies (Lindlof and Tylor, 2002). Moreover, four interview mechanisms have been used in this study: telephone interviews, face-to-face interviews, group interviews and, if requested, interviews by email.

6.2.1 The first interview collection technique

The interviewees for this interview were the Head of the Information Technology Department, Dr Nasser Almoje, the Information Technology Data Centre Manager at PNU, Dr Ghazi Alghamdi and the representative of Wipro the outsource company at PNU, Mr Mohamed Kreem. Information was collected using a questionnaire filled in while telephone interviewing or sent by email if they requested. The interviewees and the reasons for choosing them were:

- The Head of the information technology department, Dr Nasser Almojel, who was interviewed by telephone to understand:
 - How the IT staff assess security risk.
 - Whether they have a security policy documented and distributed to all employees and whether it is available online.
 - How the attempted/actual security breaches are monitored and documented.
 - What cyber law affects the IT security and are staff aware of IT regulation.

The telephone interview was in Arabic and lasted for ten minutes. Dr Nasser's responses were read back to him by the interviewer to avoid misunderstanding.

- The information technology data centre manager at PNU, Dr Ghazi Alghamdi, to know:
 - How the IT staff assess information security risk.
 - Whether they follow an information security management best practice framework.
 - How attempted/actual security breaches are monitored and documented.
 - What cyber law affects the IT security and whether staff are aware of IT regulation.

An English version of the interview questionnaire was sent to Dr Ghazi via email on his request and the responses were emailed back a few days later.

- The representative of Wipro the outsource company at PNU, Mr Mohamed Kreem, to know:
 - How Wipro assess information security risk.
 - Whether they follow an information security management best practice framework.
 - How attempted/actual security breaches are monitored and documented.
 - Whether Wipro carries out any IT security auditing.
 - How often do they conduct auditing, and whether it is self-auditing, internal auditing, and/or external auditing.

A face-to-face interview lasted for half an hour and was conducted in English, the spoken language of Mr. Kreem. His responses were then read back to him by the interviewer to avoid misunderstanding.

6.2.2 The second interview collection technique

Face-to-face interviews were conducted with the female end users who were opportunistically selected as they are mostly from the Computer Science College, the researcher's college, and categorised into four groups:

Management:

- The Dean of the Computer Science College, Dr Seham Alshabanah.
- The Head of Student Affairs, Dr Meznah Alzahrani.

Academic:

- An Information Systems Department lecturer, Manar Bagaees.
- Six lecturers from the Information Technology Department.

Staff:

- The secretary of the Dean of the Computer Science college, Affaf Alshabanh
- Seven PNU employees from Student Affairs.

- An IT female technician, Monira Almojel

Student:

- Ten students from the Information Technology Department.

A set of questions were prepared for the interviews, but a more flexible style was adopted allowing the interviewer to deviate from the set questions to enable interviewees to clarify or elaborate on the points they have made.

On the subject of the Banner System, the interview questions included:

- Is the Banner software easy to use by all employees and students?
- If not, what is the weakness of the Banner system?
- Which part of the Banner software do you find confusing, making data entry harder?
- Is there any guideline, help or manual on how to use the Banner software?
- Do you get any kind of training before using this software?
- How available is the Banner software?

Other questions were included in this interview such as:

- Do you use any external data storage media?
- How do you communicate with the IT technicians?
- How do you report an IT problem?

6.2.3 The third interview technique

Interviews on ISO security accreditation were conducted to compare two knowledge-intensive organisations in Saudi Arabia, one that has ISO27K accreditation Imam Muhammad ibn Saud Islamic University (ImamU) and the other (PNU) which is in the process of applying for accreditation. The reasons for choosing Imam University are:

- It already has ISO27K accreditation. Only ten Saudi Arabian organisations have ISO27K accreditation, including ImamU, Saudi Telecom Company (STC), SAMB Financial Group, Aramco, Takamul and Alrajhhi Bank (Mushkhs, 2008).

- Many universities in Saudi Arabia apply the same education system as ImamU, such as King Saud University in Riyadh and King Abdulaziz University in Jeddah. These universities are still seeking ISO27K.
- Although they work in separate environment, ImamU has almost equal male and female numbers of students and employees, unlike PNU which has only female students and most of the staff and employees are women.

The interview was conducted to see how the process of getting the accreditation is conducted and who and what were involved. The communication culture of both universities necessitated either a telephone call or email for this type of interview since the employees in charge of both organisations were all male. An Arabic copy of interview questionnaire was emailed to both ImamU and PNU as requested.

6.3 The data collection interview design

The lack of gender communication due to culture at PNU necessitated either a telephone or email interview for all males. As preferred, a list of either Arabic or English interview questions was used for the Head of IT Department, Dr Nasser, Mr Mohamed Kreem, Wipro representative, and Dr Ghazi Alghamdi, PNU IT data centre manager, who are all responsible for the security of the information system at PNU. Dr Ghazi Alghamdi preferred to have the English version of questionnaire sent to him via email. It was sent to him on September 20th 2013, while Dr Nasser and Mr Kreem both gave interviews of approximately 20 minutes each. The interview questionnaire consists of three parts that covers three areas:

Part 1: Checking the vulnerability of PNU information security.

Part2: Checking PNU employee and user awareness.

Part 3: Checking training programmes.

Face-to-face interviews were conducted with all the female lecturers at PNU who had agreed to be interviewed. All the interviewee female lecturers and students are from the College of Computer Science. They were picked because they are the people who were good with computers compared to other colleges. The interview time varied, depending on the

free time each lecturer had, but was about 20 minutes on average. Ten students who use the Banner application software the most also gave a 30 minute group interview, as did seven student affairs employees who work on data entry using Banner so, therefore, could pinpoint some of the Banner security breaches.

Because of the poor level of English of most the interviewees, the interview questionnaire was presented in the Arabic language to avoid misunderstanding or alienating staff members. The interviewer wrote down the answers. A formal letter of request was given to the interviewee by the Dean of the Computer Science College to explain the interviewer's mission. The interview questionnaires were focused mainly on the use of:

- Banner, the university application software, a comprehensive information database system that contains information about students, faculty, staff and courses designed by a company called Ellucian (Ellucian.com, 2012);
- Isnaad, a ticketing system used by IT staff only to submit hardware and software problem requested by end users;
- Trasul, new application software used by employees for either sending or receiving university regular mail electronically.

The interview questionnaire was focused on the usability of the university application software, gender communication, availability and security of the information they handled. Some of the interviewees, at the beginning, such as the Head of Student Affairs Dr Meznah Alzahrani, seemed to have no problems with the system and took more of a defensive position with regard to the system until more explanation of the goal of the study was given and more questions were asked to reveal some of the breaches of the system.

6.4 Initial interview

This interview was conducted to determine how and who manages the information system and what services the IT outsource company provides and measure the weaknesses and the defects of the information security system from IT management point of view, who mainly consist of male employees. It consists of three parts, the IT vulnerability, user awareness and training programmes and are explained in the next subsection, 6.4.1-6.4.3.

6.4.1 Part 1: Vulnerability of PNU's information systems

The main purpose of the interview was to check the vulnerability of PNU's information systems. Vulnerabilities can be caused by flaws in software and hardware design, weak management processes, a lack of awareness or education/training programmes, and mishandled upgrading or updating of the current practices. An update of the Banner system at the beginning of 2012 caused much disruption because of some the important features were not active. An exploitation of vulnerabilities may cause real threats to an organisation's information assets. Part 1 of the interview questionnaire consists of 12 vulnerability questions. The questions were put to senior managers, the Head of the IT department, Dr Nasser Almoajel, the IT data centre Manager, Dr Ghazi Alghmdi, and Wipro Company representative, Mr Mohamed Kreem. The questions and their answers are explained next.

Question 1: Are your employees aware of the importance of the information they are handling?

Dr Nasser, the head of the IT department at PNU, answered that the employees are the main problem for IT security and they are in the process of applying an awareness programme to resolve this problem. According to Dr Nasser, the awareness programme is designed by a "good company" which he did not reveal. He asked the interviewer for an opinion of the awareness programme and promised to send an email about this programme. This email has not yet been received by the interviewer. Mr Kreem, the Wipro Company representative has been assigned to manage the PNU network and data centre and he had never been in touch with any PNU female employees because Wipro is, due to PNU culture, in an isolated building so he could not answer this question. Dr Ghazi, on the other hand, submitted a written version of the interview questionnaire via email. He believes that all employees are aware of the importance of the information they are handling but he did not elaborate on his answer or give any further explanations (Appendix B has a copy of Dr Ghazi answers to the interview questionnaire).

Question 2: Are you aware of the risk of losing original information due to the weakness of the information security system?

Both Dr Nasser and Mr Kreem think that, technically, the PNU information system is strong and there are no weaknesses in the system. However, Wipro think that the weaknesses in the system could come from either the application program which is not under their control, or it could be caused by the two Internet service providers, STC and Mobily. Dr Nasser still thinks that if there are any system weaknesses they are caused by the system users. Dr Ghazi's answer for this question was again that he is aware of the risk of losing original information due to the weakness of the IT security system but gave no further explanations.

Question 3: Where do you think the weaknesses in the university information security system lie?

Dr Nasser believed that the weakness of the security system is always the employees. Employees are not aware of the importance of the information they are handling and the dangers of misusing this information. He believed that the awareness programme will help minimise this problem. Mr Kreem believed that the Internet service providers, STC and Mobily, were the weakness in the PNU security information system because most of the problems relating to the availability of the system were caused by these ISP companies. Dr Ghazi claimed that there is no weakness in the university information system at all.

Key answers affected by culture in Q1: Admitting to applying an awareness programme by a company but not revealing the name of the company, isolation of building separating the outsource company from the end users and that the management did not give any further explanation of their answers, all indicate there may be more of a problem than was admitted.

Key answers affected by culture Q2: The claim that the IT systems are strong with no weaknesses shows the management are unable to admit that anything can be wrong. The outsource company have no control over the application programme that may cause system weaknesses because of the hierarchal management structure. The users were blamed as the only system weakness and again the management did not give any further explanation.

Key answers affected by culture Q3: The conflict in the answers over what weaknesses exist indicates that the answers may not be truthful. Management do not like to reveal system weakness, as they do not want to accept any criticism. The outsource company have limited power, due to the hierarchal management not wanting to give away any power.

Question 4: Does the university implement and develop detection, prevention, and recovery controls to make sure that their information is protected against any risk and malicious attack?

The answer by Dr Nasser was that they do have physical technical controls such as a firewall, antivirus software and non-activate smart card access controls. They also perform a daily backup process. Mr Kreem believed that that his responsibility was only to manage the location of the data and the availability of the network. Dr Ghazi claimed that the University does implement and develop detection, prevention and recovery controls to make sure that their information is protected against any risk and malicious attack. Again he gave no further explanation.

Question 5: Do you have a backup policy? Do you regularly back up and test the organisation information and software according to the agreed backup policy?

PNU has a backup system; however does it follow a backup policy? There is no documented backup policy. However, according to Dr Nasser a daily backup is performed. They do daily backups and testing but do not follow any backup policy. The entire backup is done by male experts in the IT management building where Dr Nasser's office is. Wipro, led by Mr Kreem, is in separate building. Dr Ghazi agreed that the university has a backup policy but did not add any more details on that policy.

Question 6: In what timescale could services or data be restored?

Dr Nasser and Dr Gahzi did not understand this question. Dr Gahzi answer was "I am not getting what you mean".

Key answers affected by culture Q4: The management's claim that they implement and develop detection, prevention and recovery controls so that information is protected against any risk and malicious attack, again shows that management is unable to admit that anything could be wrong with the system. Management did not give any further explanation, being unable to accept criticism.

Key answers affected by culture Q5: There is no documented backup policy but it is claimed that a backup is performed daily; this again shows that management is unable to admit that anything could be wrong with the system. Management did not give any further explanation, and were, again, unable to accept criticism.

Key answers affected by culture Q6: The lack of understanding here indicates that the system has probably never been restored with a backed-up version. This could mean backups, if performed at all, are not executed properly to enable a system restore. However, the management would never admit this, even if they understood the question.

Question 7: How often does your information system receive malicious attacks and how do you monitor it?

Dr Nasser said that they do two kind of monitoring against any attacks; one daily and the other one is when PNU gets a warning from the Ministry of the Interior that a government department has been attacked. Information security is managed by Dr Nasser's group of workers and not Wipro. Dr Ghazi expressed that the university daily receives malicious attacks and he and the information security staff use different solutions and techniques, but he did not give any details of the type of techniques used.

Question 8: When is the last time you had a security attack and what kind was it?

Dr Nasser did not have an answer to this question; however he transferred my call to Dr Ghazi who is the Manager of Information data centre at PNU. Dr Ghazi answered that the last time they had a security attack was DDoS (Distributed Denial-Of-Service) and he did not mention when that was.

Question 9: How are attempted/actual security breaches monitored and documented?

Dr Nasser said that they do daily auditing to check for any security breaches and as requested by the Ministry of the Interior. However, they are not documented. Dr Ghazi's

answer was that they use different solutions and techniques to monitor the security breaches and again he did not give any more details.

Key answers affected by culture for Q7 and Q8: Both answers implied that a perfect defence against attack was in place, but neither gave a straight answer as to how many such attacks were received. The lack of knowledge indicates a lack of understanding of the problem and an inability to either recognise or admit that such a problem could exist.

Key answers affected by culture: The lack of documentation or any detail in the answer probably indicates the security breaches are not being properly monitored, again showing an inability to either recognise or admit to any problem.

Question 10: How do you minimise the risk of theft, fraud, or misuse of computer facilities?

Dr Nasser thought that, so far, risk of theft and missing computer facilities were the biggest problem they faced because of the lack of CCTV. They had reported a large number of thefts and missing university computer hardware and software and employees' personal belongings. However, they already have a built-in smart card access control system for computer labs and management offices that are not fully activated. The built-in devices are fully installed but the access cards are still not activated yet, but Dr Nassar did not explain the reason why the access cards are still not activated. A possible reason is that the built-in smart card access control makes a sound every time the door of any lab or management office is opened. This sound caused employees and students' frustration. Dr Ghazi believed that minimising the risk of theft, fraud, or misuse of computers facilities can be undertaken by awareness, training and policy enforcement

Question 11: Do you have any kind of physical protection against natural disasters such as fire, flood or earthquake?

Dr Nasser expressed that PNU uses backup regularly to protect the information against natural disaster. In this case the backup should be on an external server. He didn't explain whether the backup information is held in or outside the university campus. Dr Ghazi agreed

with Dr Nasser and his answer was, yes, they do have physical protection against natural disasters such as fire, flood or earthquake.

Question 12: Do you carry out annual auditing, monitoring and evaluating activities to verify the information security programme effectiveness?

Dr Nasser repeated that they do two kinds of monitoring against any attack, one daily and the other is as requested when PNU get a warning from the Ministry of the Interior when any government department has been attacked. Dr Ghazi believed that the university is planning to do annual auditing, monitoring and evaluating activities soon.

Key answers affected by culture Q10: The fact that they have a not fully activated built-in smart card access and CCTV, indicates that money to buy and built-in new technology is not the critical issue but rather a lack of expertise exists to make effective use of the technology available. Unusually, Dr. Nasser did admit to concerns over the lack of CCTV, but Dr Ghazi played down any threat from theft fraud or misuse.

Key answers affected by culture Q11: The fact that neither could say where the backups were held indicates either a lack of understanding or a lack of truthfulness about the externally held information.

Key answers affected by culture Q12: Here Dr. Nasser is avoiding answering the question, probably because he knew that there was no annual auditing, monitoring or evaluation. Dr. Ghazi, avoided the question by claiming it would be in place soon, though this does mean he had to admit that nothing is in place at the moment.

Table 6.1 shows a summary of this part of the interview on vulnerability of information systems.

Table 6.1: Summary of the first part of the first interview

Question	Dr Nasser	Wipro	Dr Ghazi
1-Are your employees aware of the importance of the information they are handling?	no	Don't know	yes
2-Are you aware of the risk of losing original information due to the weakness of the information security system?	yes	yes	yes
3-Where do you think the weaknesses in the university information security system lie?	users	ISP	No weakness
4-Does the university implement and develop detection, prevention, and recovery controls to make sure that their information is protected against any risk and malicious attack?	yes	-	yes
5-Do you have a backup policy? Do you regularly back up and test the organisation information and software according to the agreed backup policy?	Yes but not documented / no backup policy		yes
6-In what timescale could services or data be restored?	No answer	No answer	No answer
7-How often does your information system receive malicious attacks and how do you monitor it?	Daily	-	Daily
8-When is the last time you had a security attack and what kind was it?	Don't know	-	DDoS
9-How are attempted/actual security breaches monitored and documented?	Daily auditing	-	Different techniques not mentioned
10-How do you minimise the risk of theft, fraud, or misuse of computers facilities?	By activating CCTV		Awareness training and policy enforcement
11-Do you have any kind of physical protection against natural disasters such as fire, flood or earthquake?	Yes	-	Yes
12-Do you carry out annual auditing, monitoring and evaluating activities to verify information security programme effectiveness?	Yes/ daily	-	Not yet

In table 6.1 there is conflict in the answers of many of the questions, especially between the head of the IT department, Dr Nasser and the IT data centre manager, Dr Ghazi. In Q1, for example, concerning the employees awareness of the importance of the information, Dr

Nasser's answer was no, while Dr Ghazi's answer was yes. Also, in Q5, Dr Nasser said that there is no backup policy documented where as Dr Ghazi said there is. Of these two interviewees, Dr. Ghazi's gave the more evasive answers. All Dr. Ghazi's answers inferred that everything was perfect and nothing could possibly be wrong. He was also the one interviewee who did not want to speak directly with the interviewer even by telephone. His attitude illustrates the cultural attitude of Saudi males in senior roles. He would not tolerate any questioning of his role, especially from the female interviewer, to the extent that he didn't even want to speak to her. This deep seated cultural attitude of hierarchical superiority and male dominance will be very difficult to break sown in the Saudi environment and makes it very difficult to get a true picture of what is really happening in the workplace.

6.4.2 Part 2: Employee and users awareness

A huge number of employees are not aware of their exposure to security risks so the organisation should raise security awareness by involving employees in the development of security programme (Enisa, 2010). The ISF standard (Risk Intelligence Ltd, 2012) defines security awareness as "the extent to which staff understand the importance of information security, the level of security required by the organisation and their individual responsibilities." The second part of the interview questionnaire focuses on PNU employees and end user awareness.

Question 1: Do you make sure that employees understand their responsibilities before you hire them?

Dr Nasser explained to the interviewer that they don't do this when hiring a new employee and it is not in the employment requirements. He also explained that to add this requirement it would have to be approved by the Ministry of Civil Service. A written contract is required to employ non-Saudi nationals which must be approved by the Ministry of Civil Service. Dr Ghazi's answer, however, was that they do make sure that employees understand their responsibilities before they are hired.

Question 2: Do you make sure that users understand their responsibility before they use the information system?

Dr Nasser believed that all users of the IT system should know their responsibility before using it. He did not explain how the users know their responsibility nor is there a way to show or tell the users of the IT system their responsibility either electronically on the PNU webpage or in hard copy. However, he believes that it is hard with an environment dominated by women and controlled by the culture found at PNU. Dr Nasser's future plan will focus on changing the university culture. Dr Ghazi's answer was that they do make sure that all users understand their responsibility before they use the information system.

Question 3: Does an employment contract explain what will be done if the employee is found guilty of neglect or misuse of the organisation information systems?

The answer to this was "no", according to Dr Nasser. He said they are facing a big problem concerning employees misusing the university information system. He agreed with the interviewer that it should be added in the employee contract, however, he has no permission to do so. Dr Ghazi believed that all employees are aware of the university policy, even though the university has no written information security policy.

Question 4: Do you use contractual terms and conditions to make sure that all employees and users agree to comply with the organisation information security restrictions and obligation?

Contractual terms are the government's responsibility. As mentioned in question 1, employment contracts have to be approved by the Ministry of Civil Service so any government organisation is not allowed to add a new term or condition even if it is beneficial to the organisation. Dr Ghazi believed that they do so, but did not say how they do it.

Key answers affected by culture Q1: Dr Nasser's answer shows that even at the highest level, there is a reluctance to do anything unless told to do so by their superiors (in this case, the Ministry). Dr Ghazi's answer was another case of not admitting anything could be wrong.

Key answers affected by culture Q2 and Q3: Dr Nasser's answer is more honest as he at least admits there is more to do in this respect. Dr Ghazi's answer is another denial that anything could be wrong.

Key answers affected by culture Q4: This further confirms the observation made for Q1 there is a reluctance to do anything unless told to do so by their superior

Question 5: Do you use contractual terms and conditions to show employees and users how they are expected to handle and help control the organisation's information service?

Dr Nasser expressed that they do not have contractual terms and conditions to show employees and users how they are expected to handle and help control the organisation's information service. They are not allowed to add it unless approved by government. Dr Ghazi gave the same answer as question 4, but he did not say how they do it.

Question 6: Do you have a clear documented information security policy that fits the organisation's security roles and responsibilities?

According to Dr Nasser, they use a modified version of the Saudi Arabia ISO as the university standard. However, this policy is not known to many of the employees. Dr Ghazi believed that the university have a clear documented information security policy, but did not say how this fits the university security roles and responsibilities.

Question 7: Do all employees and users get a copy of the organisational information security policy?

It is not clear that PNU has a documented information security policy. Moreover, the employees are not aware of any such policy. Dr Nasser and Dr Ghazi agreed that there is no documented information security policy. Therefore, the employees did not get any kind of information security policy and have no role in the information security system. Dr Ghazi

believed that all employees get a copy of the PNU security policy without further explanation.

Key answers affected by culture Q5, Q6 and Q7: Again Dr Nasser's answer is more honest as he at least admits there is more to do in this respect. Dr Ghazi's answers make little sense, stating that there is no documented policy but all employees have a copy. This is another denial that anything could be wrong.

Question 8: Are all employees and users aware of the organisation's information security restrictions and obligation?

When interviewing both Dr Nasser and employees, the interviewer observed that the University may have information security restrictions and obligations, as simple as a password restriction, but the PNU did not inform their employees. According to Dr Nasser, the only way to restrict any services from user misuse is just to block the service from the end users. The male IT management did not explain to the employees why they block some services. Dr Ghazi believed that all of the employees are aware of the organisation's information security restrictions and obligations.

Question 9: Are you and all employees aware of cyber law and regulation?

Although Saudi Arabia has a cyber-law and regulation, and the law is available online, Dr Nasser admitted that employees, including management, were either unaware of it or did not know what it is. Dr Ghazi believed that some employees are aware of cyber law and regulation.

Question 10: Do you have policies that explain to the user the punishment if they mishandle information?

Dr Nasser explained that this is not done as such a policy would have to be agreed by the Saudi Arabian government, and they are not allowed to create a new policy unless the government approves it. This could take a significant amount of time. Dr Ghazi's answer was that, yes, they do have policies that explain to the user the punishment if they mishandle information.

Key answers affected by culture Q8: Dr Nasser's answer indicates that some security actions are carried out in a crude, unsophisticated way. This shows either a lack of understanding of what is possible, or a disregard for the users' difficulties.

Key answers affected by culture Q9: A revealing answer from Dr Nasser, but the usual denial of a problem from Dr Ghazi.

Key answers affected by culture Q10: Dr Nasser is again showing a reluctance to do anything without government instruction while Dr Ghazi denies anything is wrong

Table 6.2 is a summary of the part two questionnaire answers.

Table 6.2: Summary of part two of the interview

Question	Dr Nasser	Dr ghazi
1-Do you make sure that employees understand their responsibility before you hire them?	No	Yes, but didn't explain how
2-Do you make sure that users understand their responsibility before they use the information system?	Yes, but didn't explain how	Yes, but didn't explain how
3-Does an employment contract explains what will be done if the employee is guilty of neglect or misuse of the organisation information systems?	No	Yes
4-Do you use contractual terms and conditions to make sure that all employees and users agree to comply with the organisation information security restrictions and obligation?	No	Yes, but didn't explain how
5-Do you use contractual terms and conditions to show employees and users how they are expected to handle and help control the organisation's information service?	No	yes
6-Do you have a clear documented information security policy that fits the organisation's security roles and responsibilities?	Yes, ISO policy	Yes
7-Do all employees and users get a copy of the organisational information security policy?	No	No
8-Are all employees and users aware of the organisation's information security restrictions and obligation?	No	Yes
9-Are you and all employees aware of cyber law and regulation?	No	Some
10-Do you have policies that explain to the user the punishment if they mishandle information?	No, not PNU's responsibility	yes

In table 6.2 there is conflict in the answers of most of the questions between the head of the IT department, Dr Nasser and the IT data centre manager, Dr Ghazi. However, as Dr Ghazi has followed a consistent pattern of claiming everything is perfect and nothing could be wrong, Dr Nasser's answers could be considered to be more honest and trustworthy.

6.4.3 Part 3: Training programmes

Although training programmes are considered by some to be hard, frustrating, challenging, and thankless tasks, educating the organisation's employees on the importance of security and privacy of information and making sure they understand and comply with the requirements are significant to the success of organisation's mission (Herold, 2010). PNU has implemented many training programmes for its employees. This part of the interview covers the training programmes' quality at PNU.

Question 1: What do you think is the best method to educate employees and users about the security of the information?

Both Dr Nasser and Mr Kreem, head of Wipro at PNU, agreed that the best method to educate PNU employees about the importance of information security is through awareness and training programmes. The interviewer confronted both Dr Nasser and Mr Kreem about the level of quality of PNU female IT technicians. They both expressed that they will undertake an assessment of the IT technicians' needs and improve their quality level by giving them more training courses. The majority of the questionnaire's respondents reported that they should have more training courses and most of the respondents had not taken any training courses. Dr Ghazi added that the employees are getting "partially effective training and awareness programmes".

Question 2: Are employees getting effectively trained and receiving awareness?

From Dr Nasser's point of view, he believed that most PNU employees are getting effective training. However, the effectiveness of the training is not measured, nor is it recorded. Section 5.3.5 states that (55 out of 112 respondents) reported that they had never attended any training course and subsections 5.4.5, 5.4.15 and 5.4.19 explain that 33% of the

respondents reported that they had not had any IT related training and asked for more training courses, the majority of the respondents reported that they should have more training courses and most of the respondents had not taken any training courses. Dr Ghazi added that the employees are getting partially effective training and awareness programmes.

Question 3: Do you have adequate and effective awareness and training at all levels of the organisation?

As mentioned earlier, Dr Nasser stated he was adopting a new awareness programme, which has not been applied yet. Dr Ghazi believed that the university has partially effective awareness and training programmes. Dr Ghazi's answer did not submit any explanation of what he meant by partially effective awareness and training programmes.

Key answers affected by culture: Dr Nasser often uses the excuse that he is about to implement something to cover that there is a problem. Dr Ghazi's answer is a very rare admission from him that something may not be perfect.

Question 4: Does the organisation verify that the desired results from training occur?

In rare cases, a survey at the end of each training programme is given to the trainers to measure the quality of the trainer. However, it is not clear if they measure the trainee's performance after any training courses. Dr Nasser and Dr Ghazi stated that they are planning to do so in the future.

Question 5: What kind of measures does the organisation use to verify the effectiveness of the training programmes?

This question was answered by both Dr Nasser and Mr Kreem after the interviewer also confronted them about the poor quality of the training programmes given to PNU employees. Mr Kreem explained that they are planning to use before and after training assessment for the trainees. There is currently no assessment to measure the performance of the trainer. On the other hand, Dr Ghazi's answer was that they use tests and survey to measure the effectiveness of the training programmes.

Question 6: Does the organisation update the education program to improve communication between personnel?

So far, and according to Dr Nasser, there is no education programme to improve communication between personnel. However, he is hoping that the awareness programme would help in this case. Dr Ghazi also agreed with Dr Nasser about not having an education programme to improve communications and to get the right message out to personnel.

Key answers affected by culture: Again Dr Ghazi admits something isn't perfect! Perhaps it is because it is very difficult to say something exists when it is easy to show that it doesn't so that, for training programmes at least, Dr Ghazi is forced to be a little more honest.

Table 6.3 is a summary of part three questionnaire answers.

Table 6.3: Summary of part three of the interview

Question	Dr Nasser	Mr Kreem	Dr Ghazi
1-What do you think is the best method to educate employees and users about the security of the information?	Awareness and training	Awareness and training	No answer
2-Are employees getting effectively trained and receiving awareness?	yes	-	partially
3-Do you have adequate and effective awareness and training at all levels of the organisation?	No	No	partially
4-Does the organisation verify that the desired results from training occur?	No, but planning to do in the future	-	No, but planning to do in the future
5-What kind of measures do the organisation use to verify the effectiveness of the training programmes?	None	Will use before and after assessment of the trainer	Uses tests and surveys
6-Does the organisation update the education programme to improve communication and to get the right message out to personnel?	No	-	No

In table 6.3 there is also conflict in the answers of many of the questions, especially between the head of the IT department, Dr Nasser and the IT data centre manager, Dr Ghazi. However, even Dr. Ghazi has had to admit that the training provision is not perfect. This shows that despite the cultural pressures, a manager will be forced to admit there is a problem when the evidence is obvious. However, perhaps as a face saving measure, Dr Nasser and Dr Ghazi both cover up any inadequacies by claiming that an action for improvement is planned for the future

6.5 Second interview: Interviewing females at the University

A face-to-face interview in either a group interview or a series of individual interviews of a sample of the end users of PNU IT systems was used in which the focus of the interview was the Banner system used by all interviewees. A face-to-face interview was conducted with an opportunistically selected female lecturer at PNU. Also, two group interviews, similar to focus group meetings, were carried out, one with the students and the other with the Student Affairs employees. Most of the questions were related to the use of the data entry application software. The main software used by all the faculties, students and some of the IT staff was the Banner system. Questions related to usability of this system were asked, since usability is related indirectly to the security of information at PNU. The easier the application is to use, the more accurate the entry data will be.

Almost all of the interviewees find the Banner software, not only hard to use, but hard to access and, sometimes, the information for employees' and students' Banner accounts is not available. Lecturers at PNU have faced a lot of problems when using Banner System. Some of the problems are:

- The format of an Arabic name, called the quad name, starts with the first name, middle name (father's name), second middle name (grandfather's name), and last name. Student lists shown in the Banner system start with the last name just like the western style, which is different to the Arabic style, which starts with the first name.
- The two middle names (father's name) and (grandfather's name) share the same field and only the initial of the first middle name is shown in this list. This is also different to the Arabic style, since it is common that some students have the same

first name, middle name and last name. This also can cause duplication names in the list, which can lead to mismatching student grades.

- The total percentage of the grade of the student is entered from a drop down list with only whole numbers to choose, any fraction is rounded to a whole number. This frustrates many of the lecturers because they believe it is not fair to the other students to give students an extra fraction when rounding up.
- The font size of printed student attendance lists given to the lecturers is very small.

6.5.1 General problems

The segregation and strong hierarchical structure environment at PNU causes communication problems with the IT help desk. PNU is male dependent, especially when dealing with IT problems. The end users of the application software are almost all female and when interviewed, the Student Affairs employees explained that they found a lot of weaknesses in the data entry software, the Banner system. For example:

- the printing command is not active,
- there is only one field for the first middle name (father's name) and second middle name (grandfather's name),
- there is no field for the student major,
- it is not easy to search for information,
- After the software was updated most of the data they had entered was missing.

The lack of communication made these general problems major time consuming issues to the female staff and affected the availability and accuracy of the information they handle. Moreover, because of the culture issues and the location of the IT management (see figure 6.2), the student affairs employees tried to express these problems and many more via phone to the male IT technician. The IT male technicians do not respond to any request or feedback from the female employees. This could jeopardise the security of the information system at PNU.

6.5.2 The staff problems

End users and employees at PNU still use a flash memory or USB as an external storage media. Dr Nasser expressed that for security purposes external storage media are not allowed. However, USB ports are built into each workstation of the PNU network system. According to Manky (2010), USB drives, although they are small, cheap, hold a lot of data and are easy to use, are one of the most common ways to infect an information technology network.

They face a communication problem with the IT female technicians although they are around and available. The IT female technicians will not help unless they get a request from the IT male Technician. According to secretary, Affaf Ashabanh, whenever she had any problem she had to call 555 and request help even though the female IT technicians assigned for their college were available. Figure 2 shows the communication process with the cultural problem in which female IT technicians not doing anything unless directed to by their superiors.

Culture Issue: Female IT technicians not doing anything unless directed to by their superiors.

6.5.3 Students' problems with the system

A face-to-face group interview was carried out with opportunistically selected students from the Computer Science College at PNU. The computer science students selected know more about computer than many other students at PNU. Most of the questions were related to the use of the data entry application software. The students reported that:

- The student cannot change data in every field in her record, such as her name, if misspelled, but has to fill in a request form for that instead.
- The GUI of the Banner system is not clear and the help option is either not active or written in English. The Banner system is used by almost all universities in Saudi Arabia. The interviewer sent an English email to Ellucian, the company that designed the Banner software, expressing this problem but has received no response.

- The student has to follow a certain curriculum each semester in order to have a course schedule. If the student somehow misses any of the courses for one semester then she cannot register electronically and she won't have a printout copy of her timetable for the entire year. She has to register for each course in every semester after that manually.

6.6 The results and finding for the first and second interviews

There is a severe lack of communication between male and female employees at PNU. The employees work in two separate environments. Every college has its own separate building and its own female IT technicians. The male IT management communicate with female end users through the female IT technicians who are unqualified or new graduates with degrees unrelated to IT or computers and with no IT experience.

The communication between end users and the IT technicians at PNU is illustrated in Figure 6.3. If an end user has a computer problem, either software or hardware, she has to do the following:

- 1- Call 555, the number for an IT female help desk located in the main female management building.
- 2- The help desk employee places an order using the ticketing system software.
- 3- The help desk employee sends a request to the IT female technician located in same building as the employee who needed help.
- 4- The female technician tries to fix a problem if it is easy to do so.
- 5- If the problem is hard to fix then the local female IT technician asks a male IT technician in the IT management building for a solution.
- 6- The IT male technician sends a solution to the IT female technician.
- 7- The IT female technician fixes the problem or
- 8- The male technician visits the area where the problem is located to fix it at the end of the day, after all females have gone home.

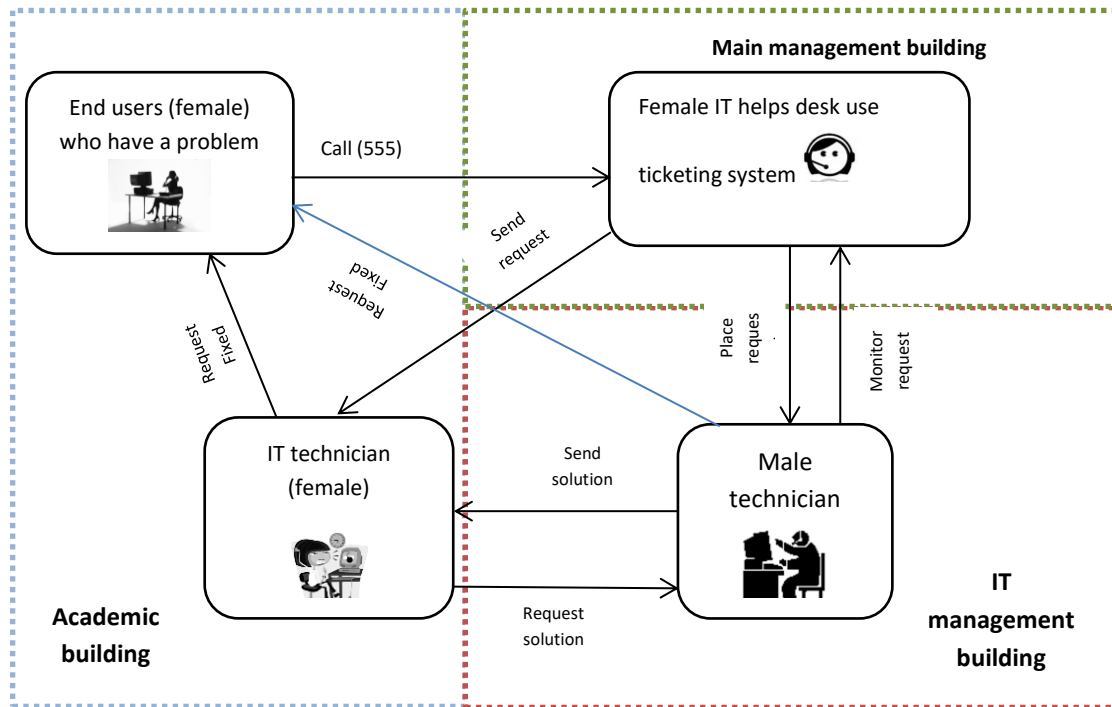


Figure 6.3: Communication between end users and IT technician at PNU

As seen from Figure 6.3, the process is male dependent. According to Monira Almojel, a female technician at PNU, the IT female technicians undertake only simple requests such as, turning an e-podium on or off, changing a printer ink cartridge or connecting a workstation to a printer. Only male IT technicians are able to address complex problems such as adding a new RAM or installing new hardware.

The employees may take a number of training programmes, but the effectiveness of these programmes is not being measured. According to the Student Affairs employees at the Computer Science College, they undertook a number of training programmes in the Banner application software but did not learn effectively from that programme. Some employees, like the secretaries of the departments at the Computer Science College, admitted that they took the training programme for reasons other than learning, for example to break the routine of their work, or because their manager required them to, or to add it to their experience record. The overall evaluation of the effectiveness of the training programme by Students' Affairs staff was that the training is not beneficial to their work and is just a waste

of their time. The employees believed that they learn more when they practice by themselves.

The interviews with PNU employees reveal the weaknesses in employees' awareness of the importance of the information they are dealing with. The employees did not realise the importance of the information in PNU until they were informed of this fact. From an employee point of view, there is no classification of the information handled and all the information is treated equally.

6.7 Third interview: ISO interviews

The purpose of this interview was to help gather information in relation to the ISO 27K (information security management and policy) accreditation of current computer information systems at knowledge-intensive organisations in Saudi Arabia. The findings from this interview helped in the formulation of the information security framework developed in next chapter, Chapter 7 which is designed to assist knowledge-intensive organisations seeking ISO 27K accreditation in Saudi Arabia. Interviews were conducted in two knowledge-intensive organisations in Saudi Arabia, one that already has the ISO 27K accreditation, Imam Muhammad ibn Saud Islamic University (ImamU) and the other in the process of getting it, Princess Nora bint Abdul Rahman University (PNU). ImamU is different from PNU in having a mixed male and female population including staff, academics, administrators and students. ImamU still runs with a segregated environment in which employee and student males are separated from females as is the practice in all Saudi Arabian universities. PNU is an all-female university that has a few male administrators, technical staff and academics. A copy of the interview questionnaires was emailed to both universities as requested. The manager of the information security department of PNU, Sami Alanzi replied to the interview questionnaires submitted to PNU. Waleed Alrodhan replied to the interview questionnaires assigned by the information security manager, Ali Algarni, at Imam University. The result of the interviews is given in table 6.4.

Table 6.4: ISO27K interviews with two universities, PNU and ImamU

Question		ImamU	PNU
1-Has your organisation got, or is it in the process of getting ISO 27k accreditation?		Yes, Nov 20 th 2014	In process
2-What steps did you follow to get ISO 27k accreditation?		Developing information security system (ISMS) in four continuous stages: <ul style="list-style-type: none"> • Plan • Do • Check • Act 	Complete execution plan has been prepared, starting with a gap analysis, then fulfilling whatever gaps are found, then recheck (redo gap analysis) then plan & do an internal audit and, finally, continually improve the maturity of the system
3-How did you choose your ISO 27k team members?	Education degree	<ul style="list-style-type: none"> • Bachelor degree • Master degree • PhD degree 	<ul style="list-style-type: none"> • Bachelor degree • Master degree
	Important skills in those to be involved in the audit	No answer	No answer
	Position held	<ul style="list-style-type: none"> • IT Administration • IT Support Staff • Management • Academics 	<ul style="list-style-type: none"> • IT Administration • IT Support Staff • Management
4-Did representatives of all types of user play a part in your ISO 27k team?		Yes	No
5-Were there any academic users in the ISO 27k team?		Yes	No
6-Were there any IT users in the ISO 27k team?		Yes	Yes (male only)
7-Were there any student users in the ISO 27k team?		No	No
8-What proportion of all types of user participant were there in the ISO 27k team?		70% administrators and staff 30% academic	100% male IT staff participate in the team
9-What proportion of female participants were there in the ISO 27k team?		Indirect participation of IT female staff as part of the awareness program	0%
10-Do you believe that the users chosen for the team were appropriate, if not why not?		yes, the team members were chosen and arranged scheduled meetings before starting getting ISO27k accreditation	Yes
11-Are all types of users, employees and students aware that there has been ISO accreditation? If so, how many of them have any idea what ISO accreditation is?		Yes, 14000 of employees including academics and staffs have been informed just after getting ISO27K	No
12- Are most of the organisation, including all types of users, employees and students, more aware of the importance of the IT security after getting the ISO 27k accreditation?		Yes, especially after inauguration of the information security awareness programme through different communication channels	Yes
13-How does your organisation ensure information security awareness among employees?		Inauguration of the information security awareness programme through different communication channels and this programme is continued during the year	As per the security incident number and compliance level among users.

Table 6.4 shows ImamU achieved ISO 27k accreditation in Nov 20th 2014. ImamU website (2015) states the process of getting the ISO 27001 is as follows:

“Steps for developing an information security system based on the ISO 27001 certificate:

- Form an Information Security Commission.
- Choose the scope of work and objectives.
- Draft a security policy.
- Develop a risk assessment approach.
- Deal with the risks.
- Implement a security controls plan.
- Promote security awareness
- Control procedures and continuous improvement of information security system.
- Maintain the information security system and implement of the proposed development.
- Carry out an internal security audit.”

ImamU involved almost all employees (70% administrators and 30% academics) in the process of getting the ISO 27k either directly or indirectly (by involving IT females) except students of both genders.

PNU is in the process of getting the ISO 27K. According to the PNU Manager of Information Security, Sami Alanzi, “a complete execution plan has been prepared, starting with a gap analysis, then fulfilling whatever gaps are found, then rechecking (redoing the gap analysis) then planning & carrying out an internal audit and, finally, continually improving the system maturity”. Male employees represent only 10% of the population at PNU. About 90% of the male employees are IT administrators and IT staff and the other 10% are academic. PNU is an all-female University and has only female students. 90% of PNU population, including academic staff and students, is female. Table 6.4 shows that none of the female users including management, academic, staff and student, are contributing in the ISO 27K accreditation team at PNU. The responses to interview questions Q5, Q7 and Q9 indicate that there are no academic users, no student users and no female users in the ISO27K team.

6.8 Recommendations:

One of the problems that most organisations in Saudi Arabia face now is the lack of communication between male and female employees. There are many issues related to the management hierarchal structures in which management dictate what their subordinates must do at all times. As discussed in section 3.4, men do not like to listen to women and expect women to do as they say. A specific problem for PNU is that, although the majority of the population is female at PNU, the PNU IT management is seeking ISO27K accreditation with no involvement of females (See Table 6.4). Many female employees are not sufficiently trained or educated to contribute in the IT security solutions. Training, education, awareness and lack of a good communication between the males and females in the work environment could be one of reasons for the lack of female involvement in IT security solutions. The next section gives a recommendation for the solution of this problem.

6.8.1 Communication solution

An illustration of the communication problem at PNU and the proposed solution is given in Figure 6.4, which consists of two parts. Part 1, the lower part of the figure, shows the existing situation at PNU where the communication gap between the female users of the systems and the male IT staff running the IT systems is as a result of the culture in Saudi Arabia. To bridge that gap there is only the flimsy hanging bridge of phone and email communication. Communication via this flimsy bridge is hampered by the trolls of ignorance, ineptitude and bad attitude. These trolls attack any attempt to communicate across the bridge and, in particular, make any communication from the female users to the male IT management almost impossible.

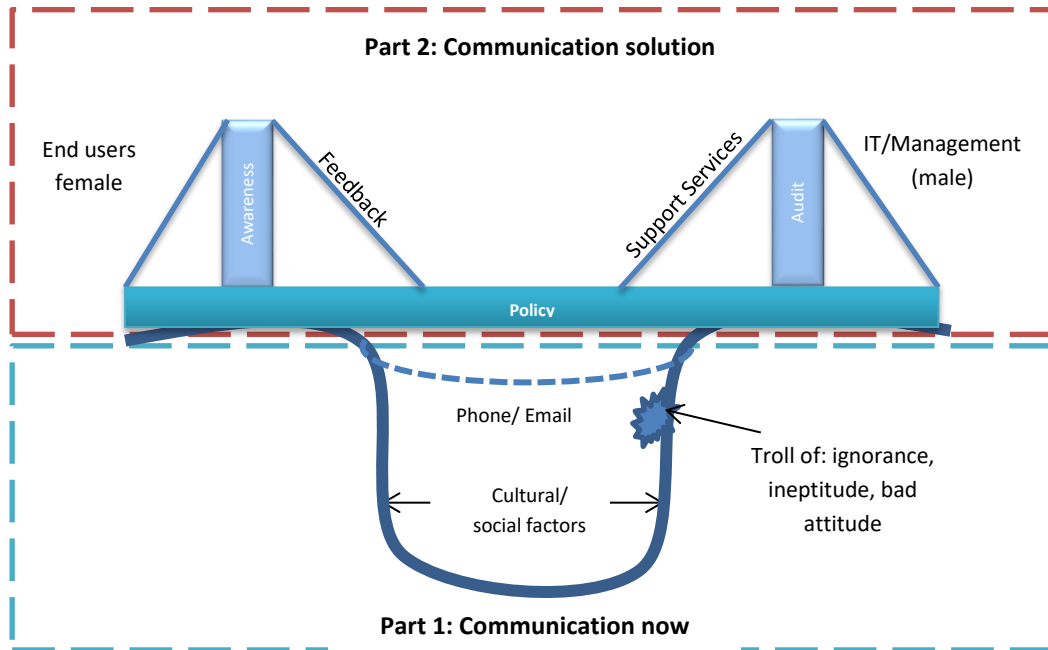


Figure 6.4: PNU Communication Structure

Part 2, in the upper part of the diagram, shows the recommended solution for the communication problem. Here the flimsy bridge is replaced by the much stronger bridge made of a clear and proscriptive communication policy. The clarity of the policy with unambiguous rules to follow keeps the trolls at bay. Helping to support this policy are two towers with cables to hold up the bridge. At the users' end of the bridge is the tower of awareness ensuring that users understand what the problems are, who to contact about the problems and how to do so. The cables from this tower are the feedback which the users supply to ensure that the communication remains supported. At the IT Management end of the bridge is the Tower of Audit which regularly checks the communication services and systems. This tower then supports the communication bridge with the cables of support services provided by the IT staff.

To summarise the recommendation, therefore, the aim is to create a clear and strictly followed policy on what communication should take place (and taken notice of), who to communicate with if there is a problem and how to communicate.

To do this the following needs to be implemented:

- Step 1: regularly carry out audits of the communication system, including gathering feedback from the users.
- Step 2: based on the result of step 1, implement a policy which clearly identifies the “what”, “who” and “how” the communication should operate.
- Step 3: develop an awareness programme for this policy so that all users and IT staff are aware of the policy.
- Step 4: Enabled by the audits of Step 1, the policy of Step 2 and the awareness of Step 3, users should give feedback communication, possibly using application software such as email and other mobile communication apps like WhatsApp, and IT staff should provide support services to act on the feedback received, and ensure the policy and IT systems work effectively and are updated and maintained as required.

6.8.2 Feedback awareness

Not submitting any feedback to the people in charge of providing services could lead them to mistakenly assume that there is no problem with services. Hooper (2011) expresses the importance of feedback as,

“Feedback is a powerful source of information for both experienced leaders and those who are young in their careers. Awareness of how you affect others should be of great interest whatever your level of experience. Yet many leaders fail to wilfully seek feedback, and some even cringe when they are receiving it.”

Therefore, service feedback is one way to communicate with people in charge to let them know how well or badly their service performs. Not submitting any feedback to the service provider gives the impression that the system has no problem. For this reason, the requirement to give feedback is an essential part of the recommendations made.

6.9 Conclusion

There is a gender communication culture issue at intensive knowledge organisations in the Saudi Arabian work environment that has an effect on the organisations’ mission and

information security. Moreover, organisations in Saudi Arabia have both a business and gender hierarchy structure environment. The gender hierarchal structure is strong enough that the women only follow the orders from men. IT male employees expect the women employees to do as they say. Women are not used to reporting any problem related to computers and some of them may assume that any problems they encounter are just a result of their lack of knowledge of the system. Management seems to not accept criticism and rarely admit that anything is wrong with the system they manage. There is also a serious issue related to the level of information security training, education and awareness among most employees.

The following chapter takes all the finding and recommendations from this chapter and previous chapters, 3, 5 and 6 and uses them in the formulation of an information security policy framework.

Chapter 7: Formulation of a culturally aware information security policy framework

This chapter focuses on the formulation of an information security policy framework and associated workflow so that the users of Higher Education oriented information systems can use it to implement their own security policy based on that framework. Developing an information security policy is not a simple task and must be conducted with due care. The need to involve employees to help in implementing and writing this policy is imperative, as described in the literature review subsections 2.5.3 and 2.5.4.

The information security policy framework is developed based on the objectives from section 1.2, the literature review, the culturally unique issues identified within chapter 3, and the collected data from chapters 5 and 6.

7.1 The development of an information security policy framework

An information security policy framework is represented by a document that provides a clear definition of all the needed policies, standards, guidelines, procedures, rules and responsibilities issued by an organisation to help reach information security goals (Hostland, et al., 2010). It should be implemented for the purpose of satisfying organisational legal and regulatory requirements.

Research in this area is discussed in section 2.5 and existing international standards, such as ISO/IEC 27001 and BS ISO/IEC 27002 (ISO/IEC 27001 and BS ISO/IEC 27002, 2005), indicate that an information security policy should embody elements adopted from current best practice such as:

- 1- A clear definition of the information security scope, objectives and the need for information security.
- 2- Management support and endorsement.
- 3- Information security implementation requirements including:

- a. Audit assessment
- b. Risk assessment
- c. Education, training and awareness
- d. Compliance
- e. Business continuity management
- f. Action required following the violation of information security

4- Responsibilities specification.

The benefits of the implementation of the information security policy framework in an organisation are to:

- Help the organisation's employees understand the importance of the information they are handling.
- Clarify to all an organisation's employees the danger of misusing this information.

This helps ensure that everyone in the organisation is aligned with the necessity and urgency of a security policy and will encourage the organisation's employees to contribute to the formation of a security policy that will be accepted across the organisation.

Figures 7.1, 7.2 and 7.3 outline the implementation of the phases of the information security framework, developed during the research.

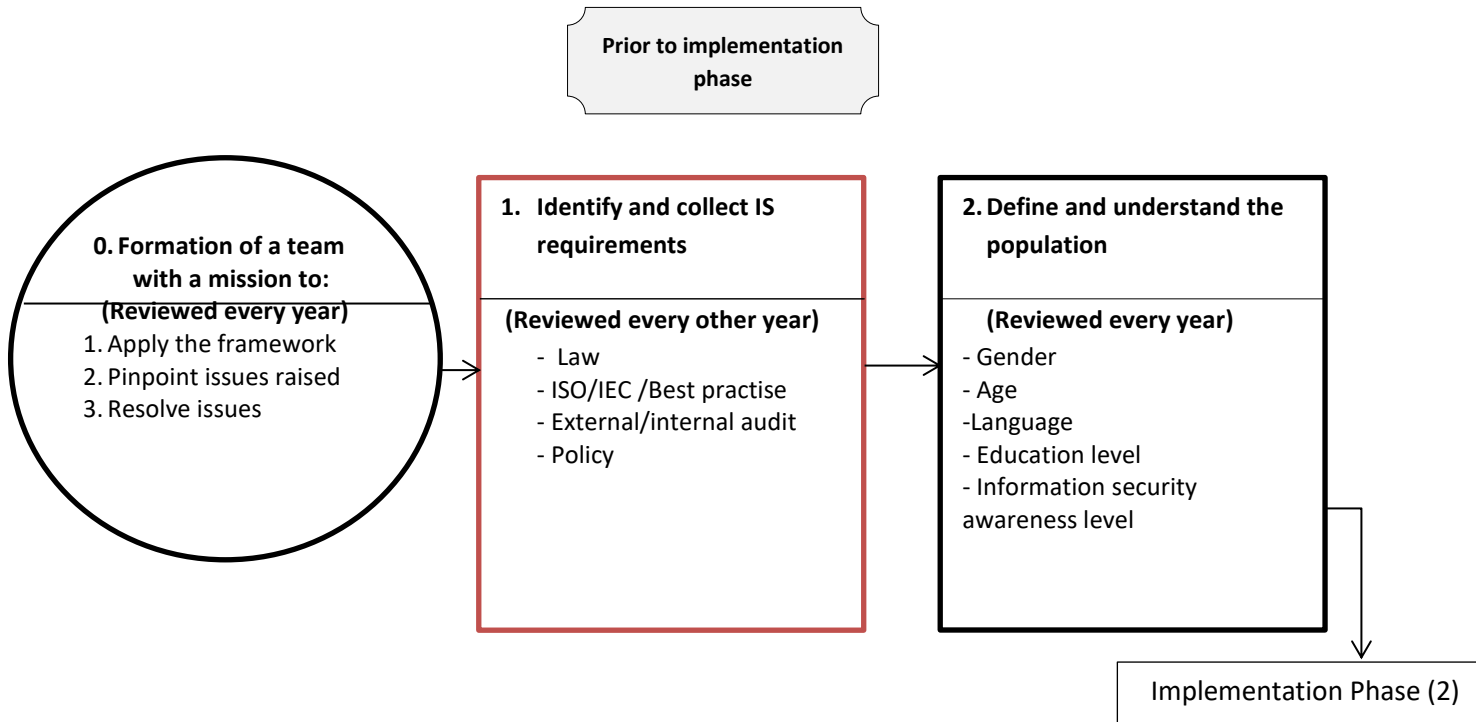


Figure 7.1: Phase 1: Prior-to-implementation phase of the Information security framework



Figure 7.2: Phase 2: Implementation phase of the Information security framework

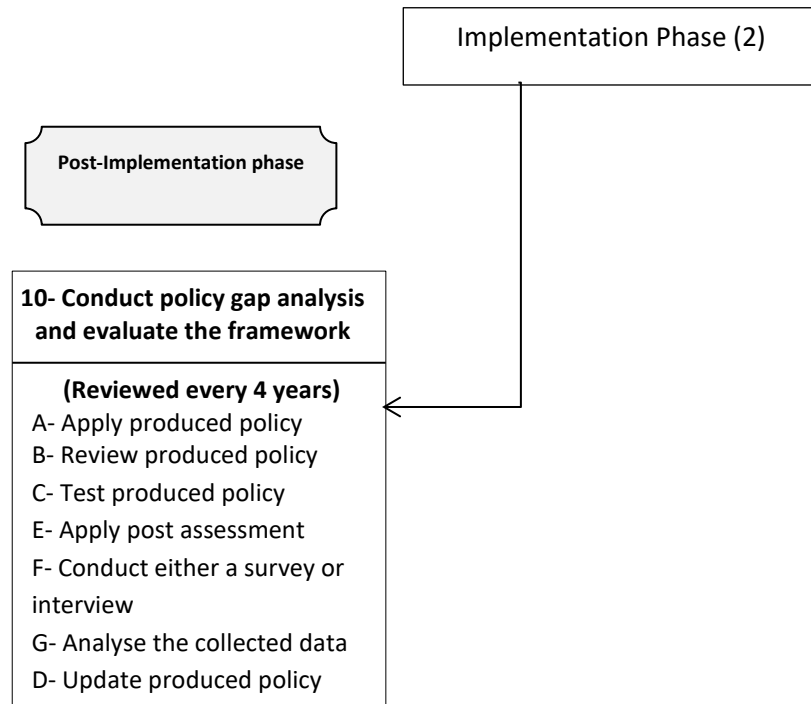


Figure 7.3: Phase 3: Post implementation phase of the Information security framework

In figures 7.1, 7.2 and 7.3 there are three phases to the implementation and evaluation of the framework:

- 1- Prior-to-implementation
- 2- Implementation
- 3- Post-implementation

The steps in Figures 7.1, 7.2 and 7.3 are collected from best practice in implementing information security plans and frameworks, see section 2.5 (ISO/IEC 27001 and BS ISO/IEC 27002, 2005; Oxford University IS Policy, 2012; Hostland et al., 2010; Burney, 2003; Pelnekar, 2011). These steps indicate processes that are generically appropriate for many organisations worldwide. However, in the case of Saudi Arabian organisations and PNU specifically, some of these steps need modification to fit their unique cultural issues. Moreover, the

researcher chose to orient the research towards ISO/IEC 27000 (ISO/IEC 27k), the International Information Security Standards framework, because Saudi Arabian organisations and universities are encouraged by the government and the Ministry of Education to get ISO/IEC 27k accreditation to improve their overall level of education accreditation locally and internationally (SASO, 2015). The ISO/IEC 27k international standard includes ISO/IEC 27001 the Information Security management standard and BS ISO/IEC 27002 the code of practice for Information Security management. As a basic rule, the researcher understands that most elements in Saudi Arabia culture are unchangeable, regardless of how poorly aligned some may be with western management practice. Thus the researcher focuses in adjusting the international best practices standards to fit these cultures, and to support users in working around issues caused by cultural difference. Investigation of ISO/IEC 27k indicates it is not wholly applicable to the Saudi Arabian work environment culture. In response to this, an entirely new additional step has been added to the ISO/IEC framework to further support its applicability in segregated work environments.

In figure 7.1 step zero is in bold to identify it as the starting point for the accreditation process and an entirely new step (step 1) is highlighted in red. Crucially, some of the steps are not in the same order as in ISO/IEC 27k. The researcher has modified the order of some of the steps and added more sub steps to fit the culture and environment in the universities in Saudi Arabia. For example, in ISO/IEC 27k step 3, definition of roles and responsibilities is after step 4, definition of system information procedures and standards. The researcher believes that because of Saudi Arabia's unique culture and environment, the roles and responsibilities should be defined first. Female employees are used to following orders of what to do and understanding their roles due to (section 3.4):

- The hierarchy work environment.
- Gender hierarchy. The male gender dominates the female gender in Saudi Arabian culture. Women do what men say.

The earlier identification of roles and responsibilities assigned to females should enable and encourage them to have their say on how information procedures and standards are defined.

Each step of the framework should be reviewed periodically. Steps 0, 1 and 2 should be reviewed every other year as they make an important contribution in raising the level of awareness among end users. The rest of the steps should be reviewed every time the organisation information security management is changed, which should be every four years. The steps of the framework are described in the next sections:

7.2 First phase: Prior-to-implementation

This is the phase in which the identification and collection of the information security sources required in the implementation of information security policy occurs and the organisation population is defined. It has three steps, step 0, step 1 and step 2.

7.2.1 Step 0: Formation of an information security team

In order to apply the steps in the culturally aware information security policy framework, a team needs to be formed consisting of a leader, a secretary and users of the system (Between 4-6). According to Wageman (2007), keeping the team small can help the team members connect and work better together. The leader is given the role of information security assistant, acting as a connection between the system end users and the information system administration. Each year, a new team will be formed and the leader will be picked from one of the members in the previous team. This will help involve most of the end users in the policy development and will help raise the information security awareness level among end user employees. The team's responsibilities are:

- The leader must:
 - Have a fixed place for the meeting known to the team members and all the end users in the department.
 - Have a timetable set in advance for all the meetings
 - Follow the framework steps and clarify each step to the team members
 - Involve the team members in the application and modification of the step when necessary.

- Identify the issues raised when applying each step with the help of the team members
 - Find solutions to these issues with the team members' help
 - Make sure that complaints raised by the all types of employee are resolved formally
 - Classify information and risk, based on the collected information
 - Develop an information security policy and deliver it to the Head of the Information Technology Department
 - Give an annual information security awareness seminar to all type of information system users and additional seminars if needed
- The team members must:
 - Help in the application of the framework steps
 - Pinpoint issues raised during the application of each step
 - Be involved in finding a proper solution for issues raised in each step
 - Get involved in modifying the steps, if necessary
 - Help in classifying information and risk
 - The Secretary must:
 - Document each meeting
 - Distribute any developed policy, forms and table to employees (and other users, such as students in the case of a University system) either by email or as a hard copy
 - Collect and document tables, forms and issues related to information security and deliver it to the group leader to classify threat, risk and information.

7.2.2 Step 1: Identification and collection of information security requirements

The initial step, or step 1, is to identify and collect the information security sources that are required in the implementation of information security policy. According to the

international standard, BS ISO/IEC 27002:2005, organisations must identify their information security requirements prior to the implementation of information security policy. In this study, the main sources of requirements to establish information security policy are best practices and standards, laws, auditing, information risk, unique culture problems and policy. They are presented in figure 7.4.

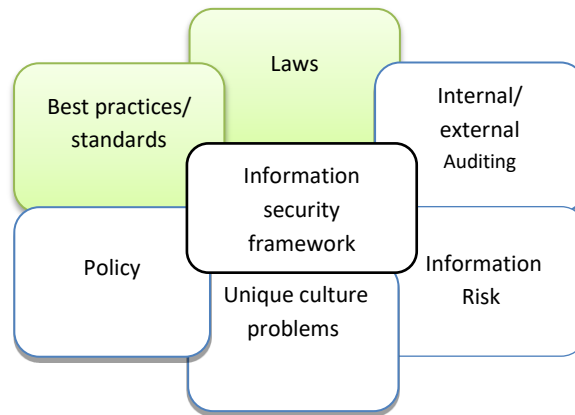


Figure 7.4: Elements required for an information security policy framework

Figure 7.4, developed by the author, identifies two types of requirements for information security policy, external requirements which cover ISO/IEC, and best practices and law (indicated in green as they already exist). Other external requirements include identified cultural problems, regulation and external auditing. Internal requirements cover an organisation objectives and mission, internal auditing of IT, IT risk assessment and identified IT system culture problems. These requirements will be explained in the subsections, 7.2.1.1 to 7.2.1.5.

7.2.2.1 ISO / Best practice

ISO/IEC 27k (the International Organisation for Standardisation/ the International Electrotechnical Commission):

Definition: ISO is an international organisation for standardisation that is recognised worldwide as a source of generic best practice for defining formal specification and advisory documentation for information security controls (ISO website 2013a). Saudi Arabia is an

ISO/IEC O-member in IT security. An O-member means that the member acts as an observer and follows the work given by ISO but cannot participate and contribute in the development process of an ISO technical committees (TC) (ISO website, 2013b).

Why this step is needed: Most Saudi Arabian organisations are working to get ISO/IEC 27k accreditation, as they are being strongly encouraged to by their government. However, Saudi Arabia has a different culture, segregated work environments, low levels of IT awareness among employees and poor communication channels, so being an O-member may lead to a mismatch between what Saudi Arabia needs and what it gets as an observer of the ISO/IEC. To contribute to the aims of this research, it is desirable to develop and assist in the implementation of a policy that fits Saudi Arabian needs by incorporating parts of best practise where possible, such as that given by ISO/IEC, into the developed information security framework. Some aspects of best practice are appropriate to incorporate into the framework without modification, but other parts will need to be modified to comply with the cultural requirements of the Saudi environment.

Example: One of PNU's objectives is to apply instructions and regulations that guarantee work flow according to international standards such as ISO/IEC 27001 and BS ISO/IEC 27002 (PNU website, 2013). At the time of writing this thesis, PNU is starting to work for the ISO/IEC 27K certificate in IT. A team of PNU employees and employees from Wipro, the IT outsource company, are working together for this purpose.

Table 7.1 shows how PNU IT is executing elements of ISO/IEC 27K:

Table 7.1: PNU execution of ISO/IEC 27K elements

ISO/IEC 27K elements	Saudi Arabia PNU	
	Process/ Documentation exists	Proper execution
1- Scope, objective and definition of information security	√	
2- Management commitment of information security	√	√
3- Approval of information security policy	√	√
4- Legal, regulation and contractual compliance		
5- User awareness training and education	√	
6- Business continuity planning	√	
7- Risk management	√	
8- Incident handling	√	
9- Information classification	√	
10- Access control		
- Physical access	√	
- password	√	
11- Roles and responsibilities	√	
12- Violation of information security policy and disciplinary action		
13- Review and evaluation of information security policy		
14- Style, format and review date of the information security policy document		
15- Distribution of the information security policy document to all type of employees including students		

Based on the research results collected from chapter 5's surveys and chapter 6's interviews and observation, Table 7.1 shows that some of the ISO27K elements are not being covered by PNU, although some of them are required and suitable for the PNU information security system for example:

- Element 1, According to the PNU website (2013), the Directorate General of Information & Communication Technology department objectives are "to support a culture of using information technology among the employees of the University by

providing high-tech and sophisticated equipment and instruments, and implementing suitable information and programming systems to provide an integrated quality of information technology and communication services.”

- Element 2: PNU management is open and committed to the idea of having a secure information system.
- Element 3: The senior management has approved information security policy
- Element 4: There is no legal, regulation and contractual compliance required (section 6.4.2 Q4,5)
- Element 5: According to subsections 5.3.5 and 5.4.5, on Q5 in each survey, although there are training and education courses, most of the employees have not taken any. Subsection 6.4.3, table 6.3 shows that the employees do not get an effective training programme. As a result of the culture, women lack confidence to put their views forward. It will take time to build the confidence in women so that they can contribute their views and knowledge, but training is a way to build that confidence. Training for women is, therefore, necessary for the long term productivity in Saudi Arabia.
- Element 6: For business continuity planning, there is no timescale for services or data to be restored (subsection 6.4.1, table 6.1, Q6).
- Element 7: The IT management is aware of the risk the IT system is facing (subsection 6.4.1, table 6.1, Q2), yet their risk assessment is undertaken by male employees only. The female involvement in the risk assessment is limited; in fact there is 0% female participation in the ISO27k team at PNU (section 6.7, table 6.4, Q9).
- Element 8: In handling the incident, PNU has no timescale for services or data to be restored and no documented backup policy (subsection 6.4.1, table 6.1, Q5 and Q6).
- Element 9: The classification of information is developed by IT male employees and it is not documented. Therefore, it is not known to most female employees.
- Element 10: Access controls are as follows:

- Physical access controls, as in the use of access cards for the computer labs and important offices, are available but are not active yet. However, the system does make audible beeping sounds, which may lead employees to believe it is operational.
- Passwords are not properly executed. Employees do not know the importance of passwords nor do they distinguish between their work password and their personal password. This could plausibly be exacerbated by the rapid expansion in IT in Saudi Arabia which can mean users not knowing exactly how many passwords they have (subsection 5.3.13, Q13). Also, passwords can be changed without employee's knowledge (subsection 5.3.10, Q10).
- Element 11: IT system roles and responsibilities are dominated by male employees in a work environment where the majority of the employees are female. This means that only a minority of the employees are involved in the making information security policy. In the case of PNU, males are only 10% of the employees' population (subsection 6.4.2, table 6.2, Q1 and section 6.7, table 6.4, questions 4-9).
- Element 12: There is no process for handling violations of security policy (subsection 6.4.2, Q8, Q9 and Q10).
- Element 13: PNU has not yet documented its information security policy nor reviewed and evaluated it. PNU IT management uses ISO/IEC 27k policy only (subsection 6.4.1, Q5 and subsection 6.4.2, Q6 and Q7).
- Element 14: There is no documented information security policy for PNU, only an English version of ISO/IEC 27k and the style, format and review date of information security policy of ISO/IEC 27k
- Element 15: There is no distribution of the information security policy document to all types of employees and students (subsection 6.4.2, Q7).

The above points show clear cultural problems that will be discussed in detail in the next subsections, 7.2.2.2 to 7.2.2.5.

7.2.2.2 Law and regulations

Definition: This sub step will cover all the available laws and regulations that have either a direct or indirect effect (positively or negatively) on the security of the information systems. The foundation of the law used in Saudi Arabia is the Islamic religion law and is called “Shareeah” (see section 2.4). This research focusses on how certain laws and regulation affect the development of comprehensive information security policy framework, since many countries, such as USA, do not have any single comprehensive data protection and computer misuse laws compatible with those in the UK (Sotto and Simpson, 2014). It is suggested that legislation and regulations, such as the western UK Data Protection legislation, which is not available in Saudi Arabia, should ideally be adapted and enacted as such laws are necessary for the security of information.

- Adopted and promulgated western legislation:
 - UK Data Protection Act 1998 (DPA 1998)
 - UK Computer Misuse Act 1990 (CMA 1990)
 - Human rights laws, such as ‘The Universal Declaration of Human Rights’ developed by the United Nations.
 - General Data Protection Regulation 2018 (GDPR 2018). This is a stronger form of data protection to come into force in the UK in 2018. It will be necessary for Saudi Arabia to adopt the equivalent law to keep up with advanced Western nations.

- Saudi Arabian laws:
 - Islamic law for communication issues
 - Saudi Arabia Cyber law No. M/17
 - The Ministry of Higher Education and university regulations

Why law and regulation is needed: Saudi Arabia has realised that action must be taken to protect modern day issues such as Information security, which are not covered in the Islamic law (See section 2.8). New laws and regulations have been developed, including both general laws for the country of Saudi Arabia and specific laws and regulation for each of the government ministries and universities.

7.2.2.3 Auditing

Definition: According to the literature review in section 2.4, an audit is the process of providing official assessment or examination of a person, organisation, systems, process, or product. According to Wright (2007) there are three types of auditing techniques:

- **Self-auditing:** undertaken by software applications that daily monitor and report on the security status of a system and record a security event log based on the organisation's security policy. These applications can send an alert message and lock an account, when an unauthorised security breach occurs.
- **Internal auditing:** undertaken by a team of IT internal employees to periodically audit the organisation's information systems to find out potential breaches of the system that may damage the IT system
- **External auditing:** undertaken by an external specialised company to do an overall testing of the organisation's security system and report any weakness and vulnerability of the IT system.

Best practice for the process of auditing should recognise factors such as the organisation's operation standards, regulation and policies.

Why auditing is needed: The main purpose of an internal audit of an IT system is to make sure that (ISO/IEC 27001:2005):

- All employees are sufficiently trained to perform their job according to operation standards, regulations, and policies.
- All types of computer, system configuration, and application software are handled, used, and upgraded according to operation standards, regulations, and policies.

- All services are undertaken according to operation standards, regulations, and policies.

How the audit process is handled by ISO/IEC 27K: According to ISO/IEC 27001:2005, the audit assessment team should involve all employees in an organisation. The audit process should cover three main areas in an organisation (ISO/IEC 27001:2005):

- Human resources: interviews and survey methodologies are used to check employees' compliance and job performance.
- Equipment: Hardware and software used by employees should be checked for any operational fault or recent updates.
- Services such as email should be checked by using the self-check software or any audit tools or techniques.

How audits are undertaken in Saudi Arabia: Most Saudi Arabian universities have almost equal numbers of male and female employees and students but sometimes, as in the case of PNU, there are more female employees and students since it is an all-female university. The IT audit assessment teams commonly have a male majority and a low level of contribution by female employees. The universities' male employees are the ones who implement, monitor and operate the three types of auditing techniques, self, internal and external. In the field of IT, female employees are used to accepting rules and orders, mainly from males, instead of making or contributing in making the rules themselves. Excluding female involvement can clearly lead to incorrect and incomplete audit assessments.

Audit cultural problem limitation within the Saudi society: In most Saudi Arabia universities, the engagement of the female employees in the audit process is limited, (section 6.7, table 6.4, Q9). This may lead to an incomplete audit assessment. There is no special training and educational programmes given to female employees to help integrate them into an audit team to contribute to an audit assessment.

Example: PNU have started their first internal auditing programme undertaken by male IT employees from PNU and a contract company, Wipro. The researcher took part in the first

PNU audit assessment. The researcher was the only female member in that team although PNU is an all-female university. However, according to the PNU ISO/IEC 27k IT male employees, when the researcher became a member of PNU ISO/IEC 27k the internal auditing assessment had been conducted already. The male members of the team did not accept any suggestion from the researcher and the researcher was given orders and expected to just follow them. The PNU IT ISO/IEC 27k team is planning to do an external audit in the near future and, again, no involvement of female employees is in any part of that plan (section 6.7 and table 6.4, Q9). Self-auditing at PNU is configured, monitored and operated by IT male employees and all emails and other information systems accounts' configuration are implemented by IT male employees. For example, IT male employees chose the number of times the password can be entered incorrectly for the system account to be locked. The audit assessment is, therefore, undertaken according to the male employees' point of view. This involves mostly technical auditing of hardware and software performance only, excluding human resources.

Researcher recommended solutions: This serious issue of attitudes needs to be resolved by:

- Training female employees and educating them to be qualified for the audit assessment through:
 - Auditing workshops and seminars in how to identify, classify, recognise and report threat and risk associated with their computer.
 - Distributing to all types of employee lists of unusual computer issues that needed to be recognised and must be reported.
 - Encouraging employees to record and report unusual computer issues and to use tools, such as the forms given in table 7.2, 7.3 and 7.4 for an easy reporting process.
- Integrating trained female employees in the audit team and helping them to contribute in the audit assessment.

Table 7.2: Recording information assets (adopted from Oxford University IS Policy, 2012)

Asset	Type	class	Owner	Vulnerability type	Risk rate	Frequency of occurrence	effect

Table 7.3: Listing threats (adopted from Oxford University IS Policy, 2012)

Threat	Type	rate	Frequency of occurrence	reported	fixed

Table 7.4: Threat rating (adopted from Oxford University IS Policy, 2012)

Threat rate	Frequency of occurrence
Low	Once a year or less
Medium	At least two a year
High	At least once a month

7.2.2.4 Risk assessment and treatment

Definition: Risk assessment is the process of detecting and evaluating risks that could endanger business continuity of an organisation. Risk assessment should be considered as a foundation for the audit process. The auditors should be familiar with the theory and execution of risk analysis techniques. Kapp (2000) recommends that those who audit a system should be familiar with the risk management and analysis theory (see section 2.3.1). An educational organisation, such as a university, should set criteria that determine acceptable risk levels and prioritise the resolution of those risks based on these criteria (section 2.3.2).

ISO/IEC and best practice risk assessment and treatment strategies: In order to assess risk, information security risk strategy should do the following (BS ISO/IEC 27002):

- 1- Identify the risk scope:
 - Define information assets
 - Assess and observe the threat to information assets
 - Assess and observe any threats that can exploit vulnerabilities
 - Observe and recognize the effect of any damaged information, confidentiality and integrity, and loss of availability of any IT assets
- 2- Manage risk and identify acceptable levels of risk.
- 3- Implement and approve criteria for an acceptable risk.
- 4- Analyse and evaluate risk according to the risk acceptance criteria.
- 5- Identify a risk assessment methodology that fits legal and regulatory requirements.
- 6- Choose the appropriate actions/plan to treat risks. Risk treatment can be done by (Pelnekar, 2011):
 - Applying prevention and detection controls to reduce risk
 - Accepting a risk if it satisfies the risk acceptance criteria
 - Avoiding risk by blocking the action that caused the risk occurrence
 - Transferring the risk to third parties for treatment.
- 7- Implement security control to reduce risk. Controls should reduce the risk into acceptable level and should considering the following:
 - National and international regulation and legislation
 - The objectives of the organisation
 - The constraints and the requirements of the operation

- The expenses of the risk treatment action in relation to the university's constraints.

8- Monitor and review residual (the remaining risk after treatment) risk and improve or change treatments if needed to minimise risk.

How risk assessment is undertaken in Saudi Arabia: Most Saudi Arabia academic organisations are exposed to a number of information security risks (see section 2.8.1). These risks need appropriate controls of process, people and systems to treat them (Humphreys 2010). Risk assessment is also undertaken by male IT administrators at most Saudi Arabian universities as they usually:

- Cover technical risks associated with hardware and software, even in female environments.
- Identify and classify the risk acceptable level.
- Choose the methodology for risk assessment and the appropriate risk action treatment.

Risk assessment cultural problem limitation within the Saudi society: The male employees do not take the females' views seriously as, traditionally, female employees have had a subservient role. In an environment where a large number of users are female, it is clearly important to involve female employees in the assessment of the risk. A female working environment may be exposed to a number of risks that would not be seen in a male working environment. Employees compliance to any policy related to risk assessment can be reached by involving all employees, male and female (BS ISO/IEC 27002).

It is not just a problem amongst the male employees, the female employees often fail to report any problems with IT, either because they do not feel important enough to make such a complaint or because they don't have confidence that anyone will listen to them. They need to learn that their views are important and that they, as users, have an essential quality responsibility to report issues when they arise. These types of attitude are not compatible with the IT enabled society of the 21st century and they have certainly inhibited the effective provision of an IT service and information security in Saudi Arabia.

Example: According to the data manager at PNU, Dr Ghazi, risk associated with people is not considered as a major problem. The ISO/IEC interview Q6 described in section 6.7 and the researcher observation as a member in PNU ISO/IEC 27K team showed that the male IT members of the PNU ISO27k team completed the internal auditing assessment, identifying the technical and process risks and classifying them according to perceived level of threat. There was no female involvement in the risk assessment and no female participation in the ISO27k team at PNU (Q9 section 6.7). The researcher became a member, for a limited time; just after the all-male ISO/IEC 27K team had identified and classified risks. The team believed that they had already adequately assessed the risks associated with the female employees' environment, e.g. spam emails, and they decided there was a need to focus on an awareness programme for female employees, which is again designed and picked by the male PNU ISO/IEC 27K team. Any suggestion of a modification to the awareness programme by the researcher was not accepted, and the researcher was only asked to do what the PNU IT team wanted her to do.

Researcher recommended solutions: This serious issue of attitudes needs to be resolved by:

- Engaging female employees in risk assessment and helping them to play an effective part.
- Training female employees and educating them to be qualified in risk assessment.
- Ensuring female employees can recognise threats to information security and risk and report them to the appropriate authority confidently and accurately.

To minimise these problems, the next step is a new step in the Information Security process.

7.2.2.5 Identifying culture problems

Definition: Culture is a combination of people's thinking, saying and making, their costumes, traditions, language, art, literature, common expected attitudes, feelings and values (Dadfar, 1990).

Why there is need to identify culture problems: Most Middle Eastern countries, and Saudi Arabia specifically, have a unique cultural environment that may negatively affect the work-

flow outlined (see section 3.2). The researcher has identified Saudi Arabian culture problems when interviewing employees and investigating the security information system, such as the trusting culture and gender communication issues (section 3.5). These cultural problems are explained in the following subsections.

7.2.2.5.1 Trusting culture

Definition: trust is when someone believes in the reliability and honesty of another person. An organisation trusting culture is where employees trust each other in sharing the most sensitive information. Almost all Saudi Arabian educational organisations (universities) have a security unaware “trusting” culture. Because of that, security awareness levels for most employees at Saudi Arabian educational organisations are low. The use of information technology is fairly new to them. As a result, the employees typically have little understanding of the importance and the danger of the information they are dealing with. Most of the employees still share passwords, use the internet for private purposes at work and reveal university sensitive information. They still find it difficult to recognise threats and they sometimes employ poor practices unintentionally, through a lack of security awareness.

Example: PNU, for example, is a newly expanding environment in which employees still share computers and passwords, don’t change their passwords, and leave their offices unlocked. According to the awareness survey, 58% (29 out 50) of PNU employees share their password with their co-worker or someone else (Figure 7.5). PNU’s culture can affect how the university responds to uncertainties and risks. PNU has implemented common technical security system controls such as a firewall, SSL, passwords and anti-virus programs. However, most of the university processes and services still operate by the “trusting” culture.

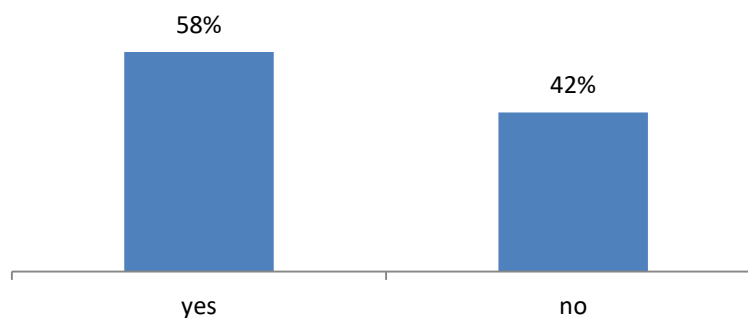


Figure 7.5: PNU employee share work password with a co-worker or someone else

Researcher recommended solution: There is a need to create and enforce an information security culture to influence and enable monitoring of the behaviour of employees by:

- Raising the level security awareness and educating the employees by providing:
 - More email security alert updates,
 - Workshops and seminars for all type of employees:

Table 7.5: workshop and seminar timing schedule

Type of end user		Workshop	Seminar
employee	new	With before/after assessment to verify the efficiency	Every time there is IT alert or update
	ongoing	Every time there is IT alert or update	Every six months
student	new	With before/after assessment to verify the efficiency	Every time there is IT alert or update
	enrolled	Every time there is IT alert or update	Every year

- Assessment and evaluation of the outcome of workshops and seminars to create an information security culture among employees.
- The use of security alerts, workshops, seminars and the survey assessment and evaluation in the spoken language of the users, avoiding jargon computer terminology so that they can be understood by all types of users.
- Integrating employees at any educational organisation in Saudi Arabia into a daily routine that ensures ethical conduct and good practice behaviour related to information security. Veiga and Eloff (2007) emphasize that it is important to cultivate the information security culture by making it part of employee everyday routine.

One of the objectives of the developed culturally aware information security framework is to involve employees in the implementation of information security policy to ensure the policy is relevant and applied appropriately within the organisation, to make policy culture and to ensure compliance with the information security requirements. In order for this cul-

ture to be a success, communication channels at all organisational levels need to be improved.

7.2.2.5.2 Gender communication

Definition: There is a challenging situation at most educational organisations in Saudi Arabia related to gender communication. Section 3.4 revealed the issue related to communication between males and females in most educational organisations in Saudi Arabia such as PNU. Males and females are segregated and are forced to work in two different work environments in the same organisation due to Islamic religious law. This weakens the communication channels between the male and female employees and may negatively affect the security of information.

Feedback between employees via channels such as voice, mail or electronic mails and face to face communication is limited. In most educational organisations in Saudi Arabia, male employees control the workflow of most female employee environments. The only way that male/female environments communicate is via voice communication, phone and mobile, mail or email. Female employees usually receive direction from male employees in how to carry out technical work. The lack of qualified female technical managers is one of the reasons that most of the technical jobs are managed by male employees (see section 3.5).

In many Saudi organisations, it takes more time than it should to finish what in the West may be considered routine jobs. Employees like to hold up jobs that can be finished in a short period of time to indicate that they are completing a complex or difficult job. It can take days to receive a response to seemingly simple requests, and sometimes there is no response at all in Saudi Arabia universities when using the mail and email communication services available at the university (Almunajjed, 2009).

Example: The researcher conducted a survey between all types of PNU email users to measure the email response rate and the result was as in table 7.6:

Table 7.6: Email response rate at PNU

		Receive any reply to emails				Total
		no	%	yes	%	
position	management	13	93%	1	7%	14
	academic	46	68%	22	22%	68
	staff	50	69%	22	21%	72
	student	48	83%	10	17%	58
Total		157		55		212

The survey showed that out of the 14 management participants, 93% commonly received no response to their emails. Only 22% of the academic participants received a response, and 69% of staff and 83% students did not receive any response to their emails.

Most employees at all levels of Saudi Arabian universities are not aware of the consequences if they fail to reply in a set time period approved by senior management. Moreover, the management neither encourages nor enforces employees to improve their response rate. There is no award or penalty for meeting and not meeting the approved reply time for mail and email.

Another communication issue is that Employees are not encouraged to report any problem with the computer system at work. These problems include (MS-ISAC, 2013):

- If a computer is slow
- If a computer displays unusual messages
- If a computer runs out of disk space
- If a computer crashes
- If a computer receives bounced back emails
- If a password doesn't work anymore

Many employees are not trained (and lack personal experience) to recognise the cause of major computer problems. There is no documented list of major computer problems dis-

played to all users to help them recognise, know and report computer problems to the authority. Applications that help employees to submit feedback are not made available to all employees.

Researcher recommended solution: The proposed information security policy framework for Saudi Arabian organisations, therefore, will need to provide a much greater emphasis on training and education so that:

- Users, especially female users, can understand and identify the problems they have with a service, such as an IT service, so that they can confidently and accurately report any problems they encounter with the service.
- Employees and users see the importance of good communication both to and from service providers in order that the service can be of an acceptable standard.
- Employees in service departments, such as the IT Service Department at PNU, can also recognise the importance of timely responses to users in order to provide an acceptable service
- Female employees can acquire the necessary technical skills to work in a service providing department, which will enable better face-to-face communication between the service provider and the female users of the service.

7.2.3 Step 2: Identification of the population of an organisation.

Definition: In this step, the population of an organisation should be defined. This means a full definition of the organisation's employees doing each job, their gender, age, language, experience and education level.

Why this additional step is needed: Because of the unique work environment and culture in Saudi Arabian organisations, such as in the audit and risk assessment female involvement limitation, for ISO/IEC 27K to be applicable, some of ISO/IEC 27K policy elements need to be modified and an additional step is needed. This entirely new additional step is the identification of the organisation's population. The overall idea of the addition of this step is

to assign the right person for the right job in the implementation of the information security policy for a unique segregated work environment. Surveys and interviews are the method used to collect information for this step. This step should be placed prior to the definition of roles and responsibilities, and should cover consideration of the following critical factors:

7.2.3.1 Gender (male/female)

Definition: The Oxford dictionary, 2015, defines gender as “the state of being male or female.” In many Arab Muslim countries the male gender dominates the female gender. Men typically do not listen to women and they expect women to do as they say (section 3.4). Although, the number of knowledge and experience of intelligent females is growing rapidly in Saudi Arabia, they are not used to the best effect.

Why this additional sub step is needed: ISO/IEC 27k was implemented for a western population that do not have the segregated work environment common amongst many Arab Muslim countries. Therefore, in the West there is no need to know the number of males and females in the organisation’s working environment. However, in the case of Saudi Arabia’s segregated organisations, the situation is different. Females’ involvement in most of the ISO/IEC 27k steps is restricted to just follow the males’ orders. According to Almunajjed, 2009, Saudi women were not engaged in decision making in universities’ policies. Most major final decisions about women’s educational work environment are made by males (Almunajjed, 2009).

Researcher recommended solution: For ISO/IEC 27k to be a success in the Arab Muslim region it is very important to recognise the population of males and females and assign responsibilities based on the proportion of the gender handling the job. If a system has almost all female employees then auditing assessment or risk assessment of a system should be conducted by female employees. Therefore, female employees should:

- Be engaged and play an effective part in the information security plan.
- Be trained and educated to be fully qualified so they can recognise threats to information security.

7.2.3.2 Age

Definition: age is a stage of a person life or the time extent of human life (Oxford dictionary, 2015).

Why this additional sub step is needed: Because ISO/IEC 27K was also implemented for a western population, in the step of assigning responsibility, age of the assigned management and its team has no effect on the team overall work since all parts of the team are chosen based on their qualifications. In Saudi Arabia, thousands of the younger generation graduate every year but are not effectively utilised (Almunajjed, 2009). Availability of jobs and restrictions on work opportunities, especially for females are the reasons that considerable resources and talented younger generation in Saudi Arabia are not effectively utilised (Almunajjed, 2009). This has led to many of the senior managers in Saudi Arabia being older, less qualified and inexperienced (section 3.7).

Researcher recommended solution: Saudi Arabian education has shifted, recently, to cover more electronics and computer education. Therefore, the younger generation are able to accept and work with new technologies. The role and responsibility should be assigned to an employee who is best able to undertake the work, even if he/she is not a manager. Responsibilities should be assigned taking into consideration the employee level of:

- Education
- Knowledge
- Experience (training)

7.2.3.3 Language

Definition: language is a way of communication, either spoken or written, between people in a country or a community (Oxford dictionary, 2015). A language barrier between two cultures such as Arabic and English can be a cause of frustration and misinformation (section 3.2).

Why this additional sub step is needed: ISO/IEC 27K is written in English because it was designed for a western population. Therefore, there is a risk that the language may not be translated accurately and this can give misinformation due to inaccurate word for word translations (see section 3.2). There is a high probability that the language used in interviews, meetings or workshops will be a mix of languages, English and Arabic.

Researcher recommended solution: The spoken language should be well known to both interviewers and interviewees. The employees should not be confused or embarrassed by the use of mixed English and Arabic language (section 3.2). This may lead to them pretending they know what they have been told in order to save face (section 3.6). Therefore when conducting a meeting, interview or survey to collect crucial and accurate data for the security of information systems, the language used should be the spoken language that each employee understands the best.

7.2.3.4 Education level

Definition: Education level is the level of knowledge, experience and training received particularly at school or university (Oxford dictionary, 2015).

Why this additional sub step is needed: The knowledge, experience and training level in Saudi Arabia is not as high as in western countries because education was introduced into Saudi Arabia a long time after western countries. The education level is not an issue in ISO/IEC 27k, since it was designed for implementation in western countries. However, the level of education, knowledge, experience and training is a real issue in Saudi Arabia. The effectiveness of training women is strongly affected by culture issues, such as women's lack of confidence to give their views, and a gender preference, choosing man over woman, which leads to women's knowledge being ignored, especially when it is contrary to the views of men. However, training does help build confidence and, although it will take a while, it should gradually increase women's confidence and the respect given to them by men so that women's views are taken more seriously. Also, because of high levels of nepotism (section 3.7) some employees may have insufficient training to undertake their jobs effectively, so training becomes a necessity in such instances.

Researcher recommended solution: there are a number of unqualified employees who may appear, on paper at least, to be fully qualified for their jobs. Therefore, it is important to:

- Train unqualified employees to raise their education level.
- Train women to give them confidence to put their knowledge and views forward
- Choose a trained person when choosing a role or responsibility as this would lead to a better information security system policy.

7.2.3.5 Information security awareness level

It is necessary to check the level of information security level among all types of employees including students through the use of the before and after assessment. This sub-step is not the same as Education Level as it is perfectly possible for an employee to have a PhD but still not have any information security awareness or an employee or a student could have had no more than school education, but have happened to be interested in information security and may even have taken online tutorials. The sub-step should be conducted by surveys, focus groups and/or interviews. The reason for doing this sub-step is:

1. To establish the information security training needs
2. To help identify the value and effectiveness of the framework itself when used with a post-evaluation step 11, evaluate the framework implementation.

The collected information from step 0, laws and regulations, and step 1, a collection of information about employees is used in the next phase, the implementation.

7.3 Second phase: Implementation

This phase consists of seven steps which are the guidelines for the implementation of the IS framework:

- Step 3: Definition of roles and responsibilities
- Step 4: Definition of system information procedures and standards

- Step 5: Classification of asset risk and threat
- Step 6: Classification of the System Information
- Step 7: Definition of the rules and access controls for handling system Information
- Step 8: Definition and selection of information security controls
- Step 9: Definition of an incident management and business continuity plan

The steps are explained in the next sub sections, 7.3.1-7.3.7.

7.3.1 Step 3: Definition of roles and responsibilities.

Definition: The management of any system information in an organisation starts with the assignment of roles and responsibilities according to the information gathered from first phase.

How roles and responsibilities are done according to ISO/IEC 27K and best practice:

According to Hostland et al. (2010) and Burney (2003), these roles should include:

a- Ownership of information policies

The person with overall responsibility for all information systems at the organisation needs to be defined. This owner must also have responsibility for the implementation of security policy for these information systems.

b- The information system designated owner:

Each information system, such as PNU's Banner administrative system, email system and online learning environment, must have a designated owner. The system owner roles are:

- To determine the required protection level for system information.
- To categorise the information of the system.
- To define procedures for the use of information in terms of copying, accessing, modifying and destroying.

- To designate the custodians of the system information.
- To designate a backup owner employee to do the owner role when needed.
- To help assess of information risk, especially in the development of information security controls.

c- Information custodians

Information custodians are the employees who operate and maintain the information systems, the information they hold, and the service they provide.

d- Information user

Users of the information systems include employees and students. The users of the systems information must:

- Know that they are responsible for the protection of the information they are handling.
- Not use the information for any purpose other than organisational purposes.
- Report any unusual situation related to information.
- Comply with laws and regulation and policies related to the security of information.

How roles and responsibilities are assigned in Saudi Arabia: After Saudi Arabian universities shifted from manual methods to handle data to computerised information systems, several departments, such as PNU's Information Systems Department, were created to deal with the technology shift. Also, roles and responsibilities have been created, most of which align to the ones defined in the ISO/IEC standard and best practices such as:

- a. The owner of information policies
- b. The information system designated owner

- c. Information custodians
- d. Information users
- e. The Information/ Chief Security Officer (CSO)

Example: Taking PNU as an example:

- The ownership of the information policies and the Head of the Information Systems department have changed in the last year from Dr Nasser Almojel to Dr Alsadhan and the Data Centre Manager is Dr Ghazi Alghamdi. All are male managers.
- Each information system has a manager. The Banner administrative system has two owners, one is male and the other is female.
- Most information custodians are male and they operate the entire university systems in the male environment. There are two types of information custodian, some operate the information systems and the others are technicians. The few female custodians of either type are basically directed by the male employees and just follow orders.
- The majority of the information users are the non IT employees and students who are all female.
- There is one information security officer, Mr Sami Alonazi.

Cultural problem limitation within the Saudi society: Nepotism and favouritism of a subordinate have a strong effect in assigning roles and responsibilities in a community dominated by males in Saudi Arabia. Although, PNU is an all-female university, most of these roles are undertaken by male managers, except a few of the information custodians with relatively nontechnical roles. The owner of information policies, the manager of the data centre, the information security officer, most information systems owners and some of the information custodians are male, despite most of the information system users being female employees and students. According to results reported in section 6.4, Q1, males represent around 10% of population compared to the female population at PNU. This means that roles and responsibilities are unbalanced between males and females.

Researcher recommended solution: the addition of step 1, defining and understanding the population, is important for the implementation of information security policy at PNU. As a result there is a need to:

- Assign female employees more roles in the information system management and operation.
- Provide a training and educational programme to raise the females' level of knowledge of information system management.

7.3.2 Step 4: Definition of system information procedures and standards

Definition: a system information procedure is a step by step set of activities or actions that have a start and an end and should be done in a certain order to perform a task correctly (Business Dictionary, 2016). An information standard is a measurable level of information quality required to achieve an objective (Oxford dictionary, 2016).

The owner of the information system with the help of the information custodians should list the procedures and standards, and the way they should be set and handled to enable a secure information system. Some of these procedures are:

7.3.2.1 Identities and accounts

Definition: identification is the process of assigning a unique identifier for each information system user or employee. An account is a way to enable an authorised user, unique identifier and password, to access the information system. Any university authorised user should have accurate identification and an individual secure account to access the university information system, network services and application. Identities and accounts of authorised users should have appropriate access privileges and policy.

How identification and accounts are created in Saudi Arabia: In Saudi Arabian universities, just as in ISO/IEC and best practice, each university workstation, excluding those in student labs, is under the authority of a user. Access control is assigned to each authorised user. An

identifying user name and an authenticating password are used to access authorised computers. The user name is usually the individuals email address. The purpose of having an ID is to know the identity of the person who is using the university system.

Each university computer should be monitored by an appropriate authority. The appropriate authority is responsible for the usage of the system. They have the power to know who is using a computer. However, there is no documented identity and access policy made available to the employees.

Culture issues in access control: Because of trusting culture, many employees tend to allow other employees to use their computers. Some employees never change their password and many employees don't change the first password assigned to them. In fact, most users think that the given user name and password is just for accessing the email sub system. Most Saudi Arabian universities and PNU users are not informed about their authorised access rights. There is no documented identity and access policy made available to the employees.

Researcher recommended solution: The appropriate authority must make the university usage rules available to all systems users and make sure that all university systems users comply with the university usage law and failure to comply is subject to disciplinary actions. All users should be informed of their authorised access policy and rights by:

- If there is already an identity and access policy, make it available to all employees either as hardcopy or softcopy.
- Develop and document the identity and access policy taking into account the users' needs and any other documentation activities, such as the writing style, the way in which it is presented and the distribution of the document (Höne and Eloff, 2002b). it should be:
 - Available to all employees
 - Be easy to use
 - Be easy to read
 - Be written in all the common languages of the user base.

- Be written in a readable text and a font size.
- Cover all the identification and access rights such as:
 - One identifier for each user
 - A unique password for each workstation computer
 - An enforced password requirement (see next subsection).
 - The sharing of workstation computers, identification or passwords being unacceptable at all levels to control the trusting culture.
 - The accessing of other employee accounts being unacceptable and grounds for disciplinary action
 - The disabling of unused accounts.
 - Be grounds for disciplinary action if users fail to comply with this policy.

In addition, all system users should be made aware of the disciplinary action for any policy misuse.

7.3.2.2 Authentication

Definition: Authentication is the process in which a system verifies an authorised user by checking his/her identity validation, (Oxford dictionary, 2016). No system, application or information system should be accessible without the user's authentication. The authentication depends in the classification and value of the information assets. It may be password approval or other access control such as a biometric sensor may be required.

Authentication in Saudi Arabia: Recently, in PNU, each authorised user has been given a unique identification and a password. A new update to the account system enforces a password change after a period of time. If the user doesn't change the password their account will be locked. As is typical in Saudi Arabia, the changes were imposed without further explanation. For example, changing the password requirement was enforced

without explaining to the user the importance of this. Therefore, many users delayed taking action until their accounts were locked and the IT system administration then had to deal with the issues of reopening their accounts.

Culture awareness issues: Because of trusting culture, many employees never change their password, furthermore, when required to do so, many employees reenter the old password. Many employees forget their password so they write it down in a piece of paper, a calendar or a sticky note next to their computer.

Researcher recommended solution: It is obvious that there is a low level of awareness of security principles and good practice amongst employees, particularly female employees. Because most female employees are not involved in the management of the security of information and just follow orders without question, they don't recognise the danger, for example, of not changing the password. A list of password requirements should be made available to all employees with explanation why it is important. Password requirements should include:

- A password must be changed upon first logon (enforced by the IT system)
- Any new password must be completely different to the old password (enforced by the IT system, as in the case of many western organisations).
- Passwords must not be written on a sticky note or stored in a cabinet near the employee computer system.
- Passwords should be changed at regular intervals (every university semester or every three months).
- Passwords must be complex and not easy to guess (see subsection 2.5.2.1).
- Account lockout should occur after a number of unsuccessful consecutive logon attempts.

7.3.2.3 Authorisation

Definition: According to the Oxford Dictionary (2016), authorisation is an official permission or approval classification to authorised users to access a system. Users of information systems are classified according to their responsibilities and duties. Accessing any information assets is controlled by the role of the users. There should be access rules to any information system. All users must use User IDs and accounts to access any authorized information. The owner of an information system is responsible for establishing and controlling access roles and building the policy of each procedure based on the level of users' awareness.

Account authorisation in Saudi Arabia: Just like the ISO/IEC 27K policy, all users must have a unique User id and account to access any authorized information. The owner of an information system is responsible for establishing and controlling access roles. However, the account user is not aware of his/her privileges and restriction in using the account.

Researcher recommendation solution: Each system user must know his/her access roles by having:

- A form for creating a new account to each user. It should include a list of end user privileges and restriction and should be completed and approved by:
 - The account user
 - The user supervisor
 - The owner of the information system
- A copy of the form should be given to the users, either via email or regular mail, and another copy stored in the administrator's user records.
- The account should be locked by the system administrator (owner) immediately when the user leaves.
- Termination of an account must occur immediately after the user leaves.

7.3.3 Step 5: Classification of asset risk and threat

Definition: A threat is an event or act which has the potential to harm an information system through unauthorised access, destruction, disclosure, modification of data, or denial of a service (see section 2.3). Risk is a situation involving exposure to danger (Oxford Dictionaries, 2013).

ISO/IEC and best practice classification of asset risk and threat: The initial approach to information security should be based on information risk assessments in order to identify and classify information asset risk. Therefore, the information system auditors need to:

- Check if there are criteria for acceptable risk and classify the risks according to this classification. Otherwise it is necessary to first create the criteria for acceptable risk.
- Choose the appropriate actions to manage risks such as (Pelnekar, 2011):
 - Applying treatment to reduce the risk
 - Accepting the risk
 - Finding work-rounds to avoid the risk
 - Transferring the risk to third parties.
- Repeat the risk assessments and classification annually or as required during a system's upgrade or maintenance.

Classification of risk and threats in Saudi Arabia: Risk assessment is carried out by teams of male employees at most Saudi Arabian universities. The teams classify each risk and choose the treatment plan for the risk. At PNU the ISO/IEC 27K team, who are male employees from the IT department and the outsource company, were the ones who classified the risks and chose the treatment plan for each risk. By doing so, they excluded the majority of information system female users, employees and students, from being part of the risk assessment.

Researcher recommended solution: System female users, employees and students need to contribute more in recognising, recording, reporting and classifying threat and risk. System authorised users need to periodically record information assets and report threats and classify the threats based on their effects and occurrence. Tables like Table 7.2, 7.3 and 7.4 should be available to system employees to help them to record their feedback (Oxford University IS Policy, 2012).

Table 7.2, 7.3 and 7.4 should be available in the language well known to all end users. The end users should not be confused or embarrassed by the use of English language. This may lead them to record inaccurate data to save face (section 3.6). Therefore, to collect crucial and accurate data for the security of information systems, the language used should be the spoken language that each employee understands the best.

7.3.4 Step 6: Classification of the System Information

Definition: All system information assets (input / output) must be classified based on their sensitivity. Information assets cover not only information (data, voice, video and paper) but also where it is stored and the system and equipment that processes them. The classification of information assets is the responsibility of information system owner.

Information classification in Saudi Arabia: In Saudi Arabian universities, the classification of their information is developed by the Information system staff, who are mainly male. The majority of the users of the system are not involved the information classification of their university. According to the result and findings collected section 6.7, the majority of PNU employees don't know if the university classifies its information. This indicates a low level of information security awareness.

Researcher recommendation solution: The information custodians and information users must be involved in the classification of information to help them recognise the important information assets. A time schedule should be set for the classification of the information and reviewed annually. A copy of information classification should be available, in its website or as a hardcopy hand-out, to all system users' members. Examples of information classification are as given in Table 7.7 (Hill, 2012):

Table 7.7: information assets classification definitions and types (adapted from Hill, 2012)

Definition	Types
<p>Public: Information that can be viewed by anyone anywhere.</p>	<ul style="list-style-type: none"> - Information on the university website - University course information - University announcements - University publications - University press releases - University Job openings
<p>Open: Information that can be accessed by all members of the university</p>	<ul style="list-style-type: none"> - University policies - University contacts such as email addresses, work phone numbers. - University news and updates.
<p>Confidential: Information that can be accessed by specific organisation members who have the appropriate authority.</p>	<ul style="list-style-type: none"> - Personal information such as: personal phone number, address and password, date of birth, national identity number - Department private information - Employee personal and contract data
<p>Strictly confidential: Information that is restricted to a small number of authorised members.</p>	<ul style="list-style-type: none"> - Student transcripts - Examination papers - Test data - Passwords - Bank details - Financial data - Medical records - Investigation and disciplinary records - University outsource contracts

7.3.5 Step 7: Definition of the rules and access controls for handling system Information

Definition: Rules are a set of principles, disciplines and regulations that control the operation of a particular activity (Oxford dictionary, 2016). Access is the ability to enter or use a system (Oxford dictionary, 2016). Access control is a set of rules and restrictions that enable a user to enter and use a system. Rules and access controls for handling system information are defined in this step in the following sub-sections.

7.3.5.1 Laws and regulations

According to ISO/IEC 27k and best practice, information assets, whether electronic or hardcopy, all university computers, such as workstations, personal computers and laptops, and electronic resources, such as networks, printers, communication facilities and remote facilities should be operated according to the university usage rules.

Saudi Arabia organisations, especially universities, are new to the electronic information assets field. The only law that has been documented and made available to the public is Saudi Arabia Cyber law No. M/17. Saudi Arabia has not yet implemented its own laws and acts related to the data protection and the use of computers.

Researcher recommended solution: Saudi organisations and universities should either develop their own law, regulation and acts related to the data protection and the use of computer or adopt relevant western law and regulation, such as the UK Data Protection legislation in the Data Act of 1998 (DPA 1998) and UK Computer Misuse Act of 1990 (CMA 1990). All computer users must then be informed and comply with these acts. All users should be provided with a simple, easy to read copy of the university rules.

7.3.5.2 Storage

Information assets, such as servers, should be kept in secure storage according to its classification and it should have the appropriate level of physical security. Storage servers for confidential information should have additional layer of file or disk encryption (BS ISO/IEC 27002, 2005).

Storing information assets in Saudi Arabian organisations: Most Saudi Arabian organisations, such as universities, have hired outsource companies to handle their information (subsection 2.8.1). According to Wipro, the PNU outsource company, information is kept at an appropriate level of physical security in the building designated the data centre. However, in the female work environment the physical security used to secure most computers and workstations is not at an appropriate level.

Example: PNU used a card access control to physically secure computer labs and management offices. However, this card access control is not active yet. In fact, it has added another issue to the work environment because of the noisy sound it produces if it is not active. Other issues are related to a large number of workstations used by some employees, which are kept open with no physical door to secure them. Many employees are complaining of the number of thefts that happen to their workstations (subsection 6.4.1, Q10).

Researcher recommended solution: Information assets are not only data and the servers that hold the information, it includes employees, employees' computers and workstations. Although according to the outsource company, the data centre is properly secure, computers and workstations need to be physically secure as well. This should be done by:

- Securing university computers by activating a security card access control or any proper physical security access controls.
- Keeping all workstations in a room with a lockable door.

7.3.5.3 Access controls

Information assets must be accessed according to its classification such that only authorised users are able to access them. Users should be requested to follow the password selection policy as described in subsection 7.3.2.2. A strict, well-defined access control policy must be used if remote access is required, and training should be given to systems administrators to minimise access to computers to give only the access that is necessary.

Controlled access to assets in Saudi Arabian organisation: Two-factor authentication (user name and password) access control is used for accessing information systems software in most Saudi Arabian organisations, except in some banks where they use three-factor authentication (user name, password and code messages). PNU used to have a different user name for each information system. However, recently PNU has unified all systems information access controls to one user name which is the employee email. The user has one password for any authorised information system and is forced to change this password at the beginning of each semester. The issue is that the users do not have any password

policy or rules for how to select a strong password so the users can re-enter the old password as a new password. Often the users share their password with other users. In fact, some employees are asked, by their manager, to leave their password on sticky notes next to their workstation so when the employee is absent any other employee can access their work.

Recommendation solution: Since most Saudi Arabian organisations are hierarchal organisations in which the employees need to be directed, information system users need to be informed:

- How to choose a password. There must be a password policy in how to choose a strong password.
- How to protect a password. Users at all level of organisation must be aware of the risk of sharing or revealing their password to other users.
- How to use a documented password policy. Password policy must be presented to all users either as a hard copy or sent via email, PNU website or any other social media.

7.3.5.4 Copying data

Information should be held electronically as there would be too much to store physically, and it would be far too costly to keep it up to date. All copies of information assets should be stored only electronically. Copying of the information assets, whether in a cloud, removable media or in hardcopy should be minimised where possible except for an official, formalised, back-up process. Employees should not take copies of the information assets with them outside the work area. Unneeded copies should be destroyed in adherence with an approved disposal policy.

Copying data rules in Saudi Arabian organisation: The information assets in most Saudi Arabian knowledge-intensive organisations are handled by an outsource company (subsection 2.8.1). The Information assets are secured electronically according to outsourced companies. However, employees can take a copy of the organisation data outside the work area. This raises many issues if employees do not know the risks and threats associated with mis-

using data by taking copies of data outside work. Typically, as in the case of PNU, there are no rules, policies or procedures for handling and distributing sensitive data and no information security policies or measures to ensure employees' compliance to any good practice in this respect.

Recommendation solution:

- There should be clear, easy to read, documented and distributed policy for handling sensitive data according to data classification as in table 7.8. The policies must be as detailed as possible to ensure all employees follow them to the letter.
- The use of removable and portable memories, such as a USB stick, should be restricted.
- Taking a copy of information assets outside the work area should not be allowed and should be subject to sanction.
- Applying sanctions to force all types of information system users to comply with the information security policies related to misuse of data, which include copying university data and taking data outside work areas in a removable memory.

7.3.5.5 Retention and disposal

According to BS ISO/IEC 27002 (2005), organisations should have a retention and disposal policy that covers the storage time period for old information and hardware, the location of storage and when and how old information and hardware should be destroyed.

Retention and disposal rules in Saudi Arabian organisation: PNU and Imam University are two of the largest universities in Saudi Arabia. They have no policy known to their employees for retention and disposal for old information and hardware (Table 6.2 Q5-7). There is also no documented policy related to the storage time period for old information and hardware, or to the secure location of storage and when and how old information and hardware should be destroyed.

Recommended solutions:

- There should be clear, easy to read, documented and distributed retention and disposal policy for old information and hardware. The policy must be as detailed as possible to ensure all employees follow them to the letter and must cover:
 - A fixed time period for disposal of old information, e.g. every year.
 - A detailed plan in how to archive the old information.
 - The way old information should be destroyed.
 - A fixed time period for disposal of old hardware. Typically, the average lifetime of electronic hardware would be between 4-6 years.
 - A proper disposal policy to ensure all information is removed from a computer, since deleting files from a computer does not destroy the information which can often be recovered. There are a number of ways that do not work to dispose of information from old hardware, such as:
 - Deleting files. This only removes part, but not all, information even if information is deleted from the 'trash' it can still be retrieved (Pesante, et al., 2012).
 - Reformatting disks (Wyman, et al., 2011). Formatting makes it hard to retrieve data but not impossible. The information can be recovered in part or in whole (Wyman, et al., 2011).
 - Encrypting disks or files. This only hides information from view and almost all encryption methods can be cracked with time and effort (Wyman, et al., 2011).
 - There are a number of better ways that could work to dispose information from old hardware as in:
 - Wiping the hard drive (overwriting) is one of the effective ways of destroying information by writing random data over the original information. This obliterates original information which, therefore,

cannot be recovered. There are a number of software tools that can be used to overwrite every bit and byte of original information (Wyman, et al., 2011).

- Physical destruction of hard disks

By using a proper disposal policy to ensure all information is removed from a computer, the computer can then be reused in two ways:

- Recycling the old hardware to have a clean environment.
- Donating the formatted old hardware to others in need, either locally or in different countries.

7.3.5.6 Exchange information and use of email

The exchange of information and use of email should be protected from unauthorised use and access. A procedure for how to handle threats associated with electronic messages should be available to all users (BS ISO/IEC 27002, 2005).

Exchange information and use of email rules in Saudi Arabian organisation: According to information system users at the two universities examined, they get only one email a year from the email system administration requesting them to report any suspicious emails. Many of the universities' email users were new users and so they did not know how to identify a suspicious email and why they would need to report it. Therefore, they do not take a suspicious email seriously, due to their limited security knowledge and low awareness level.

Recommended solution:

- The end users need to know:
 - What a suspicious email may look like
 - What it may contain
 - What is the possible damage, risk and threat associated with it

- How and why they must be reported
- The message should be distributed, not only via email, but also through the use of other social media, such as WhatsApp, and, not only once a year, but at the beginning of a semester and every time such organisations encountered a threat.
- A documented email use policy should be distributed annually via email, hard copy or social media.

Once the rules and access controls for handling information in the system are defined, the next step would be to define the full set of information security controls including technical controls, physical controls and procedural controls, as described in Step 8.

7.3.6 Step 8: Definition and selection of information security controls

In this step, information security controls are defined and selected. According to section 2.5, to accomplish an effective information security in an organisation, controls and measures such as technical measures, regulation agreement and management involvement need to be part of the implementation process. A successful information security programme is a combination of technical solutions, such as firewalls and passwords, and non-technical approaches, such as policies and human behaviour controls. This section covers three security control types, which are technical controls, physical controls and procedural controls.

7.3.6.1 Technical controls

Technical controls can be divided into two different categories: preventative controls, including passwords, cryptography, digital signatures and biometric data, and recovery controls, including antivirus programs and system integrity tools (Section 2.5.2).

Preventative controls

Preventive controls (section 2.5.2.1) are the processes that prevent errors from occurring through the use of authentication, authorisation and access control (see subsection 2.5.2.1).

- Passwords controls: See subsections 7.3.2.1 to 7.3.2.3

- Cryptography control: according to subsection 2.5.2.1, cryptography is secret writing used to secure the confidentiality of communication. The primary functions of cryptography are (Kessler, 2017):
 1. privacy, ensuring that only the intended receiver is able to read the message
 2. authentication, a process used to ensure the user's authorised identity
 3. integrity, ensuring that the original message has not been altered when received,
 4. non-repudiation, a mechanism used to ensure that the message is sent by the real sender
 5. Key exchange, the use of crypto keys between the sender and receiver.
- Firewalls: as discussed in subsection 2.5.2.1, a firewall is a device that is able to control access at the application level. It filters the traffic between an organisation - trusted networks and less trusted outside networks. Firewalls are hardware and software that protect the network from untrusted communication networks.

Detective and recovery controls (see section 2.5.2.2):

- Antivirus software is utility software made to scan and remove malicious software such as viruses, spyware and Trojan horses to protect computers. There are many types of antivirus software which are designed to scan, detect, prevent and remove all types of viruses for the purpose of protecting computers.

7.3.6.2 Physical controls

Physical controls are the protection of the organisation assets, such as hardware, software, networks and data from physical events and threats including fire, flood, natural disaster and theft. Access controls and CCTV are used as physical control protection of an organisation's assets from serious loss and damage.

- CCTV (closed-circuit television) is a private TV system that is not publicly broadcasted and is used for security purposes to prevent crime such as theft (Cambridge Advanced Learning's Dictionary, 2008).

- Fire alarm systems are a collection of devices used to alarm and warn people visually and audibly when smoke or fire are detected.
- Door access controls are physical security devices, such as card access and biometric devices, that restrict access to buildings and rooms to only the authorised people.
 - Card access involves a special plastic card, with a chip or a magnetic strip, designed to replace keys and be used to access restricted, secured doors when the card is passed over an electronic identifier device.
 - Biometric devices: biometric controls are used to verify the identity of an individual, based on physical or behavioural characteristics. The most common biometric devices are thumbprint or fingerprint readers, retinal scanners, voice scanners, and digital signatures. These devices are culturally accepted in Saudi Arabia and some of them such as thumbprint and fingerprint readers are being used in almost all Saudi Arabian universities to record employees' daily attendance.

7.3.6.3 Procedural controls

Information security procedural controls are guidelines, processes and policies that are needed to enforce information security technical and physical controls, such as:

- Distributing of documented information security policy which covers all information system elements such as data, programs, computers, networks, facilities, people, and processes. As discussed in subsection 2.5.3, the effectiveness of information security policy depends on helping the employees understand the rights and responsibilities of information resources, focusing on the safety and security of information handled in daily tasks.
- Training and education is necessary to prevent information systems from new threats. However, it is not an easy task to create a training programme (see subsection 2.6.1.1).

- Enforcement of policy is necessary when handling information assets rules, and any failure to comply should be subject to disciplinary action (subsection 2.6.1.1). All users who have access to information assets are required to comply with their country's laws and regulation and, for university students and staff, university policies and procedure related to information security. Any user who engages in unauthorised use, disclosure or destruction of information assets should be subject to disciplinary action (subsection 2.6.1.2).
- Compliance with the organisation's security policy when handling information assets should be part of any contractor's or other third party's contract if they have access to the information assets network. As discussed in subsection 2.6.1.3, a personal information security plan can be used to ensure compliance by employees.

Defining and selecting information security controls in Saudi Arabia: the three types of security controls, which are technical controls, physical controls and procedural controls, are handled differently in most knowledge-intensive organisations in Saudi Arabia (subsection 8.13). However, these controls are poorly executed. In PNU, according to subsections 5.3, 5.4, and 8.1.2.2:

- Users are forced to use passwords as a way of authentication but there is no written policy or advice on:
 - How to choose a strong password
 - When to change a password
 - How to secure access to their password

Therefore, as a result, a user will often choose an easy password, re-enter an old password or share their password with other colleagues.

- There are access card devices in all labs and important offices but they are all not active.
- Most end users cannot tell if their antivirus program is active. There is no automatic update to the user's antivirus software and most of the users' antivirus programs have expired.

- There is CCTV built in to each room of the campus building, and fire extinguishers installed, but none of them are active.
- Almost all offices, computer labs, workstations and personal belongings are not fully secured due to the lack of CCTV and the use of the “master key” that can open any locked door and that anybody can use, including students.

Researcher recommended solutions:

- Provide users with simple, easy to read Arabic copies of the organisation policies related to information security. All computer users must be informed and comply with these policies.
- Keep all workstations in a room with a door lock.
- If a knowledge-intensive organisation’s data is particularly sensitive, or there is a significant risk of access by unauthorised personnel, then a CCTV installation covering the organisation's computers should be considered. If a CCTV system is already installed, then steps should be taken to ensure it is switched on and monitored. If the CCTV covers areas which are primarily used by females then to safeguard privacy and gender sensitivities, CCTV cameras covering areas used by females should be monitored by female security staff. For example, in PNU, a CCTV system is installed but it is not switched on and working. The CCTV needs to be made fully functional. Furthermore, as most CCTV cameras will monitor computers used by the female staff and students, it is important that these cameras are monitored by suitably trained female security staff.
- As part of physical control, install a fire alarm system. If a fire alarm system is already installed, then tests should be taken to ensure it is switched on and working.
- Install physical access control devices. If physical access control devices are installed, such as PNU card access devices, then tests should be taken to ensure they are active and working.

7.3.7 Step 9: Definition of an incident management and business continuity plan

What constitutes an incident must be well-defined to help employees identify and report them. Incidents such as denial of service attacks, misuse of the information assets, virus or malware, transaction errors, legal or regulatory violations and theft of hardware, should be reported. An organization, such as PNU, must encourage all employees, staff, students and faculties to report incidents immediately by mail, email or phone to their manager or to the information security officer (BS ISO/IEC 27002, 2005). In any organisation, threats, whether they are a person, a thing, a process or technology must be reported to the appropriate authority (section 2.3). Moreover, if accidents occur internally or externally or natural disasters damage the information system, the owner of information system must make sure that the business will continue with a business continuity plan. The business continuity plan should have:

- **Complete backup and incremental backup plan**

An external copy is required for information, using mass storage media, such as servers, to prevent data loss and archive the old data that is not in use on separate, long term, mass storage media. Information needs to be safe and available all the time. Also it is necessary for information to be recovered and restored in the event of a hardware or software failure, accidental deletion, damage, or physical disaster. The backup should cover all new and old electronic stored information. All electronic information will be stored on data centre servers or on the cloud to allow backups to take place regularly. Backup and system recovery plans and processes should be in place and tested to define, for example:

- What information assets need to be backed up in the information system.
- The order the information assets should be backed up according to their importance

- The frequency and the number of information assets to be backed up, ie. which information assets need daily incremental backup and when information assets need a full backup.
 - The method and frequency of the testing of the backup
 - What, when and how backup information assets can be disposed of when they are no longer needed.
- **Off-site storage confidential data**

The organisation must make sure that copies of confidential data is secure in an off-site location in case the university encounters any natural disaster, such as fire, storm or flooding. The internet could be used as an off-site storage. Cloud computing is the use of computing resources, hardware and software, that are delivered as a service over a network especially the internet. Mirzaei (2008) defines cloud computing as a combination of computer technology and Internet cloud-based services.

- **Test of recovery processes**

The overall business continuity plan should be tested periodically to make sure the business will not stop if any accident or disaster occurs. Modification of the business continuity plan is necessary if breaches are found when the plan is tested.

Definition of an incident management and business continuity plan in Saudi Arabia:

In Saudi Arabian knowledge-intensive organizations, such as PNU and Imam University, most employees, staff, students and faculties do not immediately report incidents by mail, email or phone to their manager or to the information security officer. In fact, most of employees, staff, students and faculties cannot recognise threats whether they are a person, a thing, a process or technology. Moreover, if an accident occurs or a natural disaster damages the information systems, employees, staff, students and faculties do not play any part in the organisation's business continuity plan. There is a strong effect of Saudi Arabia culture in this step. The business continuity plan consists of:

- A complete backup and incremental plan
- Off-site storage of confidential data
- Test of recovery processes

Most of the activities of these processes are undertaken by IT staff or the outsource companies with male majority employees. Most female employees, staff, students and faculties do not play any part in most of these activities. Most employees, staff, students and faculties:

- Do not know what a complete backup and incremental plan is. The only thing they are aware of is that when sometimes some of their files are missing, they can get it back by calling for help from the IT technician staff. Sometimes they backup their own data in a portable storage device like a flash memory.
- Do not play any part in the test of recovery process. The only thing the employees, staff, students and faculties know is that the data is stored somewhere, either in their own computer or inside the organisation's buildings.

Researcher recommendation solution:

An organization must encourage all employees and system users to report incidents, either by mail, email, and phone or immediately to their manager or the information security officer (BS ISO/IEC 27002, 2005). Threats, whether they are a person, a thing, a process or technology, must be reported to the appropriate authority (section 2.3). Tables 7.5, 7.6 and 7.7 could help employees in reporting threats or incidents. Moreover, if an accident occurs or natural disasters damage the information system, the owner of information system must make sure that the business will continue with a business continuity plan. Employees and users should be involved in the activities of the organization business continuity plan.

7.4 Post implementation phase

In this phase, formation of information security policy is completed. The new produced policy is applied to check its effectiveness in raising the level of awareness among employees to obtain a secure information system.

7.4.1 Step 10: Conduct policy gap analysis and evaluation of the framework

In this step, formation of the information security policy is completed. The owner of an information system, with the rest of the team, applies the new produced policy to check its effectiveness in securing the information system, by:

1. Reviewing the produced information security policy
2. Testing the produced information security policy by
 - User post assessment survey.
 - Observation
 - Interviews
3. Updating the produced information security policy

This step would also involve doing the post implementation test to see how effective the implementation is (see Chapter 9). When coupled with the pre-evaluation results from 7.2 it will be possible to not only see how effective the implementation of the framework has been but it will also help identify any parts of the implementation that needs to improve. This will enable the organisation to continually improve their framework processes. This step should be undertaken by conducting surveys, focus groups and/or interviews.

7.5 Conclusion

This chapter describes an information security policy framework that is specially designed to fit the Middle East segregated work environment. The framework focuses in raising the level of information security awareness among employees working in an environment with a

cultural difference. Because most Saudi Arabian knowledge-intensive organisations are working to get ISO/IEC 27k accreditation, as they are being strongly encouraged to by their government, the proposed framework adapts and modifies some of ISO/IEC 27k's steps to enable it to be successfully implemented in a Saudi Arabian or similar culture. Therefore, new steps, step 0, step 1 and step 10 have been added to support employees in working around issues caused by cultural difference. In addition, the framework includes new guidance to enable the other steps of the ISO/IEC 27k to be implemented in the Saudi culture. The application and the evaluation of this framework will be covered in next chapter.

Chapter 8.0: Framework pre-implementation phase 1 and pre-assessment and information security awareness survey analysis

This chapter focuses on phase 1 of the application and evaluation of the developed culturally aware information security policy framework, the pre-implementation steps 0 to 2. The information security policy framework developed in chapter 7 is based on the objectives from chapter 2, the literature review, the culturally unique issues from chapter 3, and the collected data from chapters 5 and 6. The framework focuses on raising the level of information security awareness among employees working in an environment with cultural differences. This chapter explores in the following: the application technique used to develop the culturally aware information security policy framework, the formation of the information security framework team, the application of the framework phase 1 pre-implementation steps 0 to 2, the issues raised while applying each step and the resolution of those issues. This chapter also focuses on measuring the information security level of awareness among all types of information system users in Saudi Arabian knowledge-intensive organisations.

8.1 Application and evaluation technique

The aim of the culturally aware information security policy framework is to raise the level of information security awareness among employees by involving them in the process of information security assessment including auditing and risk assessment. The culturally aware policy framework has been designed primarily to address information security in domains which meet the following criteria:

- A gender segregated environment, typically in Saudi Arabia, where men are kept separate from women.
- A strong hierarchical management (as is nearly always the case in Saudi Arabia)
- Organisations where communication issues are endemic, particularly between the separated communities

- Where language differences exist between communities
- Where a community is likely to use jargon words and phrases that others may not understand
- Where the probability of fraud and risk associated with misuse of an information system is high.
- Where new systems have been deployed to users without providing user training
- Where a system users' population is growing rapidly.

The first information system chosen to apply and evaluate the culturally aware information security policy framework to was an email-based information system in a Saudi knowledge-intensive organisation, PNU. An email system was the first system chosen to apply and evaluate the culturally aware information security policy framework since the Saudi university had recently introduced the use of the email system, in 2013, to its employees. Moreover, email is the most frequent way to communicate in the last few years in Saudi universities and the number of email users is increasing rapidly. Initially the PNU email system was chosen as a case study because PNU is one of the largest all female universities and has a segregated working environment. Because of the segregation in PNU's working environment, multiple approaches were used to get the approval for the application and evaluation of the framework. The sending of emails to make the request to the male dominated Information Technology department, plus formal letters from the researcher advisor, phone calls, and a face to face meeting with the female email information system management, all failed. The application and evaluation ended up being rejected because the PNU email information system management have too few staff qualified to undertake the application and evaluation of the culturally aware information security policy framework task. They also had busy work schedules with some of the staff attending a workshop outside the university.

The developed framework can be applied to a system or a department in an organisation. By definition, a system is a set of elements, procedures and rules that are organised to work together for a common goal (Oxford, 2017). A department in a college can, by definition, be considered as a system since it has set of all types of employees and students that work

together using procedures and rules for a common goal. Therefore, the researcher decided to approach the Information Systems Department, an academic department at PNU, as a system to apply and evaluate the culturally aware information security policy framework. This decision was made because:

- The department has more employees to contribute in the application of the developed framework.
- The researcher already had a good relationship with most employees.
- The security awareness level of employees was known to be low.
- The employees were already aware there were communication issues.

The developed framework is divided into three phases and nine steps.

- 1- Pre-implementation, step 0, step 1 and step 2.
- 2- Implementation, steps 3, 4, 5, 6, 7, 8, 9.
- 3- Post-implementation, step 10.

The application and evaluation of phase 1 is discussed in the next sections and subsections. Phase 2 and Phase 3 are discussed in the next chapter.

8.2 The application of Phase 1 (pre-implementation)

The first Phase has three steps, step 0, step 1 and step 2 (Figure 7.1). The application and evaluation of these steps is discussed in the next subsections.

8.2.1 The formation of the information security framework team: Step 0

The formation of the information security framework team first required approval from the relevant information system administrators. The approval of the application of the developed framework within the information system department at PNU took a longer time

than expected, four weeks. The researcher asked for a supporting formal letter and encouragement from the department to the department's employees who would contribute to the trial of the developed framework by allowing them time allocated to take part, because this could help achieve team commitment. However, this support was not forthcoming. The researcher had to individually approach and gather the approval from each employee who was willing to contribute in the test of the developed framework. A number of team commitment-related issues arose as a result of this, including:

- Not all employees in the team were free at the same time.
- The only time that all employees, including students, were free was during prayer time as the time allowed for prayer usually left half an hour free from 12:00pm-12:30pm. Sunday was the only day most of the employees in the team were free and only during prayer time.
- Most of the time, a few of the employees would skip a meeting so the researcher had to repeat the missed steps which caused more lost time.

In accordance with the framework guidelines outlined in section 7.1, a team of seven members, being lecturers and a secretary from PNU's Information Systems Department, were formed. The main idea of forming this team was for the researcher to initially train a group of information system department employees who would be trainers for the team formed in the next year. The head of the team, who in the case study was the researcher, acted as the Information Security Officer Assistant. Going forward, each year a new team will be formed and its information security officer assistant chosen from one of the trainees in the previous team. The other team members should be all changed every year to give other employees and students a chance to play a part in the information security policy development. The initial team consisted of:

- The leader, the author
- Five female lecturers
- A secretary from the administration office

8.2.1.1 The team scheduled meeting

The application of the framework required regular meetings with team members. Most the initial team members were not available every time a meeting was held because of their busy time schedule. Due to the lack of time, some of the preparatory work that didn't need a face to face meeting was emailed to the members of the team. The content of the meetings is recorded in table 8.1. The researcher started each meeting explaining the purpose of the current step of the developed framework and then asked the team for their view and experiences.

Table 8.1: Meeting schedule for the framework application

Meeting day and week	time	Members attended	Topic discussed
Sunday 1	12:00-12:30 pm	6 members	Phase1, step 1 and step 2
Sunday 2	12:00-12:30 pm	5 members	step 1, step 2 and Step 3
Sunday 3	11:30-12:30 pm	5 members	Step 3 and step 4
Sunday 4	11:30-12:30 pm	5 members	Step 5

The communication structure among the selected team was shown in Figure 8.1:

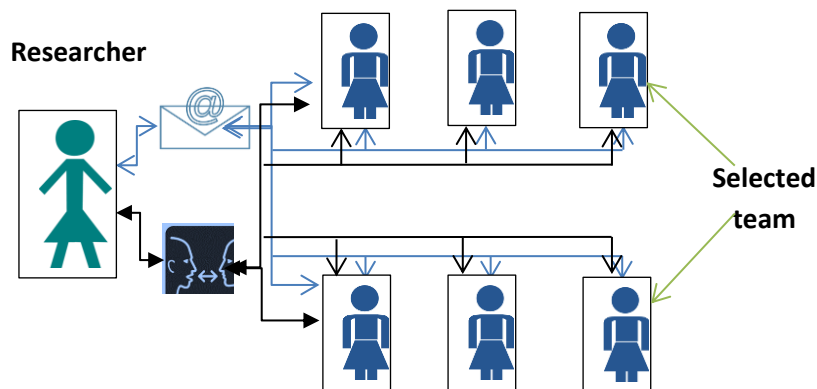


Figure 8.1: Communication structure among the selected team

Time was the main issue for the team meeting. The team members had little time when they were all free together. The only time the majority of the team members were free was half an hour on Sundays. To resolve this issue the meeting was carried out in two ways:

- Email: detailed information such as lists, tables, and figures were emailed to all team members to peruse before the face to face meeting.
- Face to face: every Sunday from 12:00 to 12:30 pm in which major topic in the developed framework was discussed and clarified.

The aim of each meeting was to clarify and discuss the application of the framework with the team members and train and prepare them to help in the application of the framework. Each step in the developed framework was discussed in at least one meeting. Sometimes a step needed more than one meeting to fully explain it and sometimes two steps were discussed in one day.

8.2.2 Identification and collection of the current information security data:

Step 1

- Step 1 (subsection 7.2.2): Identify and collect data relating to the current information security status:
 - External requirements which cover ISO and best practices and law, identified cultural problems, regulation and external auditing (subsections 7.2.2.1 to 7.2.2.4).
 - Internal requirements cover an organisation objectives and mission, internal auditing of IT, IT risk assessment and identified IT system culture problems.

In the first meeting, step 1 content was identified and discussed with the team members. In this step, rules, laws, regulations, best practices and auditing and risk assessments relating to information security were collected, whether they were local, governmental or

international. The team members did not know that there is a governmental law related to information security, the Saudi Arabia Cyber law No. M/17. They all agreed that they knew of no other law. Culture issues such as gender communication and the hierarchal structure of the management of the information System department have a strong effect on the lack of knowledge of Cyber law and that PNU is planning to achieve ISO 2700. Moreover, the Saudi Arabia Cyber law No. M/17 is only distributed as a PDF file on the Saudi Arabia Communication and Information Technology Commission CITC website. Other distribution methods such as T.V. advertising or using the social media applications, such as Twitter and WhatsApp, could raise the awareness of the law among, not only the department academics, but all Saudi Arabian information systems users. Also, they agreed that the best practice would be for all Saudi knowledge-intensive organisations to be interested in achieving the ISO 27K standard and that auditing and risk assessment should be conducted by the information technology security department.

Issues raised when forming step 1: There was a lack of knowledge of national information security laws for Saudi Arabia. Unexpectedly, no team member, other than the researcher, knew that there is a national information security Cyber law and that PNU is seeking ISO 27K accreditation. The team members blamed their lack of knowledge in this respect on:

- Their complete lack of involvement in the ISO27K accreditation process.
- The ways in which the cyber law is publicised and made available. Details of this law are available only online on the website of the Saudi Arabia Communication and Information Technology Commission (CITC).

Solution: the team agreed that due to the low level of information security awareness among Saudi Arabian cyber users generally and the negative effect on the PNU information security awareness among end users, special emphasis should be undertaken to more effectively distribute knowledge of this law to Saudi Arabia knowledge-intensive organisations by, for example:

- Advertisement signs and posters in organisations' buildings.
- The university social media applications accounts in Tweeter and WhatsApp

- A booklet attached to the new enrolled user (whether student or employee) contract.

The organisation should involve its employees in any new improvement or development of its system. In the case of PNU, all types of users should know that the university is seeking the accreditation of ISO 27K. The users should know:

- What is ISO 27K?
- What is the accreditation process?
- What must the university do to achieve accreditation?
- Who is involved in getting it?
- What is the value to the university in having it?

Another step 1 mission for the team members was to identify any IT system culture problems (see subsection 7.2.2.2).

Issues related to culture: a number of cultural issues were raised. One of the major issues raised related to IT system culture was communication between the two environments, male and female, and between the management and the colleges such as:

- The “trusting” culture in which the employees still share their password with co-workers or give their password to their managers (subsection 7.2.2.2.1).
- There is a one way communication between the male and female environments. Female system users get a command from a male in the IT department and are required to do what they are told without knowing why. According to Almunajjed (2009), communications between the male and female work environment are limited and not as frequent as they should be. The team complained that when they found problems they reported them but nothing tended to be done to resolve the problems, so they have now stopped reporting any problems (subsection 7.2.2.2.2).

- Auditing and finding fault in a system is not encouraged which caused inflexible communication between top management and colleges' departments (subsection 7.2.2.2.3). When an employee complains about a fault in a system the management ignore it. For example, department employees have only one account through which they can apply for workshop, seminar or any training programme, the Head of Department's account. A department employee must use the Head of the Department account with the Head of the Department's personal Identification number access control, revealing personal information of that person to all department employees. The account is terminated and recreated every time the Head of the Department is changed. One of the team members suggested assigning a special account for employees' applications for workshops and seminars rather than using the Head of Department's account to avoid conflict and invasion of personal privacy. The management rejected her suggestion and forced her to use the account of the Head of the Department as before.

Issues solution: A number of issues were observed during the meeting with the team members: employees still share passwords with each other, communication is limited in both the male and female working environments and reporting a fault in the information system is not encouraged nor is it taken seriously by the university Information Technology department. The team agreed suggested solutions which are:

- Prevent password sharing between employees and management formally either by sending a formal warning letter from top management to all department head managers and cc to their all employees or by verbally warning during a department meeting.
- Develop a formal information problem reporting form that must be signed by a senior manager in a college, such as the Dean of the School. This form should have the name of the employee, the type of problem faced, the frequency of occurrence and the effect and the damage of that problem.
- A follow up role assigned to one of the team member as part of her job to monitor and make sure the problem is taken seriously and fixed as fast as

possible. A problem that is not fixed should be reported back by the team leader to the Dean and the problem issue can then be reported again.

- Create an information security culture among employees (Xiao-yana, Yu-qing, and Li-lei, 2011) by:
 - Notifying all types of employee of any recent development of the university information security mission
 - Requesting employee involvement in any recent development of the university information security policies by distributing table 7.4 (listing threats) to help employees record their feedback.
 - Using email alerts when any information security risk or threat occurs or is reported
 - Using workshops and seminars presented to all types of user when any information security risk or threat occurs or is reported

The solution described would help the user understand and identify the problems they have with a service, such as an IT service, so that they can confidently and accurately report any problems they encounter with the service. This could also help in involve employees in auditing the IT system (subsections 7.2.2.2.1, 7.2.2.2)

8.2.3 The application of Phase 1: Step 2

Step 2 is to define the population of an organisation. According to subsection 7.2.3 the main idea of defining the population is to assign the right person for the right job in the implementation of the information security policy for a unique segregated work environment. This step should cover consideration of critical factors such as the employees' gender, age, language preferred, the level of education and the measurement of the awareness level.

Issues raised when forming step2:

1- Gender inequality (subsection 7.2.3.1): In the case of Saudi Arabia's segregated organisations, females' involvement in most of the ISO 27k steps is generally restricted to

just following male orders. According to Almunajjed (2009), Saudi women are not engaged in decision making regarding an organisations' policies. Most major final decisions about women's educational work environment have been made by males (Almunajjed, 2009). This is true at PNU even though the entire Information System academic department's employees, faculties and students are female.

2- Age (subsection 7.2.3.2): Although, most of the Information Systems department employees are young (between the ages of 25-40), the first female Vice Education Minister for girls' education was Ms Nora Alfayes (50+ years old), who was appointed in 2009, and the first Director General of girls' higher education was Dr Jawhara Al Saud (50+ years old). Moreover, most major administration jobs in the Ministry of Education are held by older men (Almunajjed, 2009). The younger generation need to be recognised, encouraged and involved in the major decision making at PNU (subsection 2.8.2).

3- Education (subsection 7.2.3.3): Recently, most university organisations in Saudi Arabia have a new educational policy (Almunajjed, 2009) that requires newly enrolled employees to continue their education abroad in well-known, western universities to improve their level of education. Therefore, most of the younger generation in Saudi Arabian universities are well educated (most get their higher education from well-known western universities) but these younger, better educated staff members are not involved in universities' major decision-making policies.

The information system team members agreed that the Information Systems department involvement in securing the information systems and the ISO 27K is limited. In fact, they didn't know that the university was seeking ISO 27K accreditation. The only thing they noticed was that they were requested by the IT male management to report spam emails. They also noticed that at the beginning of the year they had quite a large number of spam emails, which had decreased by the end of this year after the Information System department employees did what they were told to do, without knowing the reason behind the request. Limiting female involvement in information security is one of the major reasons the level of information security awareness is low among female employees.

Solution: The team agreed that there were qualified employees in the Information Systems department that could contribute in the information security and the ISO 27K. The contribution of the Information System department employees would raise the level awareness if they are trained to do the following:

- Contribute in auditing the information system to make sure that:
 - All types of computer, system configuration, and application software are handled, used, and upgraded according to operation standards, regulations, and policies.
 - All services are undertaken according to operation standards, regulations, and policies
- Recognise and record information system threats
- Classify threats according to the risk associated with it
- Recognise, classify, assess and report risk
- Help in developing information security policy

In all meetings, workshops, seminars and training, the language used must be the language that all the participants know best. Some terminologies and applications are used today are new and have not yet been translated in to Arabic language such as, WhatsApp, Facebook and Twitter, therefore they must be followed by a further explanation to clarify their meaning to all the participants to avoid confusion, embarrassment and misunderstanding and to save face (see subsection 7.2.3.3).

8.2.3.1 The application of Sub Step 2: Measure IT security awareness level

The measurement of IT security awareness level is used to identify the factors that have a negative effect in the level of the information security awareness. This step measures the information security level of awareness before the application of the culturally aware information security policy framework. The methodology used to evaluate framework

effectiveness is a quasi-experimental method (Mark and Cook, 1984). This method compares the outcomes of a group of participants before and after being involved in a target programme and measures the knowledge gained (Shadish et al., 2002; Mark and Cook, 1984). Therefore, before and after assessment of a population is used to measure the effect of the developed framework in raising the level of awareness among employees. Initially, a survey was carried out to determine the level of information security awareness among employees before the application of the framework.

Before the distribution of the questionnaire, an Arabic version of the questionnaire was submitted to both the PNU and Imam University Department of Scientific Research for approval. Then, a formal letter was given to the researcher, which stated the importance of participating in these surveys and specified to whom they should be distributed. The distribution of the questionnaire at PNU were handed in randomly by the researcher to the deans' secretary of four colleges, Medical, Computer Science, Pharmacologic and Art, and collected back from them after one week. Each college was given the formal letter and 25 copies of the questionnaire, a total of 200 copies, and only 50 were collected. . The questionnaire was handed out randomly by the researcher to all types of users at PNU and also sent via email to the department of research at Imam University to distribute randomly to their end users. After 3 weeks, the researcher only collected 25 copies. Both PNU and Imam University type of distribution method may lead to bias result and affect the respondents' answers, if the management collected them back.

According to the survey results (Table 8.2 Q1), Users for both Imam University (survey score 69.0) and PNU (survey score 71.5) were aware of threats and knew they should follow good security principles, controls, standards and policies, but they need training on organizational security standards and policies. They may also not know how to identify or report a security event. (See subsection 8.2.3.2.)

A multiple choice questionnaire with 24 questions was distributed to PNU and Imam University. The pre-assessment survey was distributed to 25 Imam University users of all types and 50 of all types of PNU users (management, staff, lecturer and student), see figure 8.2.

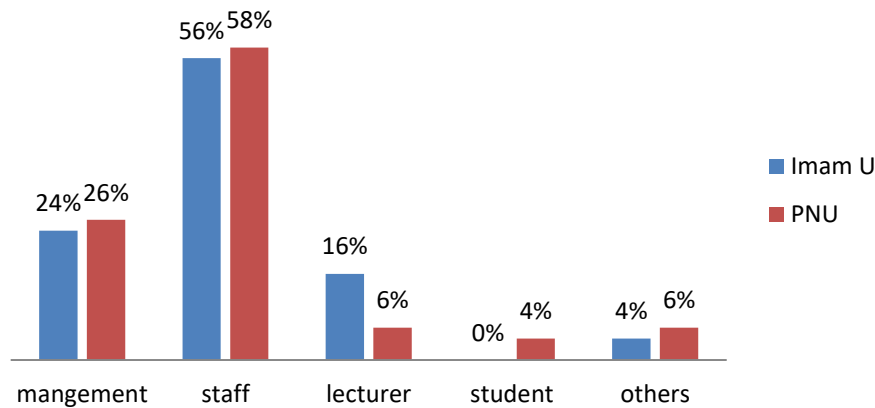


Figure 8.2: Position within the university

Figure 8.2 shows that the majority of the participants for both Imam U and PNU are staff and management and there is a lack of Imam U students' responses. The reason for the lack of the students' participants could be the time of the distribution of the survey as it was during the exam period.

The post assessment survey was applied at the end of the application of the developed framework. The results of the two assessments are compared to evaluate the effectiveness of the developed framework.

8.2.3.2 Pre-assessment awareness survey analysis

Prior to the application of the developed framework, the information security awareness survey was submitted to two knowledge-intensive organisations, Imam University which already has the ISO27K accreditation, and PNU to measure their level of security awareness. The survey assessment was used to determine whether the level of information security awareness is low, with or without the ISO 27K accreditation, and also if work environment culture issues, particularly the limited involvement of most employees in the information security assessment, affected the information security awareness of employees, particularly females.

The collected data from the pre-assessment survey is analysed in two ways in subsections 8.2.3.2.1 and 8.2.3.2.2:

8.2.3.2.1 The survey prior analysis first method

The method used to analyse the data was adopted from Bond (2013). A survey was distributed to all types of users and the responses were used as an indicator of the level of the overall participants' information security awareness levels. For each question, multiple choice responses in the survey were given a number from (1-5) according to the question's answer in a Likert Scale approach (Bond, 2013). The collected results indicate the overall classification of risk level of the surveyed university. The question responses in this survey (except for the first question) were each assigned a risk value where the highest risk (5) indicates weak awareness, negligent behaviour, or high risk activities, and the lowest risk (1) indicates strong awareness and good security practices (Bond, 2012). The collected survey results can be used to determine the overall risk score or risk level of the organization by:

- a. For each question, the risk value was multiplied for each question by the number of times it was chosen by the survey participant.

Each question total response = The participant response of each question * The response assigned risk value

- b. The average of the response totals for all survey response totals was calculated by dividing the survey cumulative response total by the number of survey participants to calculate the participants overall risk level.

The participants overall risk level = The cumulative total response / The number of survey participants

- c. Table 8.1 was used to check the Risk Levels of the participants.

For example: the assigned risk value for question 2 is:

2. How secure do you feel your computer is?

- a. Very secure (3)
- b. Secure (1)
- c. Not secure (5)
- d. I do not know how secure it is (4)

Risk value	Number of responses	Risk value *number of responses
risk value (1)	8	8*1=8
risk value (3)	1	1*3=3
risk value (4)	9	9*4=36
risk value (5)	7	7*5=35
total responses	82	

The cumulative response for all survey questions response totals is added and divided by the number of participants to find the overall risk level of the organisation participants according to table 8.2. See Appendix C.

Table 8.2: Risk Levels (adapted from Bond, 2012)

Risk level	Description
Low (25 – 39)	Users are aware of good security principles and threats, have been properly trained, and comply with all organizational security standards and policies.
Elevated (40 – 60)	Users have already been trained on organizational security standards and policies, they are aware of threats, but may not follow good security principles and controls.
Moderate (61 – 81)	Users are aware of threats and know they should follow good security principles and controls, but need training on organizational security standards and policies. They also may not know how to identify or report a security event.
Significant (82 – 96)	Users are not aware of good security principles or threats nor are they aware of or compliant with organizational security standards and policies.
High (97 – 110)	Users are not aware of threats and disregard known security standards and policies or do not comply. They engage in activities or practices that are easily attacked and exploited.

The survey result showed that Imam and PNU have almost the same risk level which, according to table 8.2, was:

Risk level	Imam	PNU
	69.0 (Moderate)	71.5 (Moderate)

The close survey result outcomes for both universities, Imam which already has ISO 27K acidification certificate and PNU which is seeking ISO 27K accreditation certificate, shows that the awareness level is still low, despite each University's involvement with the ISO standard. This is likely to be because of the limited involvement of all types of the universities' users in seeking the ISO 27K.

8.2.3.2.2 The survey prior analysis second method

An in-depth analysis was undertaken to find any relationships between the survey questionnaire's variables. The survey was organised in five sections to clarify and simplify it for the participants and to assist in drawing the associated outcome conclusions. The survey five sections are:

- Personal computer security (Table 8.3)
- University security policy (Table 8.4)
- User knowledge and security awareness (Table 8.5)
- User security practise (Table 8.6)
- User experience (Table 8.7)

Each section is analysed separately. The first section has personal computer security questions (Table8.3)

Table 8.3: Personal computer security questions

Question		Imam U	PNU
1- What is your position within the university?	Management	24%	26%
	Staff	56%	58%
	Lecturer	16%	6%
	Student	0%	4%
	others	4%	6%
2- How secure do you feel your computer is?	Very secure	4%	4%
	Secure	32%	44%
	Not secure	28%	16%
	do not know	36%	36%
3- Is the firewall on your computer enabled?	Yes	20%	18%
	No	20%	4%
	do not know	28%	44%
	do not know what a firewall is	32%	34%
4- Is anti-virus software currently installed, updated and enabled on your computer?	Yes	48%	28%
	No	20%	4%
	do not know	20%	56%
	do not know what anti-virus software is	12%	12%
5- Do you know what an email scam is and how to identify one?	Yes	8%	18%
	don't know how to identify one	68%	44%
	do not know what an email scam is	24%	38%

The data collected for section one for both universities of the survey shows that the majority of participants either thought that their personal computer is not secure or didn't even know if their computer is secure (64% for ImamU and 52% for PNU). The survey collected data also shows that the majority of participants of both universities did not know what a firewall was or, if they did, they didn't know if it was enabled or not (80% for ImamU and 82% for PNU). Similarly, the majority at both universities did not know what anti-virus software was or, if they did, they did not know if it was installed, updated and enabled on

their computer (52% for ImamU and 72% for PNU). Furthermore, at each university, only a few knew what an email scam was or how to identify one (8% for ImamU and 18% for PNU) (Table 8.3, Q2, Q3, Q4, Q5). The significant and shocking result to come from these results is the level of ignorance amongst the staff about security issues. In both universities, around two thirds to three quarters of participants revealed a dangerous lack of knowledge in most questions. It is perhaps unsurprising, therefore, that at each university only a mere 4% of staff (ie. one at ImamU and two at PNU) felt their computer was very secure.

The second section is about the university security policy. The data analysis for this section is shown in Table 8.4.

Table 8.4: University security policy questions:

Question		Imam U	PNU
6- Does the university have policies available on which websites you can access relating to website security?	No	36%	48%
	Yes, but don't know how to get the policies	52%	38%
	Yes	12%	14%
7- Does the university have policies on how and what you can and cannot use email for?	No	48%	32%
	Yes but do not know the policies	24%	32%
	Yes	12%	16%
	Do not know	16%	20%
8- Is instant messaging allowed in your university?	Yes, can use it with anyone	24%	10%
	Yes, but can only use it with other university employees	0%	10%
	No	16%	12%
	Do not know	60%	68%
9- Can you use your own personal devices, such as your mobile phone, to store or transfer confidential university information?	Yes	32%	26%
	No	36%	40%
	Don't know	32%	34%

The data collected from section two, university security policy, of the survey for both universities shows that most of the participants either thought that the university did not have policies available or that the university did have policies but they did not know how to get them (88% for ImamU and 86% for PNU). The majority of the participants of both universities did not know if the university has policies on how and what they can and cannot use email for (88% for ImamU and 84% for PNU), and did not know if instant messaging was allowed in their university (86% for ImamU and 80% for PNU). Moreover, most of the participants thought that they either can use their own personal devices, such as their mobile phone, to store or transfer confidential university information or they did not know if they can (64% for ImamU and 60% for PNU) (Table 8.4, Q6,Q7, Q8, Q9).

These results show that there is no effective information security policy at either university and, as a result, users are unaware of what is and isn't good practice and the university lacks control over information security.

The data analysis of the third section, user knowledge and security awareness is shown next (Table 8.5).

Table 8.5: User knowledge and security awareness questions:

Question		Imam U	PNU
10- Does the university have an information security team?	Yes	28%	30%
	No	40%	22%
	Don't know	32%	48%
11- Do you know who to contact in case you are hacked or if your computer is infected?	Yes	28%	38%
	No	72%	62%
12- Do you know how to tell if your computer is hacked or infected?	Yes	28%	22%
	no	72%	78%
13- How careful are you when you open an attachment in email?	Do not open attachments	4%	2%
	Always make sure it is from a known person	20%	18%
	Open it if known person or company	68%	62%
	Nothing wrong with opening attachments	8%	18%
14- Do you know what an email phishing attack is?	Yes	24%	16%
	No	76%	84%
15- Do you think that your computer has no value to hackers, so no one would target it?	Yes	44%	62%
	No	56%	38%
16- If you delete a file from your computer or USB stick, that information can no longer be recovered	True	40%	30%
	False	60%	68%
	don't know	0%	2%

The data collected from section three, user knowledge and security awareness, of the survey for both universities shows that most of the participants either thought that the university did not have an information security team or did not know if the university had an information security team (72% for ImamU and 70% for PNU). Most of the participants did not know who to contact if they were hacked or if their computer was infected (72% for ImamU and 62% for PNU), and an even greater proportion did not know how to tell if their

computers were hacked or infected (72% for ImamU and 78% for PNU). They were not careful when opening an email attachment (76% for ImamU and 80% for PNU) and did not know what email phishing attacks were (76% for ImamU and 84% for PNU). A high proportion of the participants thought that their computer had no value for hackers to target (44% for ImamU and 62% for PNU) and some thought that if they deleted a file from computer or USB stick, that information can no longer be recovered (40% for ImamU and 32% for PNU), (Table 8.5, Q10, Q11, Q12, Q13, Q14, Q15, Q16).

This section again confirms that information security awareness is very low at both universities and that users didn't know what procedures they could or should follow to keep their information safe.

The data analysis of the fourth section, user experience is shown next, (Table 8.6).

Table 8.6: User experience questions:

Question		Imam U	PNU
17- Have you ever found a virus on your computer at work?	Yes, it has been infected before.	44%	26%
	Never	36%	48%
	Yes, but don't know if it has ever been infected	12%	26%
	Do not know what a virus is	8%	0%
18- Have you ever given your work password to a co-worker or someone else?	Yes	64%	58%
	No	36%	42%
19- Has your manager or anyone else you know at work ever asked you for your password?	Yes	60%	58%
	No	40%	42%

The data collected from section four of the survey, user experience, for both universities shows that most of the participants thought that they had found a virus on their computer at

work (56% for ImamU and 52% for PNU). Most participants had shared their work password with a co-worker (64% for ImamU and 58% for PNU), had given their manager or anyone else they know at work their password (60% for ImamU and 58% for PNU), (Table 8.6, Q17, Q18, Q19). From this section, it is clear that most participants at both universities did not follow basic security practices, so it is not surprising that many had been victim of a computer virus.

The data analysis of the fifth section, user security practise is shown next, (Table 8.7).

Table 8.7: User security practise questions:

Question		Imam U	PNU
20- Is your computer configured for the security to be automatically updated?	Yes	56%	30%
	No	44%	22%
	Don't know	0%	48%
21- Have you downloaded and installed software on your computer at work?	Yes	28%	24%
	No	72%	76%
22- Do you use the same passwords for your work accounts as you do for your personal accounts at home, such as Facebook, Twitter or your personal email accounts?	Yes, for many personal accounts.	28%	4%
	Yes, but only for some accounts	32%	30%
	No	40%	66%
23- How often do you take information from work and use your computer at home to work on it?	Almost every day	20%	24%
	At least once a week	16%	26%
	At least once a month	16%	14%
	Never	48%	36%
24- Have you logged into work accounts using public computers, such as from a library, cyber cafe or hotel lobby?	Yes, many times	8%	18%
	Yes, only on rare occasions	24%	34%
	No	68%	48%

The data collected from section five, user security practise, of the survey for both universities shows that many of the participants either thought that their computers were not automatically updated to be configured for the security or did not know if they were (44% for ImamU and 70% for PNU). Some participants had downloaded and installed software on their computers at work (28% for ImamU and 24% for PNU). Many participants used the same passwords for their work accounts as they did for their personal accounts at home, such as Facebook, Twitter or their personal email accounts (60% for ImamU and 34% for PNU), took information from work and used their computer at home to work on it (52% for ImamU and 64% for PNU) and logged into work accounts using public computers, such as from a library, cyber cafe or hotel lobby, (60% for ImamU and 34% for PNU) (Table 8.7, Q20,Q21, Q22, Q23, Q24).

While some of these actions are not necessarily incorrect in themselves (installing legitimate software, for example) these actions are all high risk if the participant does not understand security issues. The answers also show the universities have a lack of policy or control over the actions of their staff and students.

8.3 Conclusion

According to the data analysis from the five sections of the survey the users for both universities are not aware of the information security due their lack of knowledge of the threat and risk involved in the misuse of information. The data collected from section one shows that many or most users:

- Did not know if their personal computers were secure,
- Did not know what a firewall is, and did not know what anti -virus software is,
- Did not know what an email scam is.

Also, the users in both universities did not have any kind of security policies available to them related to the information security email usage or what and where to store

confidential university information. The data collected from sections two and four show users believed that they:

- Did not have information security policies available or, if they did, they did not know how to get them,
- Did not know if their university has policies on the use of email,
- Did not know if instant messaging was allowed in their university
- Would use their own personal devices, such as their mobile phone, to store or transfer confidential university information.

Because most users in both universities are not involved in the development of the information security systems, the users generally did not know if their university had an information security team or whom to contact if their computers get hacked. They cannot tell if their computer was hacked or which actions are bad practice that could lead to hacking. The data collected from sections three and four show many users:

- Thought they did not have a university information security team,
- Did not know if the university has an information security team,
- Did not know who to contact if they were hacked or if their computer was infected,
- Did not know how to tell if their computers were hacked or infected,
- Were not careful when opening email attachments,
- Did not know what an email phishing attack is,
- Thought that their computer had no value to hackers to target
- Thought that if they delete a file from computer or USB stick, that information can no longer be recovered.
- Had found a virus on their computer at work,
- Had shared their work password with a co-worker,
- Had given their manager or someone else they know at work their password.

The users from both universities do not understand security issues and the risk associated with misusing their accounts and work computers. The data collected from section five shows many users:

- Thought that their computers were not automatically updated to be configured for the security.
- Had downloaded and installed software on their computers at work.
- Use the same passwords for their work accounts as they do for their personal accounts at home, such as Facebook, Twitter or their personal email accounts.
- Take information from work and use their computer at home to work on it.
- Logged into work accounts using public computers.

This shows that there is, clearly, a severe lack of awareness of security issues and those bad or dangerous practices are common at both universities. These security issues are widespread and involve all types of university staff and students. The results also show a lack of any effective policy and university control for information security. This shows the value of the application of the culturally aware information security policy framework focussed on involving users of all types in the information security processes by being part of a team that helps in developing information security policies (pre-step team formation section 7.1.1). This will help users to know the university information security team (step 3, figure 7.2) and know the processes of the information systems they use. The result should be to help in developing proper procedures and standards that are understood and relevant to the users (step 4, figure 7.2). Being part of risk assessment and information security auditing (step 5, figure 7.2) will maintain and enhance the understanding and also ensure the assessment and audits are more effectively carried out. The application of the framework also focusses on involving the users in classifying system information (step 6, figure 7.2), defining rules and access controls for handling system information (step 7, figure 7.2), defining and selecting proper information security controls (step 8, figure 7.2), defining an incident management and business continuity plan (step 9, figure 7.2) and conducting a policy gap analysis (step 10, figure 7.3). The next chapter explains the application of the framework main steps, 3 to 10.

Chapter 9: Evaluation of a culturally aware information security policy framework

This chapter covers the application and evaluation of the implementation and post implementation phases of the developed culturally aware information security policy framework. The information security policy framework developed in chapter 7 is based on the objectives from section 1.2, the literature review, the culturally unique issues from chapter 3, and the collected data from chapters 5 and 6. The framework focuses on raising the level of information security awareness among employees working in an environment with cultural differences. The identified factors that have a negative effect on the level of information security awareness, collected from the outcome of chapter 8, are used to produce a framework that helps in raising the level of awareness. This chapter explores in the following sections the application technique used to develop the culturally aware information security policy framework, the formation of the information security framework team, the application of the framework phases 2 and 3 and steps 3-10, the issues raised while applying each step and the resolution of the those issues.

9.1 The application of Phase 2: Step 3 - Definition of roles and responsibilities

Step 3 is the definition of roles and responsibilities. At PNU roles and responsibilities have been created, most of which are equivalent to the ones defined in the ISO standard and best practices such as:

- The ownership of the information policies and the head of the Information technology department changed during the previous year from Dr Nasser Almojel to Dr Alsadhan, and the Data Centre Manager is Dr Ghazi Alghamdi, both are male managers.
- Each information system has an owner. The Banner administrative system has two owners, one is male and the other is female.

- Most information custodians are male and they operate most of the university information systems in the male environment. There are two types of information custodians, some use the information systems and the others are technicians. The few female custodians of either type are commonly directed by the male employees and just follow orders.
- The majority of the information users are the non-IT employees and students who are all female.

Issues raised when forming step 3: There were culture factors and issues. PNU structure is a management and gender hierarchy structure. Most employees just follow orders from the top management. If the top management do not tell their employees what to do, jobs do not get accomplished. The male employees dominate the female employees. Men typically do not listen to women and they expect women to do as they say. Female employees do not contribute in decision making and are not encouraged to report issues. Female employee involvement was found to be limited in the decision making on information security policies. This was one of the reasons that the newly formed information security team did not know of these roles nor did they know who was responsible for the information security policy at PNU. Furthermore, according to the survey result in Chapter 8, approximately 70% of the participants did not know the people in charge of information security, see Figure 9.1.

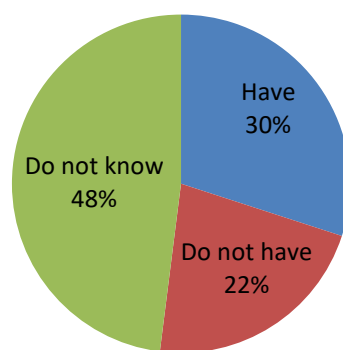


Figure 9.1: Does the university have an information security team?

Moreover about 62% did not know who to report threats to, see Figure 9.2.

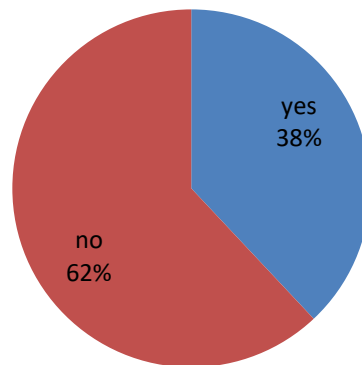


Figure 9.2: Do you know who to contact in case you are hacked or if your computer is infected?

Solution: Each department in each college at PNU should create an information security team and the team leader should act as the Information Security Officer Assistant (female) (figure, 7.1, step 0). The Information Security Officer is replaced yearly by one of her most qualified team members. The role of the information security officer assistant is to:

- Act as a conduit between the university college department and information technology security team.
- Form the Framework implementation team.
- Train the team members to:
 - Contribute in auditing the information system
 - Recognise and record the information system threats
 - Classify threats according to the risk associated with it
 - Recognise, classify, assess and report risk
 - Help in developing information security policy
- Develop information security policy

The developed information security policies for each department are collected and sent to the Information Security Officer. The Information Security Officer should then develop a comprehensive information security policy that covers all part of the collected policies.

9.2 The Application of Phase 2: Step 4 - Definition of information system procedures and standards

Step 4 is the definition of information system procedures and standards. Information system users should be aware of all the system procedures and standards. The owner of the information system, with the help of the information custodians, should list the procedures and standards and the way they should be set and handled, with the help of the Information System Team members and the system users, to enable a secure information system to be formed (subsection 7.3.2).

- Creation and termination of an account (subsection 7.3.2.1):
 - An online form for creating a new account for each user, with his/her privileges and restrictions listed, should be completed and then approved by:
 - The account user
 - The Dean of the user's school
 - The owner of the information system
 - A copy of the form is given to the user, either via email or regular mail, and another copy is sent to HR to be stored in the user file.
 - A form for termination of an account for a user who leaves the information system due to changing or leaving the organisation should be completed and approved by the user, school Dean and owner of the information system.
 - Termination of an account must occur immediately after the termination form is approved.

Issues raised creating an account: According to one of the formed information security team members, each information system user must fill in an online form that only covers one aspect, the personal information of the new account user. However, there are no privileges, policy and restrictions listed. There is no approval signature by the account user, school Dean or the owner of the information system. There is a gender hierarchy culture factor that limits female employee involvement in the decision making when creating an information security account policy and, even then, females are only expected to follow the orders of their senior, male managers.

Solution: The form to create an account should be modified so that privileges, policy and restrictions are added to it. Unused accounts must be disabled if not used for a month or immediately when the user contract terminates. Female employee involvement and contribution in the development of the university information security account creation policy is recommended. The form should consist of three parts:

- Personal user account information
- A list of all the privileges and restrictions on the account
- The user account access authorisation
- The disciplinary action for each policy misuse referred to as university internal disciplinary policy.
- A check box for user agreement that:
 - Sharing the user's computer identification or password is not acceptable at any level.
 - Accessing other employees' accounts is not acceptable and should be subject to disciplinary action
 - Their password will be replaced with a complete new password periodically.
 - User failure to comply with this policy is subject to disciplinary action.
- Approval signatures by the account user, school Dean and the owner of the information system

9.3 The Application of Phase 2: Step 5 - Risk and threat assessment and classification

Step 5 involves conducting risk and threat assessment and classification in which system users, employees and students, male and female, need to recognise, record, report and classify threat and risk. Authorised system users need to know how to periodically record information assets and report threats and classify the threats based on their effects and occurrence (subsection 7.3.3).

Issues raised when carrying out step 5: Because of the PNU management and gender hierarchy structure, most employees just follow orders from the top management. Female employees do not contribute in decision making and are not encouraged to report issues. The team admitted that they were not involved in recognising, recording, reporting and classifying threat and risk. They admitted that this was one of the reasons that the information security awareness level among them is low. They are qualified enough to contribute and would have liked to help in raising the information security awareness level. However, the only task they were asked to undertake was to report spam emails. The team admitted that they know what spam email is but other, non-computer departments may not know. According to the awareness survey 82% of the employees and information systems users did not know and could not identify spam and scam emails, see Figure 9.3.

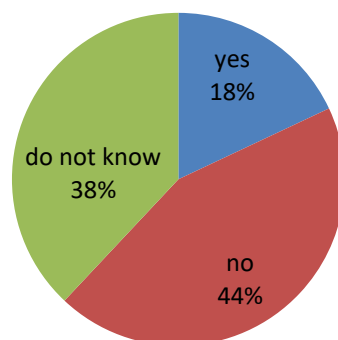


Figure 9.3: Do you know what an email scam is and how to identify one?

Solution: The team needed help in how to periodically record information assets and report threats and classify the threats based on their effects and occurrence. Therefore, table 7.4, 7.5 and 7.6, adopted from the Oxford University IS Policy, 2012, were modified and used to help them in recording their feedback. The team found the tables very helpful and agreed that these tables could help if distributed to all employees in the department to record, report and classify threat and risk. The tables are to be collected at the end of the semester and the information security team members will use them in developing information security policy.

Table 9.1: Recording and reporting information assets problems

Asset	Type	Location	User Position	Problem faced	Frequent occurrence	Risk rate	effect	reported	fixed

Table 9.2: Risk rating

Risk rate	Frequency of occurrence
Low	Once a year or less
Medium	At least once a semester
High	At least once a month

Table 9.1 and 9.2 were distributed to all types of employees to record their feedback. Table 9.1 is used to record and report problems faced by employees. Table 9.2 is used as a reference for employees to record the risk rate according to the number of occurrences. At the end of each semester the tables were collected by the formed information security team secretary either by email or hand in. The collected information from table 9.1 was used by the formed information security team members for:

- Risk and threats classification based on the frequency of occurrence
- Risk assessment

- Audit assessment
- Follow up of the reported problems

Table 9.3: Recording information assets

Asset	Type	Location	User Position	Problem faced	Frequent occurrence	Risk rate	effect

Table 9.4: Listing threats (adopted from Oxford University IS Policy, 2012)

Threat	Type	rate	Frequency of occurrence	reported	fixed

These tables were distributed to IT students and staff to record their feedback during the formation of the framework. Distribution of tables is to involve all types of information system end users in the development of the information security policy so that employees' contributions can help raise their level of information security awareness.

Tables 9.2, 9.3 and 9.4 were modified and distributed both in English and Arabic languages. The English version was distributed to students and the Arabic version was distributed to the staff. The collected recorded feedback data showed that using a language that is not well known to them led students to record inaccurate data. The students were confused by the use of English language, whereas the tables collected from staff which were written in Arabic, a language well known to all end users, had accurate feedback data (see Appendix C). Therefore, to collect crucial and accurate feedback data for the security of information systems, the language used should be the spoken language that each employee understands the best (subsection 7.2.2.3).

9.4 The application of Phase 2: Step 6 - Classification of the System Information

Step 6 is the classification of the System Information, in which all system information assets (input / output) must be classified on their sensitivity (subsection 7.3.4). Information assets cover not only information (data, voice, video and paper) but also where it is stored and the systems and equipment that process them. According to ISO 27k, the classification of information assets is the responsibility of the information system owner. However, in countries with a culture of segregated working environments, the information custodians and all types of information users must know the university classification of information to help them recognise the importance of information assets.

Issues raised when carrying out step 6: There are culture issues because PNU has a gender hierarchy structure. The male employees dominate the female employees. Men typically do not listen to women and they expect women to do as they say. Female employees do not contribute to decision making and are not encouraged to report issues. Therefore, at PNU the classification of the information is developed by the Information system staff, who are mostly male. Section 6.7 shows that the majority of PNU female employees did not know whether the university classified its information, due to their limited involvement in the university classification of information. The team agreed that this is one of the system administration faults that lowered the level of information security awareness.

Solution: Forming an information team annually to involve female end users is one solution to the issue raised when carrying out step 6. Another solution that the team agreed was to distribute tables 7.2 and 7.3 as these can help the user recognise threat and the risk level and this can help in classifying the information according to the risk level associated with it. The team also agreed that table 7.4 could be used as a starting guideline in classifying system information. Being part of information classification can help the end users recognise the importance of information handling and the level of risk associated when it is mishandled.

9.5 The application of Phase 2: Step 7 - Defining rules and access controls

Step 7 is defining rules and access controls for handling system information assets. Information assets are not only data and the servers that hold the information, it includes employees and their computers and workstations. According to subsection 7.3.5, rules and access controls include laws and regulation, storage, access controls, copying data, retention and disposal and exchange information and use of email.

- **Laws and regulations:** The Saudi Arabian government has not developed its own laws, regulations and acts related to data protection and the use of computers or adopted relevant western laws and regulations, such as the General Data Protection Regulation 2018 (GDPR 2018), the UK Data Protection legislation of the Data Act 1998 (DPA 1998) and the UK Computer Misuse Act 1990 (CMA 1990) (Subsection 8.12.2, Table 8.2 Q6,7,9). Therefore, Saudi universities such as PNU need to adopt appropriate laws, regulation and acts from elsewhere. The team members recommended the Data Protection Act of 1998 (DPA 1998) and the UK Computer Misuse Act of 1990 (CMA 1990) since they are more comprehensive than the USA's acts.
- **Storage:** Most Saudi universities have used outsource companies to handle their information. At PNU, information is kept at an appropriate level of physical security, within a building called the Data Centre, according to the outsource company, Wipro. However, in the female work environment the physical security used to secure most computers and workstations is not under an appropriate level of physical security. For example, PNU have a card access control to physically secure computer labs and management offices. However, this card access control is not active yet. Other issues are related to the large number of workstations used by most employees which are kept in open spaces with no physical door to secure them (observed by the author and confirmed by all group members and co-workers). Some of the offices that have a physical door are not as secure as expected because there is a "master key" that can open any door in the school which is available to

anyone who asks for it, including students and the janitor according to one of the information security team members. Most employees complain about the number of thefts that have happened from their offices and workstations.

- **Access controls:** Although most information assets in most Saudi universities have used two-factor authentication, user name and password, as access controls, allowing only authorised users to be able to access information, there is no clear documented policy of a secure selection password that is distributed to users (Subsection 8.2.3.2.2, Table 8.4 on Q6 and Q7, and Table 8.6 on Q18, Q19, and Q22). PNU's information system users have no documented password selection policy. According to the prior assessment survey, there is no strict, well-defined access control policy in use (Subsection 8.2.3.2.2, Table 8.4, Q6 and Q7).
- **Copying data:** In most Saudi universities, copies of information are stored electronically but, with the lack of physical secured locked offices, cabinets or drawers, employees can take copies of the information assets with them outside the work area (Subsection 8.12.2, Table 8.5 on Q21, Q23 and Q24).
- **Retention and disposal:** Most Saudi Arabian knowledge-intensive organisations, such as PNU, have no documented policy for legacy information no longer needing retention and for legacy hardware disposal. Such a policy should cover the storage period for old information and hardware, the location of storage and when and how old information and hardware should be destroyed. According to one of the team members, there is no policy for how to dispose of the old exams papers. The lecturers at PNU are only told that at the end of the year they can get rid of the old exam papers, and one of the department maids would collect them in a trash bag.
- **Exchange of information and use of email:** PNU and most Saudi Arabian knowledge-intensive organisations have no documented policy for exchange of information and the use of email to protect them from unauthorised access. There is no procedure for how to handle threats associated with electronic messages available to users (Subsection 8.2.3.2.2, Table 8.3 on Q4 and Q5, Table 8.4 on Q7 and Table 8.5 on Q13 and Q14).

Issues raised when carrying out step 7: several issues were raised when carrying out this step:

- There were no clear documented laws, regulation or acts related to the security of the information.
- It was not clear to the users if the university had adopted any type of law, regulation or act related to the protection of data or computer misuse.
- There had been no distribution, via email or hard copy, of regulation, acts, laws or policies to any users.
- Almost all offices, computer labs, workstations and personal belongings were not fully secured due to the use of the freely available “master key” that can open any locked door, and the lack of CCTV.
- There is no documented policies for the use of password selection, retention and disposal of information or old hardware that is no longer needed and the exchange of information and use of email to prevent unauthorised use and access.

Recommended solutions: The information security team members agreed that the solutions to these issues would be to do the following:

- Distribute a clear, Arabic, hard and soft copy of any law, regulation and acts to all types of information system users.
- Secure university computers by activating the security card access control or any proper physical security access controls.
- Keep all workstations in a room with a door lock.
- Activate the already built in CCTV, and have all female employees to monitor it in order to avoid privacy issues.
- Provide clear and easy to read information security policies, documented and distributed via email and hard copy, which covers the use of email, password selection, retention and disposal of information or old hardware that is no longer needed, and the exchange of information and use of email. The policies must be as detailed as possible to ensure all employees follow them to the letter.

Once the rules and access controls are defined for handling the information of the system, the next step would be to define the technical controls, physical controls and procedural controls.

9.6 The application of Phase 2: Step 8 - Information security controls are defined and selected

Step 8 is where information security controls are defined and selected. This section covers the three types of security controls, which are technical controls, physical controls and procedural controls. According to subsection 7.3.6, technical controls can be divided into two different categories: preventative controls, including passwords, cryptography, digital signatures and biometric data and recovery controls, including antivirus programs.

Technical controls:

- **Preventative controls**
 - Passwords controls
 - Cryptography controls.
 - Three-factor authentication, username, password and a text message code.
- **Detective and recovery controls**
 - Antivirus software

Physical controls

- CCTV
- Fire alarm system
- Door access controls
 - Cards access
 - Biometric controls

Procedural controls:

- Documented information security policy: This covers all information system elements such as data, programs, computers, networks, facilities, people, and

processes. According to subsection 2.5.3, the effectiveness of information security policy depends on helping the employees understand the rights and responsibilities of information resources, focusing on the safety and security of information handled in daily tasks.

- Training and education: This is necessary to protect PNU from new threats. However, it is not an easy task to create a training programme, see subsection 2.6.1.1.
- Enforcement: All users who have access to information assets are required to comply with the country's laws and regulation and university policies and procedure related to information security. Any user who engages in unauthorised use, disclosure or destruction of information assets should be subject disciplinary action (section 2.6.1.2).
- Compliance: Compliance with the organisation's security policy when handling information assets should be part of any contractor's or other third party's contract if they have access to the information assets network. According to section 2.6.1.3, a documentation of a personal information security plan can be used to ensure compliance by employees.

Issues raised when carrying out step 8: According to the system observation by the information security team members, the controls were not properly executed. Users are forced to use passwords as a way of authentication but there is no written policy or advice on:

- How to choose a strong password
- When to change a password
- How to handle a password

Therefore, as a result, a user will often choose an easy password, re-enter an old password or share their password with other colleagues.

- There are access card devices in all labs and important offices but none of them are active.

- Most end users cannot tell if their antivirus program is active. There is no automatic update of the user's antivirus software and most of the users' antivirus programs have expired.
- There is CCTV built-in to each room of the campus building, but none of them are active.
- The fire extinguishers are installed in each room of the campus building, but some fire alarm devices are not active or need their batteries changed. This is very critical to check as part of physical security controls.
- Almost all offices, computer labs, workstations and personal belongings are not fully secured due to the lack of CCTV or the use of the "master key" that can open any locked door and can be used by anyone, including students.

Recommended solutions:

- Provide users with simple, easy to read, Arabic copies of the PNU policies related to information security. All computer users must be informed about and comply with these policies.
- Keep all workstations in a room with a door lock.
- If the data is particularly sensitive, or there is a significant risk of access by unauthorised personnel, then a CCTV installation covering PNU computers should be considered and monitored by suitably trained female security staff.
- The fire alarm system is already installed, but has not been tested. Some of the alarm devices in employees' offices were not active and, more importantly, the employees could not tell if devices were working or not. The alarm system should be tested to ensure it is switched on and working in all rooms.
- Install physical access control devices. If any physical access control devices are installed, such as PNU card access devices, then tests should be taken to ensure they are active and working.

9.7 The application of Phase 2: Step 9 - The incident management and business continuity plan

Step 9 is the incident management and business continuity plan. When an accident or natural disaster occurs which damages the information system, the owner of the information system must make sure that the business will continue with a business continuity plan. The business continuity plan should have (subsection 7.3.7):

- **Complete backup and incremental plan**

An external copy is required for information, using mass storage media, such as servers, to prevent data loss and archive the old data that is not in use on separate, long term, mass storage media. Information needs to be safe and available all the time. Also, it is necessary for information to be recovered and restored in the event of a hardware or software failure, accidental deletion, damage, or physical disaster. The backup should cover all university new and old electronic stored information. All electronic information will be stored on data centre servers or on the cloud to allow backups to take place regularly. Backup and system recovery plans and processes should be in place and tested to define, for example:

- What information assets need to be backed up in the information system.
- The order the information assets should be backed up according to their importance
- The frequency and the number of information assets to be backed up. Which information assets need daily incremental backup and when the information assets need a full backup.
- The method and frequency of the testing of the backup
- The backup information assets to be disposed of when they are no longer needed.

- **Off-site storage confidential data**

The organisation must make sure that copy confidential data is secure in an off-site location if the university encounters any natural disaster, such as fire or flooding. The

Internet could be used as an off-site storage. Cloud computing is computer resources, hardware and software, services that are delivered over a network, especially the internet (Mirzaei 2008).

- **Test of the recovery process**

The overall business continuity plan should be tested periodically to make sure the business will not stop if any accident or disaster occurs.

Issue raised when carrying out step 9: There were cultural factors and issues caused by the PNU management and gender hierarchy structure. Most employees just follow orders from the top management. Most employees, staff, students and faculties:

- Do not know what a complete backup and incremental plan is. The only thing they are aware of is that sometimes, if some of their files are missing, they can get them back by calling the IT technician staff. Sometimes they back up their own data in a portable storage device such as a flash memory.
- Are not involved in the classification of the data and do not know what information is confidential or if it is stored anywhere outside their own computers.
- Do not play any part in the test of the recovery processes. The only thing the employees, staff, students and faculties knew is that the data are stored somewhere either in their own computer or inside the organisation's building.

Recommended solution: The formed information security team admitted that this step to create the incident management and business continuity plan are undertaken by IT staff or the outsource companies with male majority employees. The female employees, staff, students and faculties have no say in:

- When PNU does an incremental or complete backup,
- Where PNU stores confidential data
- How PNU does a test of data recovery

In the application of the culturally aware information security policy framework, the formed information security team was convinced that this step should be undertaken by people who were qualified for this job, i.e. IT staff or the outsource companies. The

end users can only contribute in the classification of the information and which information is more confidential. Moreover, the IT staff or the outsource companies would allow them to take part in very few of the process in this step.

9.8 The application of Phase 3: Step 10 – Application of the Information Security Policy

According to subsection 7.4.1, by this step formation of information security policy is completed. The owner of information system with the rest of the formed information security team applies the newly produced policy to check its effectiveness in securing the information system. They should:

1. **Review the produced information security policy:** a copy of the information security policies produced during the application of the cultural aware information security framework was reviewed with the formed information security team for further modification (See Appendix D).
2. **Test the produced information security policy:** This involved carrying out a survey of PNU employees and comparing the results with that obtained before the implementation. This is described in Section 9.8.1.
3. **Update the produced information security policy:** After the formed information security team reviewed, test and modified the produced information security policy for the information system department based on the data collected from the assessment survey, the produced information policy was updated to best fit the PNU system and users.

9.8.1 Testing the produced information security policy at PNU

The wider user base at PNU was informed of the information security policy developed by the information security policy team by:

- Presenting it to the end-users, students and staff through a presentation called “My Information, My Wealth”, covering:
 - o The meaning of information

- The importance of information
- The meaning of information security
- What information we need to secure
- How we protect the information

Workshops and meetings with other staff and students on how to be part of the development information security policy, how to recognise risk or threat and why they need to participate in reporting any risk or threat. Tables 9.1 and 9.2 were discussed in the workshop before copies were given to them to help them report threat and risk.

A test of the produced information security policy framework was then undertaken by:

1. **Applying a post-assessment survey:** a survey identical to the prior assessment survey in chapter 8 was distributed to all types of users who were involved in the application of the cultural aware information security framework.
2. **Analysing the collected data:** The survey result showed that PNU have lowered the level of risk compared to the level of risk before the application of the framework (52.4 compared to 71.5). The risk level was lowered after the application of the cultural aware framework due to the involvement of users in the development information security policies (See Table 9.5).

Table 9.5: PNU IS Department Risk level before and after the application of the cultural aware information security framework

	Risk level	Description
PNU IS Department	52.4 (Elevated)	Users have already been trained on organizational security standards and policies, they are aware of threats, but may not follow good security principles and controls.
PNU before Framework Application	71.5 (Moderate)	Users are aware of threats and know they should follow good security principles and controls, but need training on organizational security standards and policies. They also may not know how to identify or report a security event.

The post assessment survey result for PNU shows that the risk level is lower than it was before the application of the framework. However, PNU still did not have any documented security policies distributed to the users. Therefore, the PNU end users do not have good security principles and controls to follow.

Table 9.6: Personal computer security questions

Question		PNU After Framework Application	PNU Before Framework Application
1- What is your position within the university?	Management	15%	26%
	Staff	25%	58%
	Lecturer	20%	6%
	Student	40%	4%
	others	0%	6%
2- How secure do you feel your computer is?	Very secure	10%	4%
	Secure	65%	44%
	Not secure	20%	16%
	do not know	5%	36%
3- Is the firewall on your computer enabled?	Yes	50%	18%
	No	5%	4%
	do not know	30%	44%
	do not know what a firewall is	15%	34%
4- Is anti-virus software currently installed, updated and enabled on your computer?	Yes	75%	28%
	No	15%	4%
	do not know	10%	56%
	do not know what anti-virus software is	0%	12%
5- Do you know what an email scam is and how to identify one?	Yes	60%	18%
	don't know how to identify one	35%	44%
	do not know an email scam	5%	38%

Table 9.7: University security policy questions

Question		PNU After Framework Application	PNU Before Framework Application
6- Does the university have policies available on which websites you can access relating to website security?	No	20%	48%
	Yes, but don't know how to get the policies	65%	38%
	Yes	15%	14%
7- Does the university have policies on how and what you can and cannot use email for?	No	35%	32%
	Yes, but do not know the policies	45%	32%
	Yes	15%	16%
	Do not know	5%	20%
8- Is instant messaging allowed in your university?	Yes, can use it with anyone	20%	10%
	Yes, but can only use it with other university employees	0%	10%
	No	10%	12%
	Do not know	70%	68%
9- Can you use your own personal devices, such as your mobile phone, to store or transfer confidential university information?	Yes	30%	26%
	No	60%	40%
	Don't know	10%	34%

Comparing the Phase 3 collected data (Table 9.6 and Table 9.7) with the earlier collected data (Table 8.3 and Table 8.4), in chapter 8 subsection 8.2.3.2.2, before the application of the framework, shows that after the application of the framework, many or most users:

- Did know if their personal computers were secure (75% compared to 48%),
- Did know what a firewall is (50% compared to 18%), and did know what anti-virus software is (75% compared to 28%),
- Did know what an email scam is (60%, compared to 18%).

- Did know all information security components - most of the post assessment participants responses for the answer “don’t know” were between 0% and 15% compared to 12% and 38% before.
- Did have information security policies available (65% compared to 38%), but unfortunately they still did not know how to get them,
- Did know that their university has policies on the use of email (60% compared to 48%),
- Still did not know if instant messaging was allowed in their university (75%)
- Although bring their own devices are not restricted by PNU management, and it was easy to use their own devices, respondents would not use their own personal devices, such as their mobile phone, to store or transfer confidential university information (60% compared to 40%).

According to the above result of the pre-post application of the framework, the users show an improvement in their level of information security awareness e.g. they improved in knowing what a firewall is, knowing what anti-virus software is and knowing what an email scam is. The areas where there was little no improvement, such as knowing where to access policies and knowing whether instant messaging was permitted shows areas where the training and provision of information could be improved in any future application of the framework.

Table 9.8: User knowledge and security awareness questions

Question		PNU After Framework Application	PNU Before Framework Application
10- Does the university have an information security team?	Yes	50%	30%
	No	5%	22%
	Don't know	45%	48%
11- Do you know who to contact in case you are hacked or if your computer is infected?	Yes	60%	38%
	No	40%	62%
12- Do you know how to tell if your computer is hacked or infected?	Yes	60%	22%
	no	40%	78%
13- How careful are you when you open an attachment in email?	Do not open attachments	15%	2%
	Always make sure it is from a known person	25%	18%
	Open it if known person or company	60%	62%
	Nothing wrong with opening attachments	0%	18%
14- Do you know what an email phishing attack is?	Yes	60%	16%
	No	40%	84%
15- Do you think that your computer has no value to hackers, so no one would target it?	Yes	25%	62%
	No	75%	38%
16- If you delete a file from your computer or USB stick, that information can no longer be recovered	True	20%	30%
	False	80%	68%
	don't know	0%	2%

Table 9.9: User experience questions

Question		PNU After Framework Application	PNU Before Framework Application
17- Have you ever found a virus on your computer at work?	Yes, it has been infected before.	50%	26%
	Never	40%	48%
	Yes but don't know if it has ever been infected	10%	26%
	Do not know what a virus is	0%	0%
18- Have you ever given your work password to a co-worker or someone else?	Yes	10%	58%
	No	90%	42%
19- Has your manager or anyone else you know at work ever asked you for your password?	Yes	10%	58%
	No	90%	42%

Comparing the collected data (Table 9.8 and Table 9.9) with the earlier collected data (Table 8.5 and Table 8.6) from chapter 8 subsection 8.2.3.2.2, before the application of the framework, shows that after the application of the framework, many or most users :

- Did know that the university have information security team (50% compared to 30%),
- Did know who to contact if they were hacked or if their computer was infected (60% compared to 38%),
- Did know how to tell if their computers were hacked or infected (60% compared to 22%),
- Were careful when opening email attachments (100% compared to 80%),
- Did know what an email phishing attack is (60% compared to 16%),
- Did know that their computer had value to hackers to target (75% compared to 38%),
- Did know that if they delete a file from a computer or USB stick, that information can still be recovered (80% compared to 68%),
- Can recognise if their computer at work has a virus (50% compared to 26%),

- Will not share their work password with a co-worker (90% compared to 42%),
- Will not give their manager or someone else they know at work their password (90% compared to 42%).

The above result of the pre-post application questionnaire of the framework showed that the users significantly improved their level of information security awareness by not sharing their work password with a co-worker, not giving their manager or someone else they know at work their password, taking care when opening email attachments, knowing what an email phishing attack is and knowing that their computer had value for hackers to target.

Table 9.10: User security practice questions

Question		PNU After Framework Application	PNU Before Framework Application
20- Is your computer configured for the security to be automatically updated?	Yes	50%	30%
	No	20%	22%
	Don't know	30%	48%
21- Have you downloaded and installed software on your computer at work?	Yes	30%	24%
	No	70%	76%
22- Do you use the same passwords for your work accounts as you do for your personal accounts at home, such as Facebook, Twitter or your personal email accounts?	Yes, for many personal accounts.	20%	4%
	Yes, but only for some accounts	5%	30%
	No	75%	66%
23- How often do you take information from work and use your computer at home to work on it?	Almost every day	20%	24%
	At least once a week	10%	26%
	At least once a month	25%	14%
	Never	45%	36%
24- Have you logged into work accounts using public computers, such as from a library, cyber cafe or hotel lobby?	Yes, many times	10%	18%
	Yes, only on rare occasions	30%	34%
	No	60%	48%

Comparing section five's collected data (Table 9.10) with the earlier collected data (Table 8.7) from chapter 8 sub section 8.2.3.2.2, before the application of the framework, shows that after the application of the framework, many or most users :

- Did know that their computers were automatically updated to be configured for the security (50% compared to 30%).
- Had not downloaded and installed software on their computers at work (70%).
- Use passwords for their work accounts different from their personal accounts at home, such as Facebook, Twitter or their personal email accounts (75% compared to 66%).
- Minimised the information they take from work and use their computer at home to work on (45% compared to 36%).
- Do not log into work accounts using public computers (60% compared to 48%).

In the above collected results of the pre-post application of the framework, the users showed significant improvement in their level of information security awareness because they no longer download and install software on their computers at work and they now use different passwords for their work accounts from their personal accounts at home, such as Facebook, Twitter or their personal email accounts. They also minimise the information they take from work to use on their computer at home and they do not log into work accounts using public computers.

9.9 Factors affect the application of the framework

The application of the information security awareness framework was affected by several factors. These factors are:

- **Cultural factors and issues:** PNU structure is mainly a gender and hierarchy structure. Most employees just follow orders from the top management. If the top management do not tell their employees what to do, jobs do not get accomplished. The male employees dominate the female employees. Men typically do not listen to women and they expect women to do as they say. Female employees do not contribute in decision making and are not encouraged to report issues.

- **The time taken and difficulty of getting PNU information management authority and permission:** The application of the framework required more time and effort than would be required in a Western country. For example, because of the unique close working environment culture in Saudi Arabian universities and because most major decisions were taken by the male administration, it took a long time to get the approval to start the application of the developed framework. That is because, according to Almunajjed (2009), in Saudi Arabia major administrative educational decisions are made by male employees, therefore, communication between the male and female work environment is slow and not as frequent as it should be.
- **Resource limitations:** It was hard to get sufficient employee buy-in to make the application of the culturally aware information security policy framework work.
- **The dedication and commitment of the information security team:** The team were not fully dedicated nor committed to the assigned schedule meeting and tasks due to their busy work schedule and personal issues. As a result they would frequently miss meetings and not respond to email requests from the researcher, especially in the later steps of the policy framework implementation.

9.10 Chapter Conclusion

The purpose of the application of the developed cultural aware information security framework is to involve all types of employees to contribute to the development of information security policy to raise the level of information security awareness among employees. This chapter covers the application of each of the ten steps in the cultural aware information security framework. The chapter describes the application of the steps, including any issues raised during the application and presents possible solutions to the issues raised. The chapter also discussed critical factors faced during the application of the cultural aware information security framework.

The last chapter, chapter 10 presents the research findings, achievements and contributions in raising the level of information security awareness among all types of system users. Chapter 10 also presents the research limitations, recommendations and future work and conclusions.

Chapter 10: Recommendation, Conclusion and Future work

This chapter presents the research contributions and achievements of the developed cultural awareness information security framework. The chapter also reviews the final research results and summarises the research overall findings. The last section of the chapter presents the research limitations, recommendations and suggestions for future work.

10.1 Research contributions and achievements

The research contributes knowledge in areas that have not been covered in the literature before, specifically the establishment of solutions to overcome the factors and issues of a closed culture environment that have a negative effect on the security of information in developing countries such as Saudi Arabia. The research aim was to raise the level of information security awareness among all types of information system users in Saudi Arabian knowledge-intensive organisations by involving them in the development of a system information security policy. The research developed a culturally aware information security framework, which is a multi-step process used to enhance the information system users' awareness in the security of information and reduce risk and threats to the system information. The framework is used to achieve the aim and objectives that had been identified in chapter 1. The research followed specific actions to fulfil the research objectives which are:

Objective 1: Carry out a literature review to discover:

- a. What technology, policies and actions are regarded as best practice to safeguard the security of information systems in an organisation?**
- b. What are the potential dangers and types of attack that could be a threat to the security of IT systems, and whether any of these dangers pose a greater risk in Saudi Arabia than elsewhere?**
- c. What are the potential barriers to a successful implementation of these technologies, policies and actions, and in particular whether the awareness levels,**

cultural attitudes, practices and the law in Saudi Arabia contribute to these barriers?

- d. What are the possible policies and actions to overcome these barriers and whether these could be applied in Saudi Arabia?**

In Chapter 2, the literature review on previous work identified the potential dangers and types of attack that could be a threat to the security of IT systems, with some of these dangers posing a greater risk in Saudi Arabia than in western countries. Most importantly, the research identified the potential barriers to a successful implementation of these technologies, policies and actions and, in particular, showed that the awareness levels, cultural attitudes, practices and the law in Saudi Arabia contribute to these barriers. Therefore, applicable policies and actions were developed and analysed to overcome these barriers so that they could be applied in Saudi Arabia.

Objective 2: By means of interviews, surveys and experiments, determine what is the current state of IT security at PNU, the case study, in particular:

- a. How adequate are the IT security policies and practices at PNU and how susceptible to possible attacks and dangers are the PNU information systems?**
- b. Could the IT security best practice identified in the literature review be applied at PNU?**
- c. Do the dangers to IT security identified in the literature review exist at PNU and are there any other dangers particular to PNU?**

The initial collected data results identified cultural factors and issues of a closed culture environment that have negative effect in the security on information. The culture related factors and issues found were language barriers, hierarchy, gender communication, fear of losing face, nepotism and wealth, and these affected the information security of Saudi Arabian knowledge-intensive organisations as described in Chapter 3. These culture issues have a negative impact in the communication, the level of information security training, education and awareness among all types of users within an organisation. These issues were determined from the analysis of surveys and interviews in chapter 5 and 6.

Objective 3: Analyse the findings from Objective 2 to formulate a practical and effective policy and action plan for any Saudi Arabian knowledge-intensive organisations to improve their IT security, with particular emphasis on overcoming the awareness, cultural specific and legal barriers to IT security at Saudi Arabian knowledge-intensive organisations.

The findings of the survey and interviews from chapters 5 and 6 were used in the implementation of a culturally aware information security policy framework in Chapter 7. This consists of eight steps that have been adapted and modified from some of the ISO 27k steps, because Saudi Arabian knowledge-intensive organisations are working to get ISO 27k accreditation, as they are being strongly encouraged to by their government. Basing the proposed information security policy on the ISO 27K, therefore, is politically expedient to enable it to be successfully implemented in a Saudi Arabian or similar culture. Three additional steps were then added to support employees in working around issues caused by cultural differences, as described in chapter 7.

The developed framework is developed based on the objectives from chapter 1, the literature review, the culturally unique issues identified within chapter 3, and the collected data from chapters 5 and 6. The requirements for the implemented framework were derived in Chapter 7, which involve:

- a. Audit assessment
- b. Risk assessment
- c. Education, training and awareness
- d. Compliance
- e. Business continuity management
- f. Action required following the violation of information security

Objective 4: By conducting interviews and/or surveys at other organisations, determine how common are the dangers and barriers to information system security in other service organisations in Saudi Arabia and how much of the plan for PNU would be applicable to other organisations in Saudi Arabia.

The collected data method used was a before-assessment survey to measure and compare the information security level of awareness among two of the largest universities in Saudi Arabia, PNU and Imam University. Then, an after assessment survey applied to PNU the case study after the application of the developed culturally aware information security policy framework to measure the effectiveness of the framework in raising the information security awareness among employees. As described in Chapter 8, these were conducted before the application of the culturally aware information security policy framework and then after the application.

The finding shows that there is clearly a severe lack of awareness of security issues and bad or dangerous practices are common at both universities. These security issues are widespread and involve all types of university staff and students. The results also show a lack of any effective policy and university control for information security.

Conducting the testing at only one university and no non-university organisation is clearly a limitation of the testing of the application of the framework. However, the strong similarity in the pre-implementation survey results from the two academic institutions does show that the application of the framework will be potentially beneficial for all Saudi Arabian universities at least, and there is, therefore, at least a strong possibility that it would also be applicable in other knowledge intensive organisations in Saudi Arabia.

Objective 5: By analysing the results from Objective 4, apply the culturally aware information security framework to develop recommendations of policy and action for information system security in Saudi Arabian organisations.

In Chapters 8 and 9, the implementation of the framework focused on involving users of all types in the application of the culturally aware information security policy framework processes. This was carried out by being part of a team that helped in developing information security.

Objective 6: Test the framework. At this stage, the application of the developed framework for information security has been completed. The newly produced framework was tested to check its effectiveness in raising the level of awareness among employees to obtain a secure information system, by:

- User survey, post assessment.
- Observation
- Interviews

Moreover, a post-implementation test was conducted to determine how effective the implementation was. It was coupled with the pre-implementation results to see how effective the implementation of the framework has been and this helped identify parts of the implementation that need to improve.

The main contribution of this research is the developed culturally aware framework that helps to raise the level of information security awareness among all types of end-users in knowledge intensive organisations in Saudi Arabia. The framework was implemented at the case study organisation, PNU, using the collected data from surveys and interviews as described in previous chapters, and analysing this by quantitative and grounded theory methods (see Figure 10.1).

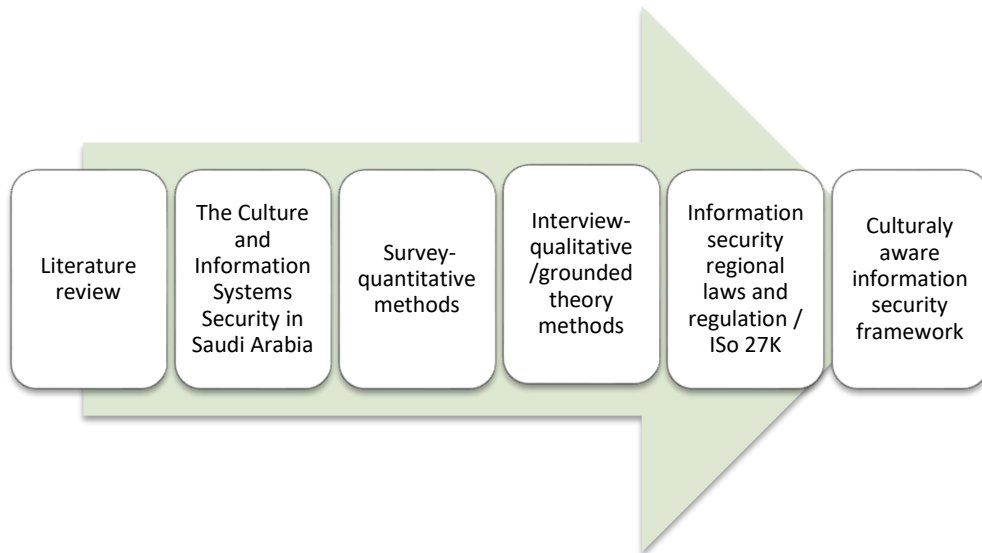


Figure 10.1: The research process in developing the framework

10.2 Research Limitations

Several limitations were raised when developing this research that affect the implementation of the proposed culturally aware information security policy framework:

- Difficulties were faced and time consumed in obtaining the authority and permissions from the PNU organisation to conduct the case study. The application of the developed framework required more time and effort because of the unique close working environment culture in Saudi Arabian knowledge-intensive organisations and because most major decisions on granting permission were taken by the male administration but the researcher was female, it took a long time to get the approval to start the application of the developed framework.
- Even with granted authority to conduct the case study, PNU required full control over the application of the framework for privacy reason. Therefore, testing of the framework was under significant constraints such as:
 - Team commitment due to the busy work schedules
 - Time constraints

- Employees preference to follow orders rather than come up with their own ideas
- It was not possible to extend the developed culturally aware information security policy framework to other universities in Saudi Arabia due to time and the difficulty of getting authorisation to do so.
- There were limited human resources available. It was difficult to get sufficient employee buy-in to make the application of the culturally aware information security policy framework work properly.
- There could be a bias response in collected data from the survey and interview questionnaires. Cultural factors such as saving face, inability to accept criticism, believing everything is fine, and the age of the respondent, all affected the responses especially when interviewing management.
- It was not possible to compare the survey outcome of Saudi Arabian knowledge-intensive organisations with other countries such as the UK due to time constraints. This limitation restricts the generalisation of the developed framework for use in other nations except where there are near identical conditions to those in Saudi Arabia.

10.3 Conclusions

This research reveals the existence of significant cultural issues that affect the level of information security awareness and make information systems in Saudi Arabian knowledge-intensive organisations vulnerable and victim to threats. There are no obvious policies or laws to protect information security other than the single Saudi Crime Act (see subsection 6.4.2 Q8-Q10 and Table6.2), but remarkably few people in Saudi Arabia seem to be aware of this law. Many researchers have only considered developed countries when examining the security of information and so have not considered regional culture to be a serious factor in the security of information in developing nations such as Saudi Arabia and the Gulf states.

This study initially examines the users' level of knowledge of information system security at Saudi Arabian knowledge-intensive organisations through the use of a survey and an interview questionnaire and analysis through using quantitative and grounded theory methodologies. The outcome of these questionnaires shows the existence of information security users' ignorance, their misuse of information and their unawareness of the threat and danger associated with their actions. The initial survey results showed that because of the users' commitment to their society culture, their information security awareness level was controlled by the regional culture factors, such as language, management hierarchy, gender communication, fear of losing face and nepotism, which have strong impacts on the success and security of an information system.

An awareness survey was developed to measure the level of information security awareness among all types of information system users. The results showed a clear lack of information security awareness, especially on how to detect and report threat and risk, to whom the threats should be reported, leaving their offices open, not knowing if their anti-virus is active or updated, and all aspects of spam and phishing emails. The findings of the research showed that the majority of users had high expectations and trust of each other, which can, in turn, affect the security of information. Examples of the bad practices resulting from this lack of awareness are that many users still share passwords and stick their passwords on 'Post-it' notes on their computer monitors.

The analysed of the findings have led to a recommended framework that focusses on minimising the culture issues and raising the information system users' security awareness level. The recommended framework has been designed to engage information system users in:

- the development of the information security policies,
- the auditing of the information systems,
- the identification of threats and the associated risks,
- the reporting of attacks,
- the classification of information and risks,

- Collaborative work to raise the of information security awareness level.

The success of the culturally aware information security framework suggests it could be it could be more widely applicable and, in particular, it could be useful for the Middle Eastern countries, Gulf Cooperation Council countries (GCC) and any developing or developed county that has similar cultural and management hierarchical conditions.

10.4 Future work

The research findings and results suggest possible recommended areas for further research:

1. The information security policy framework needs to be tried in other universities to confirm the framework's applicability to all academic institutions and then it needs to be applied in a range of non-academic organisations to confirm its use as a generic framework for all knowledge intensive organisations in Saudi Arabia. The framework needs to be applied to general elementary and high schools, the public and private schools. Finally, the framework needs to be applied in other countries in the Middle East and further afield to determine how well it will work in other developing countries with strong cultural and other environmental influences. It is the researcher's belief that the framework would be found to more widely applicable, at least within the Middle Eastern counties, but this needs to be confirmed by an extensive research programme.
2. Before the information security policy framework is tried in wider contexts, it would be useful to reduce some of the barriers that led to the limitations of this research. The culture of a very male dominated higher management in a very hierarchical management structure has yielded managers that are not properly qualified and subordinates that do not want to do anything other than what they are directed to do, but just follow orders without question. These cultural problems are deep rooted in the Saudi environment and would be hard to change. Nevertheless, the following are suggested ways of overcoming some of these barriers that should be tried to make the implementation of the information security policy framework easier to do:

- i. The qualifications gap and the negative attitudes towards continual learning needs to be addressed. Simply providing courses will not in itself solve the lack of qualifications problem if attending these courses is seen by senior managers as admitting to inadequacies in their knowledge. The message must be promoted that IT is developing so rapidly that it is essential to not only keep up with developments, but be seen to keep up with developments to have credibility with subordinates. Managers should be persuaded to hang their course certificates on their office walls as a badge of honour to show they are keeping up with technology. This way, even if nepotism does lead to unqualified people being appointed to senior positions, the lack of qualifications can, at least, be addressed over time. It would be beneficial to add identification of further training required, incentives to take the training and measures to change attitudes to training as new aspects of the information systems policy framework. These aspects would need a new research programme to ensure the measures taken are tested and effective.

- ii. A strong information security policy statement needs to be created. This then needs to be endorsed by the highest manager, whether or not that manager is knowledgeable in IT. The policy statement then becomes a form of instruction for all levels of management and employees. As the Saudi culture requires precise instructions to be passed from managers to subordinates, it will be important for the policy statement to be as clear, proscriptive and detailed as possible to ensure all employees follow it to the letter. In this respect, the strong hierarchical management culture in Saudi Arabia could be employed to spread the knowledge and awareness of information security that this thesis has shown is needed. This would also mean the encountered problems of the lack of time and motivation of employees to participate in the implementation of the information security policy framework would be reduced or even eliminated.

- iii. A means of auditing the security of an organisation needs to be developed such that it is not seen as a criticism of the management if any problem is found. This could be implemented as a form of self-audit for managers to test their own

systems security and fix any problems without losing face. The use of the self-audit would, of course, have to be specified in the security policy statement.

- iv. A culture of openness needs to be developed. This will be difficult as this is not the normal Saudi approach. To help overcome this, a message must be given that security attacks are inevitable, and that they will become ever more frequent and sophisticated. Therefore, if there are no security attacks reported it can only mean that either the organisation's security is so unimportant that no-one would bother to attack it or that the attacks were not being detected. This would turn the problem of losing face around so that it becomes an advantage. Managers would lose face if they had no attacks to report! An effect of this policy would also be to increase managers' interest in information security which should also enable the information security policy framework to be more easily implemented.

10.5 The success of this PhD Research

This research is considered as the initial step in revealing the cultural problems that affect the information security awareness among all type of information system users in Saudi Arabian knowledge-intensive organisations. While the research has identified the need for future work to extend the investigations, nevertheless, this research has achieved its aims and objectives successfully. There were however, some limitations as in section 10.2, which could be overcome with more time. However, these limitations, (section 10.2) were not critical to the success of the research within the time constraints available for a PhD project.

The research has made a valuable contribution in raising the knowledge of information security among the information systems users at PNU, the case study organisation. A framework has been developed which helps users to play a supporting role in an organisation's information system security and acts as a guideline for information security policies implementation. This research has shown that the information security policy framework can be implemented at an organisation with positive effect. Moreover, the users' contribution in participating in the framework implementation, organising

information security policies, helped raise the information security awareness level among the participants and those that work with them.

This research has produced an information security framework which can be implemented and can increase the information security awareness of those involved. It is, therefore, recommended that PNU, the case study, and Imam University which has ISO27K accreditation, should take the research forward in future years, involving more people in the shaping and updating of the security policy, and for other universities and knowledge intensive organisations in Saudi Arabia to undertake their own framework implementation. The research reported in this thesis has given them the foundation to do so.

References

Abu-Musa, A. 2006. Perceived Security Threats of Computerized Accounting Information Systems in the Egyptian Banking Industry. *Journal of Information Systems*, vol.20, no.1, pp. 187-203. ISSN 08887985.

Abu-Musa, A. 2011. Exploring Information Systems/Technology Outsourcing in Saudi Organisations: An Empirical study. *Journal of Accounting-Business and Management*, vol.18, no.2, pp. 17-73.

Adeyemi-Bello, T. and Kincaid, K.G. 2012. The Impact of Religion and Social Structure on Leading and Organizing in Saudi Arabia, *East Carolina University*.

Al Arabiya News, 2013. Available at:

<https://english.alarabiya.net/en/tools/tags.html?tags=b299fa55-6b75-4852-b143-14e52256951f&tagLabel=saudi%20arabia>. [Accessed: 25 May 2013].

Al-Furaih, I. S. 2002. Internet Regulations, The Saudi Arabian Experience, In Proceeding of The Internet Society's 12th Annual INET Conference, June 18-21, Washington.

AL-Gahtani, S. 2003. Computer Technology Adoption in Saudi Arabia: Correlates of Perceived Innovation Attributes. *Information Technology for Development*, vol.10, no.1, pp. 57. ISSN 02681102.

AL Qahtani, S. 2016. Cyber Crimes Committed by Social Media Users in Saudi Arabia. *ALTamimiand Co*. Riyadh, Saudi Arabia.

Al Hamed, M., Ziadeh, M., Al Oteibi, B., and Mutawalli, N. 2007. *Al Taalim fi AlMamlaka al Arabiya ALSaudia: Rouyat al Hader wa Istishraf al Mustakbal*. 4th ed., Al Rushd Library, Beirut, Lebanon.

Ali, A. J. 1986. Public Managers: Are They Different? A Study of Managerial Belief Systems in Saudi Arabia. *International Review of Administrative Science*, vol.52, pp. 67-79.

Ali, A. J. and Schaupp, D.L. 1992. Value Systems as Predictors of Managerial Decision Styles. *International Journal of Manpower*, vol.13, pp. 19-26.

Al-Lehaibi, M. M. 2001. Faculty Adoption of Internet Technology in Saudi Arabian Universities. School of Information Studies, Florida State University. Doctoral Dissertation.

Almunajjed, M. 2009. Women's Education in Saudi Arabia: The Way Forward. Ideation Center Advance Look, *Booz and Company Inc*. USA.

Al-Saleh, Y. 2004. GRADUATE STUDENTS' INFORMATION NEEDS FROM ELECTRONIC INFORMATION RESOURCES IN SAUDI ARABIA. A Dissertation submitted to the School of Information Studies In partial fulfillment of the Requirements for the degree of Doctor of Philosophy.

- ALshumaim, Y., and ALhuassan, R. 2010. Current Availability and Use of ICT Among Secondary EFL Teacher Saudi Arabia: Possibility and Reality. King Saud University, College of Education – Dept. of Curriculum and Instruction.
- Al-Wehaibi, K., Al-Wabil, A., Alshawi, A. & Alshankity, Z. 2008. Barriers to Internet Adoption among Faculty in Saudi Arabian Universities. In J. Luca & E. Weippl (Eds.), Proceedings of EdMedia: World Conference on Educational Media and Technology, Association for the Advancement of Computing in Education (AACE), pp. 24-33.
- Al-Zarouni, M. 2006. The reality of risks from consented use of USB devices. In Proceedings of the 4th Australian Information Security Conference. School of Computer and Information Science, Edith Cowan University, Perth, Western Australia.
- Atiyyah, H.S. 1991. Effectiveness of Management Training in Arabic Countries. *Journal of Management Development*, vol.10, pp. 22-29.
- Atiyyah, H.S., 1993. Management Development in Arabic Countries: The Challenges of the 1990s. *Journal of Management Development*, vol.12, pp. 3-12.
- Badewi, A. 2013. MIS Research Methodology Course (2) Positivism V.S Interperitivism. Available at: <http://misresearchmethodologies.blogspot.com.br/>. [Accessed: 12 August 2013].
- Ballou, S., 2003. Malicious Code - What Should We Do? SANS Institute. GIAC Security Essentials Certification (GSEC). Practical Version 1.4b.
- Bandaranayake, T., 2012. Understanding Research Philosophies and Approaches. Available at: <https://www.slideshare.net/thusharabandaranayake/understanding-research-philosophies>. [Accessed: 22 September 2014].
- Banks, Simon, 1990. Security Policy. *Computers & Security*, vol.9, pp. 605-610.
- Berg, B. L. 2001. *Qualitative Research Methods for Social Sciences*. 5th Ed. Long Beach, California: Pearson Education Inc.
- Biskup, J., Piero, B. 2004. Controlled Query Evaluation for Enforcing Confidentiality in Complete Information Systems. *International Journal of Information Security*, vol.3, no.1, pp. 14-27. ISSN 16155262. DOI 10.1007/s10207-004-0032-1.
- Blumberg, B., Copper, D.R. and Schindler, P. S. 2005. *Business Research Methods*. Berkshire: McGraw Hill Education.
- Bond, T. 2012. Employee Security Awareness Survey. Admin- Version 1.3. Available at: <http://www.trent.bond@gmail.com>. [Accessed: 15 May 2016].
- Bouma, D. and Atkinson, B. J. G.1996. Social Science Research. *Oxford University Press*.
- BS ISO/IEC 27002, 2005. International Standard. Information Technology-Security Technologies-Code of Practice for Information Security Management. 2nd Edition.2005-06-15. Reference Number ISO/IEC27002:2005.
- Bowles and Hernandez-Castro, 2015. The first 10 Years of the Trojan Horse Defence. *Computer Fraud & Security*, pp. 5-13. University of Kent.

- Bulgurcu, B. Cavusoglu, H. and Benbasat, I. 2010. Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly*, vol.34, no.3, pp. 523-47. ISSN 02767783.
- Burkeman, O., 2012. Online Passwords: Keep it Complicated. *The Guardian*, [Online]. Available at: <https://www.theguardian.com/technology/2012/oct/05/online-security-passwords-tricks-hacking>. [Accessed: 5th October 2012].
- Burney, C. 2003. Roles and Responsibilities of the Information Systems Security Officer. *Data Security Management*, vol.26, no.2, pp. 1. ISSN 10967907.
- Business Dictionary 2016. *Business Dictionary*, [Online]. Available at: <https://businessdictionary.com/definition/procedure.html>. [Accessed: 12 June 2016].
- Caballero, A., 2006. What Does an ISO 9001: 2000 Audit Entail. *Terremark Worldwide, Inc. IAPMO R&T*. East Philadelphia, Ontario California. USA.
- Caballero A. 2010. Information Security Essentials for IT Managers: Protecting Mission-Critical Systems. *Terremark Worldwide Inc.* East Philadelphia, Ontario California. USA.
- Cambridge Advanced Learning's Dictionary 2008. *Cambridge University Press*. 3rd addition, pp. 17. ISSN 978-0521-858045. Edinburgh building, Cambridge. UK.
- Chandra, I. 2008. The Five C's of IT Policy. *Internal Auditor*, vol.65, no.6, pp. 23-24. ISSN 00205745.
- Cisco, 2014. Cisco 2014. Annual Security Report. Americas Headquarters Cisco Systems, Inc. San Jose, CA. pp. 80. Available at: http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf. [Accessed: 5th May 2014].
- CMA, UK Computer Misuse Act. 1990. [online] available at: https://www.legislation.gov.uk/ukpga/1990/18/pdfs/ukpga_19900018_en.pdf. [Accessed: 15 July 2014].
- Collins, 2002. *Collins Thesaurus of the English Language-Complete and Unabridged 2nd Edition*. HarperCollins Publishers.
- Collins, H. 2010. *Creative Research: The Theory and Practice of Research for the Creative Industries*. Lausanne: AVA Publishing SA.
- Collis, J. and Hussey, R. 2003. *Business Research: A Practical Guide for Undergraduate and Postgraduate Students*. 2nd Edition. Basingstoke: Palgrave Macmillan.
- Communicaid Group Ltd., 2013. Doing Business in Saudi Arabia | Saudi Arabian Social and Business Culture. Available at: <http://www.communicaid.com/access/pdf/library/culture/doing-business-in/Doing%20Business%20in%20Saudi%20Arabia.pdf>. [Accessed: 5th August 2013].
- Creswell, J. W. 1994. *Research Design: Qualitative and Quantitative Approaches*. Thousand Oaks, California: SAGE Publications.
- Creswell, J. W. 1995. *Qualitative Inquiry and Research Design: Choose Among Five Traditions*. Thousand Oaks, California: SAGE Publications.

- Creswell, J. W. 2003. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. Thousand Oaks, California: SAGE Publications.
- Crossan, F. 2003. Research Philosophy: Towards an Understanding. *Nurse Researcher*, vol.11. no.1, pp. 46-55.
- Curry, A., and Kadash, N. 2002. Focusing on key elements of TQM- Evaluation for sustainability, *The TQM Magazine*, vol.14, pp. 207-216.
- Dadfar, A., Norberg, R., Helander, E., Schuster, S., & Zufferey, A. 2003. Intercultural Aspects of Doing Business with Saudi Arabia. *Linkoping University, Linkoping*.
- Dadfar, H. 1990. Industrial Buying Behaviour in the Middle East. *Linkoping University, Linkoping*.
- Dalto, J. 2014. How to Create an Effective Training Program: 8 Steps to Success. Convergence Training.
- DeMauro, J. J., and Grottke, T. W. 2008. Filling the Information Security Officer Role within Community Banks. Practical Security Solutions.
- Dhillon, G. and Backhouse J., 2000. Technical Opinion: Information Systems Security in the Management New Millennium. *Communication of the ACM*, vol.43 no.7, pp.125-128.
- Diffie ,Whitfield, 2008. INFORMATION SECURITY:50 YEARS BEHIND, 50 YEARS AHEAD. *COMMUNICATIONS OF THE ACM* , vol.51 no.1, pp. 55-57.
- Dillard, K., Pfost, J., Ryan, S. and Master, C. 2006. Security Risk Management Guide. *Microsoft Corporation*. pp. 83-86. Creative Commons, San Francisco, California, USA.
- Doherty, N.F., Anastasakis, L. and Fulford, H., 2009. The information security policy unpacked: A critical study of the content of university policies. *International Journal of Information Management*, vol.29 no.6, pp. 449-457.
- DPA, UK Data Protection Act. 1998. United Kingdom of Great Britain and Northern Ireland. [online] available at:<http://www.gov.uk/data-protection/the-data-protection-act>. [Accessed: 15 January 2014].
- Durkota, M. D. and Dormann, W. 2008. Recovering From a Trojan of Virus. Carnegie Mellon University.
- Easterby-Smith, M. Thorpe, R. and Lowe, A. 1991. *Management Research: An Introduction*. London: Sage.
- Easterby-Smith, M, Thorpe, R and Lowe, A., 2006. *Management Research: An introduction*, 2nd Edition. *Sage Publications*.
- ENLASO, 2011. Arabic and Bidirectional challenges for translation and software development. White paper. Available at: http://www.enlaso.com/Language_Tech_Center/White_Papers/Arabic_and_Bidirectional_Challenges.aspx. [Accessed: 5th August 2013].
- Ellucian.com, 2012. Available at: <http://www.ellucian.com/emea-ap/Software/Banner-by-Ellucian>. [Accessed: 16 April 2012].

Enisa, 2010. A User Guide: How to Raise Information Security Awareness. *European Network and Information Security Agency*, pp. 64.

F-secure, 2001. White paper: Computer Viruses – from an Annoyance to a Serious Threat. *F-Secure Inc.* 675 N. First Street, 5th floor San Jose, CA 95112, USA.

Fatmax 2007. ICT in Education. Licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 2.5. Administration. Distance Learning.

Frost, D. 2013. Teacher-led development work: a methodology for building professional knowledge. *HertsCam Occasional Papers, HertsCam Publications* [Online]. Available at: <http://www.hertscam.org.uk>. [Accessed: 10 April 2013].

Fischer, A.H. and Manstead, A.S.R., 2000. The relation between gender and emotions in different cultures. In: *Gender and emotion: Social psychological perspectives* A. H. Fischer (ed.), *Cambridge University Press*, pp. 71 – 94.

GAO, 1991. Using Structured Interviewing Techniques. *GAO/PEMD*, vol.10 no.1. United States General Accounting Office, Washington, D.C.

GAO Reports, 2011. INFORMATION SECURITY: Weaknesses Continue Amid New Federal Efforts to Implement Requirements. *GAO Reports*, vol.10 no.3, pp. 1-41.

Garbs, 2013. Livingsocial Under Attack By Hackers, Customers Personal Data Stolen. *ABCNews* [Online]. Available at: <http://abcnews.go.com/WNT/video/livingsocial-attack-hackers-customers-personal-data-stolen-19062684>. [Accessed: Apr 28, 2013 07:16 PM].

GDPR, General Data Protection Regulation, 2018. [Online]. Available at: <http://gov.uk/government/consultations/general-data-protection-regulation-call-for-views>. [Accessed: 20 October 2017].

Geier, E. 2012. Use Sandboxing to Protect Your PC. *PC World*, vol.30, no.4, pp. 84-86. ISSN 07378939.

Gordon, Lawrence A., Martin P. Loeb, William Lucyshyn, and Robert Richardson. 2004. "2004 CSI/FBI Computer Crime and Security Survey," Computer Security Institute 2004. Accessed 20 July 2004 <<http://www.gocsi.com/forms/fbi/pdf.html>>

Glaser, B. G. and Strauss, A. L. 1967. *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Chicago, Aldine.

Grimey, 2013. Clients site hacked by sejeal. *Grimeymedia* [Online]. Available at: <http://blog.grimeymedia.com/clients-site-hacked-by-sejeal/>. [Accessed: 31 January 2013].

Gross, G. 2006. Cisco Plans to Expand Saudi Arabian Presence. *Computerworld*, vol.40, no.17, pp. 20-20. ISSN 00104841.

Guo, K.H., Yuan, Y., Archer, N.P. and Connelly, C.E. 2011. Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model. *Journal of Management Information Systems*, vol.28, no.2, pp. 203-236. ISSN 07421222.

- Herold, R. 2010. *Managing an Information Security and Privacy Awareness and Training Program*. 2nd edition. CRC Press; ISBN-10: 1439815453. ISBN-13: 978-1439815458. LLC, Van Meter, Iowa, USA.
- Hill, John, 2007. Security Management at the University of Denver University College. *Journal of Security Education*, vol.2 no.4, pp. 133-147.
- Hill, C. 2009. *International Business: Competing in the Global Marketplace*. New York, NY: McGraw Hill.
- Hill, D. 2012. *Information Asset Classification Policy*. Computing Services Department. Corporate Services & Facilities Committee (Nov 2012). *CSD Information Security*. v. 1.2.
- Hooper, D. 2011. Feedback, Self-Awareness, and Confidence. *The Houston Home Journal*.
- Höne, K. and Eloff, J.H.P. 2002a. Information Security Policy — what do International Information Security Standards Say? *Computers & Security*, vol.21, no.5, pp. 402-409. ISSN 0167-4048.
- Höne, K. and Eloff, J.H.P. 2002b. What Makes an Effective Information Security Policy? *Network Security*, vol.21, no.6, pp. 14-16. ISSN 1353-4858.
- Hostland, K., Enstad, P.A., Eilertsen, O. and Boe, G. 2010. Information Security Policy Best Practice Document. *UNINRTT led working group on security*. GN3-NA3-T4-UFS126.
- Hu, Q., Xu, Z., Dinev, T. and Ling, H. 2011. Does Deterrence Work in Reducing Information Security Policy Abuse by Employees? *Communications of the ACM*, vol. 54, no. 6, pp. 54. ISSN 0001-0782.
- Humphreys, E. 2010. Information Security Risk Management. Handbook for ISO/IEC 27001. *BSI British Standards Institution*. ISBN 978-580-60745-5.
- Hunt, T. 2011. The Only Secure Password is the One You can't Remember. Password Security. *Lifehacker* [Online]. Available at: <https://lifehacker.com/5785420/the-only-secure-password-is-the-one-you-cant-remember>. [Accessed: 24 March 2013 at 3:25].
- Hussey, J. and Hussey R. 1997. Business Research: A Practical Guide for Undergraduate and Postgraduate Students. *Macmillan Business*. Basingstoke, Palgrave.
- Hyde, K. 2000. Recognising Deductive Processes in Qualitative Research. Qualitative Market Research: *An International Journal*, Vol.3 no.2, pp. 82-90. doi:10.1108/13522750010322089. MCB Up Ltd.
- ImamU website, 2015. Available at: <https://www.imamu.edu.sa/Pages/ISO27001.aspx>. [Accessed: 12 June 2015].
- IPA, 2006. Countermeasures against Bots: Are you sure your computer is not infected with Bot? *Information-technology Promotion Agency IT Security Center*, vol.2-28-8, no.4 Honkomagome, Bunkyo, Tokyo, 113-6591 Japan.
- ISF standard Risk Intelligence Ltd, 2012. ISSA Security Awareness Column July 2012 – Security Induction Sessions. *ISSA Security Journal* [Online]. Available at: <https://www.risk-intelligence.co.uk/issa-security-awareness-column-july-2012-security-induction-sessions/#more-67>. [Accessed: 14 June 2013].

ISO website, 2013a. International Organization for Standardization [online]. Available at: <https://www.iso.org/who-develops-standards.html>. [Accessed: 10 March 2013].

ISO website, 2013b. *International Standard. Information Technology-Security Information Security Management System-Requirements* [online]. Available at: <https://www.iso.org/isoiec-27001-information-security.html>. [Accessed: 10 March 2013].

ISO/IEC 27001, 2005. *International Standard. Information Technology-Security Information Security Management System-Requirements*. Edition.2005-11. Reference Number SN ISO/IEC 27001:2005.

Jait, A. 2011. Government E-Service Delivery Requires Citizens' Awareness: The Case of Brunei Darussalam. PhD Thesis, Loughborough University, Loughborough, United Kingdom.

J.M., Acton and M., Hibbs, 2012 Fukushima Accident 2011. Carnegie Paper. *World Nuclear Association Website*, registered in England and Wales, number 01215741.

Kadam, A.W. 2007. Information Security Policy Development and Implementation. *Information Systems Security*, vol.16, no.5, pp. 246-256. ISSN 1065-898X. DOI 10.1080/10658980701744861.

Kagioglou, K.,Coope, R. Aoud, G. and Sexton, M. 1998. A generic guide to the design and construction process protocol: Final Report. University of Salford, Salford.

Kagioglou, K.,Coope, R. Aoud, G. and Sexton, M. 2000. Rethinking construction: The Genetic Design and Construction Process Protocol. *Engineering Construction and Architectural Management*, vol.7, no.2, pp. 141-153.

Kark, K. 2008. From Chaos to Compliant: Managing your Information Security Polities? *Silicon India Inc.*

Kapp, J. 2000. How to Conduct a Security Audit. *Pc Network Advisor [Online]*. Available at: <http://www.itp-journals.com>. Issue 120, pp. 3-8. [Accessed: 2nd June 2014].

Kasi, P. 2009. *Research: What, Why and How? A Treatise from Researchers to Researchers*. 1st Edition. Bloomington: Author House.

Katadae, A. 2000. Phenomenological Understanding of the Meaning in Lifeworld: Bridging Philosophy and Research Methodology. *Olive Kagawa University Academic Information repository*, pp. 11-19.

Keller, S., Powell, A., Horstmann, B., Predmore C., and Crawford, M. 2005. Information Security Threats and Practices in Small Businesses. *Information Systems Management*, vol.22, no.2, pp. 7-19. ISSN 1058-0530.

Keppel, G. 1991. *Design and Analysis: A Researchers Handbook*. 3rd Edition. New Jersey. Prentice Hall.

Kessler, G. C. 2017. An Overview of Cryptography. Available at: <http://www.garykessler.net/library/crypto.html>. [Accessed: 10 February 2017].

Kohzer, S. Basting, N., and Gutmann, J. 2016. Security in focus. German federal office for information security. *BSI Magazine*, vol. 16, pp. 703-1.

- Knox, K. 2004. A Research's Dilemma-Philosophical and Methodological Pluralism. Nottingham Business School, Trent University. Nottingham, UK.
- Lindlof, T.R. and Taylor, B. C. 2002. *Qualitative communication Research Methods*. 2nd Edition. Thousand Oaks, CA: Sage.
- Laudon, K.C. and Traver, C.G. 2012. *E-commerce 2012 business. technology. society*. Edinburg Gate, Harlow: Pearson.
- Lee, M.,Y. 1998. Dust can do most damage to your computer system. *St. Louise Business Journal*.
- Liang, H., and Xue, Y. 2009. AVOIDANCE OF INFORMATION TECHNOLOGY THREATS: A THEORETICAL PERSPECTIVE. *MIS Quarterly*, vol.33, no.1, pp. 71-89.
- Locke, G. and Gallagher, P. D. 2009. Recommended Security Controls for Federal Information Systems and Organizations, *NIST Special Publication*, pp. 800-53.
- Locke, G. and Gallagher, P. D. 2011. Managing Information Security Risk: Organising, Mission and Information System View. *NIST, National Institute of Standards and Technology/ U.S. Department of Commerce*.
- MacDonald, S. and Headlam, N. 2011. Research Methods Handbook: Introductory Guide to Research Methods for Social Research. *CLES, Express Network*. Manchester, UK.
- Manky, Derek. 2010. Top 10 Vulnerabilities inside the Network. *Network World*, [Online]. Available at: <http://www.networkworld.com/news/tech/2010/110810-network-vulnerabilities.html>. [Accessed: 25 May 2014]
- Mark, M. and Cook, T. 1984. Design of randomized experiments and quasi-experiments, in: L. Rutman (ed.), *Evaluation Research Methods: A Basic Guide* (2nd ed.). Newbury Park, CA: Sage.
- Mccourt, M. 2012. Cloud Computing. *SDM: Security Distributing & Marketing*, 02, vol.42, no.2, pp. 62-70 ISSN 00490016.
- Mirzaei, N., 2008. Cloud computing. Pervasive Technology Institute Report, Community Grids Lab, *Indiana University*, pp.1-12.
- Mohamed, S, F. 2006. Improving Construction Site Management Practices Through Knowledge Management. PhD Thesis, Loughborough University, Loughborough, United Kingdom.
- MS-ISAC, Multi-State Information Sharing and Analysis Center, 2013. Cyber Security Getting Started: Anon Technical Guide. Division of the Center For Internet Security (CSI).
- Mushkhs, H. 2008. Only Ten Saudi Organisations Get the ISO27001 Accreditation in Management information security. Alriyadh [online]. Available at: <http://www.alriyadh.com/348301>. [Accessed: 25 Oct 2017]
- Neuman, W.L. 2006. *Social Research Methods: Qualitative and Quantitative Approaches*. 6th Edition. Pearson Education, Boston.
- Neville, C. 2007. Effective Learning Service: Introduction to Research and Research Methods. University of Bradford School of Management. UK.

Nikzad, N. 2013. *Arabic Translation: The importance of breaking the language barrier*. Available at: <http://www.selfgrowth.com/articles/arabic-translation-the-importance-of-breaking-the-language-barrier>. [Accessed: 5th August 2013].

Orlikowski, W.J. and Baroudi, J.J. 1991. Studying Information Technology in Organizations: Research Approaches and Assumptions. *Information System Research*, vol.2, no.1, pp. 1-28.

Oxford University IS Policy, 2012. Available at: http://www.it.ox.ac.uk/sites/dandy/files/documents/policies/Information_Security_Policy_2012_07-url_edit_2014_10%20rev.pdf. [Accessed: 13 2017].

Oxford Dictionaries, 2013. *Oxford University Press* [Online]. Available at: <http://oxforddictionaries.com/definition/english/barrier>. [Accessed: 01 April 2013].

Oxford Dictionaries, 2014. *Oxford University Press* [Online]. Available at: <http://oxforddictionaries.com/definition/english/barrier>. [Accessed: 14 May 2014].

Oxford Dictionaries, 2015. *Oxford University Press* [Online]. Available July at: <http://oxforddictionaries.com/definition/english/barrier>. [Accessed: 9 July 2015].

Oxford Dictionaries, 2016. *Oxford University Press* [Online]. Available at: <http://oxforddictionaries.com/definition/english/barrier>. [Accessed: 5 June 2016].

Oxford Dictionaries, 2017. *Oxford University Press* [Online]. Available at: <http://oxforddictionaries.com/definition/english/barrier>. [Accessed: 11 August 2017].

Palmer, M., Robinson, C., Patilla, J. and Moser, E. 2006. Information Security Policy Framework: Best Practices for Security Policy in the E-Commerce Age. *Information Systems Security*, vol.10, no.2, pp. 1-15 ISSN 1065-898X.

PC Magazine Encyclopaedia, 2013. Available at: <http://www.pcmag.com/encyclopedia/term/52809/the-computer-glossary>. [Accessed: 10 April 2013].

PC World, 2012. Top 10 Security Suites for 2012. *PC World*, vol. 30, no. 3, pp. 76-77. ISSN 07378939.

Pelnekar, C. 2011. Planning for and Implementing ISO 27001. *ISACA JOURNAL*, vol.4. Texas, USA.

Pfleeger, C.P. and Pfleeger, S.L. 2007. *Security in Computing*. 4th edition. Upper Saddle River, N.J.: Prentice Hall.

PNU website, 2013. Available at: <http://www.pnu.edu.sa/en/University/Pages/Objectives.aspx>. [Accessed: 12 January 2013].

Poore, R. S. 2001. Information Security Standards: Deluge and Dearth. *Information Systems Security*, vol.10, no.1.

Price, I. 2000. Research Methods and Statistics PESS202 Lecture and Commentary Notes. *University of New England, Armidale, NSW, 2351*.

- Puhakainen, P. and Siponen, M. 2010. Improving Employees' Compliance through Information Systems Security Training: An Action Research Study. *MIS Quarterly*, vol.34, no.4, pp. 767-844. ISSN 02767783.
- Rabe, M. 1992. *Kulturella glasogan med svensk syn utomlands*, Göteborg: Tre böcker förlag AB.
- Radack, S. 2012. Conduction Information Security-Related Risk Assessments; Updated Guide for Comprehensive Risk Management Programs. *ITL bulletin*. NIST, National Institute of Standards and Technology/ U.S. Department of Commerce.
- Rajasekar, S., Philominathan, P. and Chinnathambi, V. 2013. RESEARCH METHODOLOGY. [online]. Available at: <https://arxiv.org/pdf/physics/0601009.pdf>. [Accessed: 23 May 2014].
- Remenyi, Dan, William, Brian, Money, Arthur and Swartz, Ethne, 1998. *Doing Research in Business and Management. An Introduction to Process and Method*. London: Sage.
- Rotvold, G. 2008. How to Create a Security Culture in Your Organization. *Information Management Journal*, vol.42, no.6, pp. 32-38. ISSN 15352897.
- Rouse, M. 2013. Hacker. *TechTarget* [Online]. Search Security. Available at: <http://searchsecurity.techtarget.com/definition/hacker>. [Accessed: 23 April 2013].
- Sabbagh, S. 1996. Arab Women: Between Defiance and Restraint, *Olive Branch Press*. Northampton, Mass.
- Sanger, D.E., Barboza, D. and Perloth, N. 2013. Chinese Army Unit Is Seen as Tied to Hacking Against U.S. *New York Times. Business Day Technology*.
- Salton, G. 1980. A Progress Report on Information Privacy and Data Security. *Journal Of the American So city for Information science*. Department of Computer Science, Cornell University, Ithaca, NY.
- SAMA, Ministry of Education. 2008. Statistical Report (1426-27); Al Rajhi Report, p. 374. *Arab News*.
- SANS organisation website 2013. Information Security Resources. Available at: <https://www.sans.org/information-security>. [Accessed: 4 May 2013].
- Saso, 2015. KINGDOM OF SAUDI ARABIA. SAUDI STANDARDS, METROLOGY AND QUALITY. ORGANIZATION. SASO. SAUDI STANDARD. DRAFT No. 30061/2015. Available at: <http://www.saso.gov.sa/ar/about/PublicConsultation/Documents/30061E.pdf>. [Accessed: 20 November 2015].
- Saudi Arabia MCIT website, 2011. Available at: <https://www.saudi.gov.sa/wps/portal/saudi/aboutKingdom/aboutEgovernment>. [Accessed: 16 March 2011].
- Saunders, M. Lewis, P. and Thornhill., 2007. *Research Methods for Business Students*. 4th Edition. London: Financial Times Prentice Hall, Harlow, 624 p.
- Schjolberg, J. S., 2012. Recommendations for potential new global legal mechanisms against global cyberattacks and other global cybercrimes. An International Criminal Tribunal for Cyberspace (ICTC) Prosecution for the Tribunal Police investigation for the Tribunal. 41 pages. *EastWest Institute (EWI) Cybercrime Legal Working Group*. Norway.

Scott, H. and Ives, B., 1982. MIS Research Strategies. *Information management*, vol.5, no.6. pp. 330-347. Elsevier B. V. USA.

Shadish, W. R. 1995. Philosophy of Science and the Quantitative- Qualitative Debates: Thirteen common Errors. *Evaluation and Program Planning*, Vol. 18, No. 1 pp. 63-75. Elsevier Science Ltd. USA.

Shadish, W.R. 2002. Revisiting field experimentation: Field notes for the future. *Psychological Methods*, vol.7, no.1, pp. 3-18.

Shmueli, G. 2009. To Explain or to Predict? Working Paper. *Smith School of Business*. University of Maryland. USA.

Simon, D. and Yaras, D. 2000. *Lagom svenskt*. Stockholm: Bilda forlag.

Siponen, M. and Vance, A. 2010. Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly*, vol. 34, no. 3, pp. 487-A12. ISSN 02767783.

Smith, E. P., Orvos, D. R., and Cairns, J. Jr. 1993. Impact Assessment Using the Before-After-control-Impact (BACI) Model: Concerns and Comments. *Can. J. Fish. Aquat. Sci.*, vol.50.

Smith, K. 2013. Charities Toolkit: A toolkit for effective risk management. *The Institute of Chartered Accountants in England & Wales* [Online]. Available at: <http://www.kingstonsmith.co.uk>. [Accessed: 3 June 2013].

Snyder, J. 2012. Next-Generation firewall (Part2).Application Layer Firewalls: off to a Good Start. *Networkworld* [Online]. Available at: <http://www.networkworld.com>. [Accessed: 7 May 2012].

Son, J. 2011. Out of Fear Or Desire? Toward a Better Understanding of Employees' Motivation to Follow IS Security Policies. *Information & Management*, vol.48, no.7, pp. 296-302. ISSN 0378-7206.

Sotto LJ, Simpson AP. 2014. United States. In: Robertson G (ed) *Data protection & privacy*. *Law Business Research Ltd*, London, pp 208-214

Spears, J.L. and Barki, H., 2010. User Participation in Information Systems Security Risk Management. *MIS Quarterly*, vol. 34, no. 3, pp. 503-A5. ISSN 02767783.

The Uslegal website, 2013. Available at: <https://definitions.uslegal.com/g/grey-hat-hacker>. [Accessed: 2nd December 2013].

Titchen, A. and Hobson, D., 2005. Phenomenology. In Somekh, Bridget and Cathy Lewin (eds.) *Research Methods in the Social Science*, pp 121-130. New Delhi:Sage.

Tracy, R.P., 2007. IT Security Management and Business Process Automation: Challenges, Approaches, and Rewards. *Information Systems Security*, vol.16, no.2, pp. 114-122. ISSN 1065-898X. DOI 10.1080/10658980601051706.

Trčcek, Denis Trobec, Roman Pavešić, Nikola Tasić, J. F. 2007. Information Systems Security and Human Behaviour. *Behaviour & Information Technology*, vol. 26, no. 2, pp. 113-118. ISSN 0144929X. DOI 10.1080/01449290500330299.

Turban, E., King, D. and Lee, J. 2010. *Electronic Commerce 2010*. Upper Saddle River, N.J. Pearson.

Tuban, E., Volonino, L. and Wood, G. R. 2013. *Information Technology for Management: Advancing Sustainable, Profitable Business Growth*, 9th ed. New York: John Wiley and Sons Inc.

Uc Davis website, 2011. UC Davis Student Information System (SIS), Banner. Available at: <https://www.ucdavis.edu/>. [Accessed: 6th March 2013].

Vance, A., Siponen, M. and Pahlila, S. 2012. Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory. *Information & Management*, vol. 49, no. 3-4, pp. 190-198. ISSN 0378-7206.

Veiga, A.D. and Eloff, J.H.P. 2007. An Information Security Governance Framework. *Information Systems Management*, 10/02; 2012/08, vol. 24, no. 4, pp. 361-372 ISSN 1058-0530. DOI 10.1080/10580530701586136.

Vijayan, J., 2005. Targeting the Enemy within. *Computer World*, vol.39, no.32, pp.23-27.

Vijayan, J., 2012. Saudi Aramco hacked; company confirms disruption: Attacks Come as Security Firms warn of Shamoon Malware Targeted at Energy Firms. *Computerworld* [online]. Available at: <http://www.computerworld.com/article/2506020/cybercrime-hacking/saudi-aramco-hacked--company-confirms-disruption.html>. [Accessed: Aug 17, 2012 4:53 PM PT].

Viteritti, J.P. 1978. Implementing Change through Training--a Case Study. *Public Administration Review*, vol.38, no.5, pp. 469-475. ISSN 00333352.

Wageman, R. 2007. Senior Leadership Teams: What It Takes to Make Them Great. Hay Group [online]. Available at: http://www.haygroup.com/Downloads/it/misc/Top_Teams_Presentation.pdf. [Accessed:17 May 2015].

White, G. 2009. Strategic, Tactical, & Operational Management Security Model. *Journal of Computer Information Systems*, Spring2009, vol. 49, no. 3, pp. 71-75 ISSN 08874417.

Wipro website, 2012. Wipro annual report. Available at: <http://www.wipro.com/documents/investors/pdf-files/Wipro-annual-report-2012-13.pdf>. [Accessed: 11 April 2012].

Wright, G. S. 2007. A Taxonomy of Information Systems Audits, Assessments and Reviews: GIAC Systems and Network Auditor. (*GSNA*) *Auditing Networks, Perimeters & Systems*, AUD-507 Gold Certification. SANS Institute.

Wylder, J.O. 2003. Improving Security from the Ground Up. *Information Systems Security*, vol.11, no.6, pp. 29-38. ISSN 1065-898X. DOI 10.1201/1086/43324.11.6.20030101/40429.6.

Wyman CE, Balan V, Dale BE, Elander RT, Falls M, Hames B, Holtzapple, M. T. Ladisch M. R., Lee Y.Y., Mosier N., Pallapolu V. R., Shi J., Thomas S. R., Warner R.E. 2011. Comparative data of effects of leading pretreatments and enzyme loadings and formulations on sugar yields from different switchgrass sources. *Bioresour Technol*, vol.102, no.4, pp. 11052-62.

- Xiao-yan, GE, Yu-qing ,Yuan and Li-lei, L. 2011. An Information Security Maturity Evaluation Mode. *Procedia Engineering*, vol.2, pp. 335 – 339.
- Yesser website, 2014. Available at: <http://www.yesser.gov.sa/EN/Pages/Sitemap.aspx>. [Accessed: 20 July 2014].
- Yildirima, Y., E., Akalp, G., Aytac, S. and Bayram, N. 2010. Factors Influencing Information Security Management in Small- and Medium-Sized Enterprises: A Case Study from Turkey. *International Journal of Information Management*, vol.31, no.4, pp. 360-365. ISSN 0268-4012.
- Yin, R. K., 1984. *Case Study Research: Design and Methods*. Beverly Hills, CA: Sage Publication.
- Yin, R. K., 1993. *Case Study Research: Design and Methods*: 1st Edition. Newbury Park: Sage Publication.
- Yin, R. K., 1994. *Case Study Research: Design and Methods*: 2nd Edition. Newbury Park: Sage Publication.
- Zainal, Z., 2007. Case Study as a Research Method. University Teknologi. *Malaysia Journal Kemanusiaan Bil.9*. Malaysia.

Appendix A

Surveys and interviews Questionnaires

Survey 1

Initial Information Gathering Questionnaire Princess Nora University

(For non-IT employees)

The purpose of this questionnaire is to help gather information in relation to the use of Information Technology (IT) systems at PNU. The findings from this questionnaire will help to improve facilities at PNU therefore your assistance is greatly appreciated in the participation.

Please note: No personal information is sought and all information is submitted anonymously.

1. **Gender**
 - a. Male
 - b. Female

2. **Age Group:**
 - a. Under 20
 - b. 21 – 25
 - c. 26 – 34
 - d. 35 – 40
 - e. 41 – 45
 - f. 46 – 50
 - g. 51 +

3. **What is your highest qualification:**
 - a. High School
 - b. Bachelor degree
 - c. Master degree
 - d. PhD degree

4. **Do you have IT related qualification at undergraduate/ postgraduate level?**
 - a. Yes
 - b. No

5. **Have you attended any IT related training courses?**
 - a. No

- b. Yes (1 Course)
- c. Yes (1 – 3 Courses)
- d. Yes (3 or more)

6. Position held at PNU:

- a. Support Staff / Administration
- b. IT Support Staff
- c. Management
- d. Academic / Lecturer
- e. Student

7. Which of the tasks below do you perform whilst at the University? Tick where appropriate:

- a. Typing
- b. Data Entry
- c. Administration of Data
- d. Academic Research
- e. Communication
- f. General Secretarial
- g. Computer Maintenance
- h. System Development / Programming
- i. Management

8. Which of the University's computer systems do you use?

- a. Banner
- b. Don't Know
- c. Other _____

9. Do you often face problems when using the University's computer systems?

- a. Yes
- b. No

10. Please list and rate (1-5) any problems that you have faced in the past month:
(1 = Nominal Problem 5 = Significant Problem)

11.

problem	Severity (1-5)

12. When dealing with IT related tasks, do you consider yourself someone more likely to have to help others, or to ask for help yourself?"

- a. Ask for Help
- b. Help Others

13. On a scale of 1 – 5 how computer literate do you see yourself?

(1 illiterate / 5 very literate)

- a. _____

14. Do you feel the IT systems at PNU are difficult to use?

- a. Strongly disagree
- b. Disagree
- c. Neither agree nor disagree
- d. Agree
- e. Strongly agree

15. Which parts of the current IT systems do you find the most difficulty with?

- a. _____
- b. _____
- c. _____
- d. _____
- e. _____

16. How many passwords do you use to access the various IT systems at PNU?

- a. 1
- b. 2
- c. 3
- d. 4
- e. 5 or more

17. If you would like to add any additional information in relation to using the IT facilities at PNU please write them below:

Thank you for taking the time to complete this questionnaire, your responses will help to significantly improve facilities at the University. If you are interested in helping further with this research please enter your email or telephone number here: _____

Survey 2

Initial Information Gathering Questionnaire Princess Nora University

(IT DEPARTMENT)

The purpose of this questionnaire is to help gather information in relation to the use of current computer information systems at PNU. The findings from this questionnaire will help to improve facilities at PNU therefore your assistance is greatly appreciated in the participation.

Please note: No personal information is sought and all information is submitted anonymously.

1. Gender

- a. Male
- b. Female

2. Age Group:

- a. Under 20
- b. 21 – 25
- c. 26 – 34
- d. 35 – 40
- e. 41 – 45
- f. 46 – 50
- g. 51 +

3. What is your highest qualifications:

- a. High School
- b. Bachelor degree
- c. Master degree
- d. PhD degree

4. Is your education IT related?

- a. Yes
- b. No

5. Please list the main subject for your following qualifications:

- a. Undergraduate (Bachelors) : _____
- b. Postgraduate (Masters): _____

- c. PhD (Doctorate): _____
6. Have you attended any IT related training courses?
- No
 - Yes (1 Course)
 - Yes (1 – 3 Courses)
 - Yes (3 or more)
7. Position held at PNU:
- IT Support Staff
 - IT Management
 - Other _____
8. Which of the tasks below do you perform whilst at the University? Tick where appropriate:
- Typing
 - Data Entry
 - Administration of Data
 - Computer Maintenance
 - System Development / Programming
 - IT Management
 - Other _____
9. Which of the University's computer systems do you use (please list)?
- Banner
 - Don't Know
 - Other 1 _____
 - Other 2 _____
 - Other 3 _____
 - Other 4 _____
10. Do you often face problems when using the University's computer systems?
- Yes
 - No

- 11. Please list and rate (1-5) any problems that you have faced in the past month:
(1 = Nominal Problem 5 = Significant Problem)**

problem	Severity (1-5)

- 12. Do you find yourself asking others for help, or helping others?**

- a. Ask for Help
- b. Help Others

- 13. On a scale of 1 – 5 how computer literate do you see yourself?**

(1 illiterate / 5 very literate/expert)

- a. _____

- 14. Do you feel the IT systems at PNU are difficult to use?**

- a. Strongly disagree
- b. Disagree
- c. Neither agree nor disagree
- d. Agree
- e. Strongly agree

- 15. Which parts of the current IT systems do you find the most difficulty with?**

- a. _____
- b. _____
- c. _____
- d. _____
- e. _____

- 16. How many passwords do you use to access the various IT systems at PNU?**

- a. 1
- b. 2
- c. 3
- d. 4
- e. 5+

17. PNU mainly uses the Banner collection of software solutions. Using these systems is difficult, do you:

- a. Strongly disagree
- b. Disagree
- c. Neither agree nor disagree
- d. Agree
- e. Strongly agree

18. How much training on the banner systems have you received?

- a. None
- b. A little
- c. Average
- d. A lot
- e. Too much

19. Have you found this training to be beneficial?

- a. Yes
- b. No
- c. Somewhat

20. If you have found some training very useful and other training not useful please give details below:

21. What do you see the solution being to improve the computer systems at PNU

(Multiple Selection):

- a. Change of system
- b. More IT staff
- c. More training for non-technical staff
- d. Modification of current systems
- e. More funding
- f. Other _____

22. Which other software at the University do you utilise:

- a. _____
- b. _____
- c. _____
- d. _____

23. Do you face any difficulties with this software? If so please provide details below:

24. How much external support does PNU currently utilise for the current information systems:

- a. Daily Support
- b. Weekly Support
- c. Monthly Support
- d. Other _____

25. Do you feel the current IT department is managed correctly?

- a. Strongly disagree
- b. Disagree
- c. Neither agree nor disagree
- d. Agree
- e. Strongly agree

26. What changes would you like to see in the IT department?

27. What are the common problems faced by employees in your opinion?

- a. _____
- b. _____
- c. _____
- d. _____
- e. _____
- f. _____

28. How secure do you feel the current computer systems are at PNU?

- a. Very Secure
- b. Secure
- c. Somewhat Secure
- d. Not secure

29. Please list any security concerns you have for the software systems at PNU:

30. If you would like to add any additional information in relation to using the IT facilities at PNU please write them below:

Thank you for taking the time to complete this questionnaire, your responses will help to significantly improve facilities at the University. If you are interested in helping further with this research please enter your email or telephone number here: _____

Interviews

Three areas of interview questionnaires

The purpose of this interview is to help gather information in relation to the use of current computer information systems at PNU. The findings from this interview will help to improve facilities at PNU therefore your assistance is greatly appreciated in the participation.

Checking the vulnerability of the information security:

- 1- Are your employees aware of the importance of the information they are handling?
- 2- Are you aware of the risk of losing the origination information due to the weakness of the information security system?
- 3- Where do you think the weakness in the university information security system?
- 4- Does the university implement and develop detection, prevention, and recovery controls to make sure that their information is protected against any risk and malicious attack?
- 5- Do you have a backup policy?
- 6- Do you regularly back up and test the organisation information and software according to the agreed backup policy?
- 7- In what timescale could services or data be?
- 8- How often does your information system receive malicious attack, and how do they monitor it?
- 9- When is the last time you have a security attach, and what kind was it?
- 10- How are attempted/actual security breaches monitored and documented?
- 11- How do you minimize the risk of theft, fraud, or misuse of computers facilities?
- 12- Do you have any kind of physical protection against natural disasters such as fire, flood earthquake explosion?

- 13- Do you carry out annual auditing, monitoring, and evaluating activities to verify information security program effectiveness?

Checking employee and user awareness:

- 1- Do you make sure that employee understand their responsibility before you hire them?
- 2- Do you make sure that users understand their responsibility before they use the information system?
- 3- Does employment contract explain what will be done if the employee neglect and misuse the organisation information security requirement?
- 4- Do you use contractual term and conditions to make sure that all employees and users agree to comply with the organisation information security restrictions and obligation?
- 5- Do you use contractual term and conditions to show employees and users how they are expected to handle and help control the organisation information service?
- 6- Do you have a clear documented information security policy that fit the organisation's security roles and responsibilities?
- 7- Do all employees and users get a copy of the organisational information security policy?
- 8- Are all employees and users aware of the organisation's information security restrictions and obligation?
- 9- Are you and all employees aware of cyber law and regulation?
- 10- Do you have policies that explain to the user the punishment if they mishandle information?

Checking training program:

- 1- What do you think is the best method to educate employees and users about the security of the information?

- 2- Are employees getting effectively trained and receiving awareness?
- 3- Do you have adequate and effective awareness and training at all levels of the organisation?
- 4- Does the organisation verify that the desired results from training occur?
- 5- What kind of measures that the origination uses to verify the effectiveness of the training programs?
- 6- Does the organization update the education program to improve communications and to get the right message out to personnel?

Thank you for taking the time to complete this questionnaire, your responses will help to significantly improve facilities at the University.

Survey 3

ISO Interview questionnaires

The purpose of this interview is to help gather information in relation to the security of information. The findings from this interview will help to improve information security awareness in Saudi Arabian organisations; therefore your assistance is greatly appreciated in the participation.

1. Has your organisation got, or is it in the process of getting ISO 27k accreditation?

Yes

No

2. What steps did you follow to get ISO 27k accreditation?

3. How did you choose your ISO 27k team members?

- **Education degree**

Bachelor degree

Master degree

PhD degree

- **Skills that you perceive to be important in choosing those to be involved in the audit**

- **Position held**

IT Administration

IT Support Staff

Management

Academic staff

Student

4. Did representatives of all types of user play a part in your ISO 27k team?

Yes

No

5. Were there any academic users in the ISO 27k team?

Yes

No

6. Were there any administrative users in the ISO 27k team?

Yes

No

7. Were there any student users in the ISO 27k team?

Yes

No

8. What proportion of all types of user participant were there in the ISO 27k team?

9. What proportion of female participants were there in the ISO 27k team?

10. Do you believe that the users chosen for the team were appropriate, if not why not?

11. Is all type of users, employees and students knew that there had been ISO accreditation? If so, how many of them have any idea what ISO accreditation is?

12. In your opinion, are most of the organisation, including all type of users, employees and students, more aware of the importance of the IT security after getting the ISO 27k accreditation?

13. How does your organisation ensure information security awareness among employees?

Thank you for taking the time to complete this questionnaire, your responses will help to significantly improve the information security awareness in Saudi Arabian organisations.

Survey 4

Prior and Post Assessment

Employee security awareness Questionnaire

The purpose of this questionnaire is to help gather information to measure the level of the Information security awareness among all type of university female employees. The findings from this questionnaire will help to improve the security awareness therefore your assistance is greatly appreciated in the participation.

Personal question:

1. What is your position within the university?
 - a. Management
 - b. Support Staff
 - c. Academic / Lecturer
 - d. Student
 - e. Other, please specify:

Personal computer security questions:

2. How secure do you feel your computer is?
 - a. Very secure
 - b. Secure
 - c. Not secure
 - d. I do not know how secure it is
3. Is the firewall on your computer enabled?
 - a. Yes, it is enabled.
 - b. No, it is not enabled.
 - c. I know what a firewall is but I do not know if it is enabled.
 - d. I do not know what a firewall is.
4. Is anti-virus software currently installed, updated and enabled on your computer?
 - a. Yes it is.
 - b. No it is not.
 - c. I do not know how to tell.
 - d. I do not know what anti-virus software is.

5. Do you know what an email scam is and how to identify one?
- Yes I do.
 - No, I know what an email scam is but I don't know how to identify one
 - No, I do not know what an email scam is.

University security policy questions:

6. Does the university have policies available on which websites you can access relating to website security?
- No, there are no policies, I can visit whatever websites I want while at work.
 - Yes, there are policies limiting what websites I can and cannot visit while at work, but I do not know the policies.
 - Yes, there are policies and I know and understand them.
7. Does the university have policies on how and what you can and cannot use email for?
- No, there are no policies, I can send whatever emails I want to whomever I want while at work.
 - Yes, there are policies limiting what emails I can and cannot send while at work, but I do not know the policies.
 - Yes, there are policies and I know and understand them.
 - I do not know if there are any policies on what I can use email for.
8. Is instant messaging allowed in your university?
- Yes, I can use it with anyone.
 - Yes, but I can only use it with other university employees
 - No, instant messaging is not allowed.
 - I do not know.
9. Can you use your own personal devices, such as your mobile phone, to store or transfer confidential university information
- Yes I can.
 - No I cannot.
 - I do not know.

User knowledge and security awareness questions:

10. Does the university have an information security team?
- Yes, we have an information security team.
 - No, we do not have an information security team.
 - I do not know.

11. Do you know who to contact in case you are hacked or if your computer is infected?
 - a. Yes, I know who to contact.
 - b. No, I do not know who to contact.

12. Do you know how to tell if your computer is hacked or infected?
 - a. Yes, I know.
 - b. No, I do not know.

13. How careful are you when you open an attachment in email?
 - a. I do not open attachments.
 - b. I always make sure it is from a person I know and I am expecting the email.
 - c. As long as I know the person or company that sent me the attachment I open it.
 - d. There is nothing wrong with opening attachments.

14. Do you know what an email phishing attack is?
 - a. Yes, I do.
 - b. No, I do not.

15. Do you think that your computer has no value to hackers, so no one would target it?
 - a. Yes I do.
 - b. No, I do not

16. If you delete a file from your computer or USB stick, that information can no longer be recovered.
 - a. True
 - b. False
 - c. I don't know

User experience questions:

17. Have you ever found a virus on your computer at work?
 - a. Yes, it has been infected before.
 - b. No, it has never been infected.
 - c. I know what a virus is but I do not know if it has ever been infected.
 - d. I do not know what a virus is.

18. Have you ever given your work password to a co-worker or someone else?
 - a. Yes
 - b. No

19. Has your manager or anyone else you know at work ever asked you for your password?
- Yes, they have
 - No, they have not.

User security practise questions:

20. Is your computer configured for the security to be automatically updated?
- Yes, it is.
 - No, it is not.
 - I do not know.
21. Have you downloaded and installed software on your computer at work?
- Yes I have.
 - No I have not.
22. Do you use the same passwords for your work accounts as you do for your personal accounts at home, such as Facebook, Twitter or your personal email accounts?
- Yes I do for many personal accounts.
 - Yes I do, but only for the following accounts:
 - No I do not.
22. How often do you take information from work and use your computer at home to work on it?
- Almost every day.
 - At least once a week.
 - At least once a month.
 - Never
23. Have you logged into work accounts using public computers, such as from a library, cyber cafe or hotel lobby?
- Yes, I have done so many times.
 - Yes, but only on rare occasions
 - No, I have never done so.

Thank you for taking the time to complete this questionnaire, your responses will help to significantly improve facilities at the University. If you are interested in helping further with this research please enter your email or telephone number here: _____

Appendix B

Sample of Interview Responses

Dr Ghazi interview

Three areas of interview questionnaires

The purpose of this interview is to help gather information in relation to the use of current computer information systems at PNU. The findings from this interview will help to improve facilities at PNU therefore your assistance is greatly appreciated in the participation.

Checking the vulnerability of the information security:

1- Are your employees aware of the importance of the information they are handling?

Yes, they are

2- Are you aware of the risk of losing the origination information due to the weakness of the information security system?

Yes, we are

3- Where do you think the weakness in the university information security system?

None

4- Does the university implement and develop detection, prevention, and recovery controls to make sure that their information is protected against any risk and malicious attack?

Yes, it does

5- Do you have a backup policy? Yes, we do

6- Do you regularly back up and test the organisation information and software according to the agreed backup policy? Yes, we do

7- In what timescale could services or data be? (I am not getting what you mean)

- 8- How often does your information system receive malicious attack, and how do they monitor it? **Every day, different solutions and techniques**
- 9- When is the last time you have a security attack, and what kind was it? **DDoS**
- 10- How are attempted/actual securities breaches monitored and documented? **By different solutions and techniques s**
- 11- How do you minimize the risk of theft, fraud, or misuse of computers facilities?
Awareness, training and policy enforcement
- 12- Do you have any kind of physical protection against natural disasters such as fire, flood earthquake explosion?
Yes, we do
- 13- Do you carry out annual auditing, monitoring, and evaluating activities to verify information security program effectiveness?
Planned to do so

Checking employee and user awareness:

- 1- Do you make sure that employee understand their responsibility before you hire them? **Yes, we do**
- 2- Do you make sure that users understand their responsibility before they use the information system? **Yes we do**
- 3- Does employment contract explain what will be done if the employee neglect and misuse the organisation information security requirement? **Yes, they are aware of the policies**
- 4- Do you use contractual term and conditions to make sure that all employees and users agree to comply with the organisation information security restrictions and obligation? **Yes, we do**

- 5- Do you use contractual term and conditions to show employees and users how they are expected to handle and help control the organisation information service?

Yes, we do

- 6- Do you have a clear documented information security policy that fit the organisation's security roles and responsibilities?

Yes, we do

- 7- Do all employees and users get a copy of the organisational information security policy?

Yes

- 8- Are all employees and users aware of the organisation's information security restrictions and obligation? Yes

- 9- Are you and all employees aware of cyber law and regulation? Some of them

- 10- Do you have policies that explain to the user the punishment if they mishandle information? Yes,

Checking training program:

- 1- What do you think is the best method to educate employees and users about the security of the information? (am not getting what you mean)

- 2- Are employees getting effectively trained and receiving awareness? (partially)

- 3- Do you have adequate and effective awareness and training at all levels of the organisation? partially)

- 4- Does the organisation verify that the desired results from training occur? Planned to do so

- 5- What kind of measures that the origination uses to verify the effectiveness of the training programs? (test, survey)

- 6- Does the organization update the education program to improve communications and to get the right message out to personnel? **None**

Thank you for taking the time to complete this questionnaire, your responses will help to significantly improve facilities at the University.

ISO Interview with the manager of the information security at PUN Sami Alanzi

مقابلة شخصية PNU

ان هدف هذه المقابلة الشخصية هو المساعدة فى جمع البيانات المتعلقة بأمن المعلومات. ستساعد نتائج هذه المقابلة فى تنمية الوعى بأمن المعلومات فى المؤسسات فى المملكة العربية السعودية و لهذا فإننا نقدر مشاركتك و مساعدتك:

1- هل حصلت مؤسستك على شهادة، أو فى طريقها للحصول عليها ISO 27k؟

■ نعم in the process of getting it

■ لا

2- ما هى الخطوات التى اتبعتها للحصول على ISO 27k؟

Complete execution plan has been prepared starting gap analysis, then fulfilling whatever gap found, then recheck (redo gap analysis) then plan & do internal audit and finally continual improve the maturity

3- كيف تم اختيار اعضاء فريق ISO 27k الخاص بالمؤسسة التعليمية التى تعمل لديها؟

- الدرجة العلمية

■ درجة البكالوريوس

■ درجة الماجستير

■ درجة الدكتوراه

- المهارات التى تشعر انها مهمة فى اختيار من يقومون بمراجعة الحسابات

- المنصب

■ ادارة تكنولوجيا المعلومات

■ فريق دعم تكنولوجيا المعلومات

■ الإدارة

■ فريق اكاديمى

■ طالب

4- هل لعب ممثلى المستخدمون من مختلف الأنواع دورا فى فريق ISO 27k الخاص بك؟

■ نعم

■ لا

5- هل هناك الأكاديميين فى فريق ISO 27k؟

- نعم
- لا

6- هل يوجد اداريين فى فريق ISO 27k؟

- نعم
- لا

7- هل كان هناك من الطلاب فى فريق ISO27k؟

- نعم
- لا

8- ماهى نسبة جميع انواع المستخدمين من الموظفين و الطلاب المشاركة فى فريق ISO27k ؟

0% academics and 0% students

9- ماهى نسبة المشاركين من الإناث فى فريق ISO27k؟

لا يوجد

10- هل تعتقد بأن المستخدمين من الموظفين و الطلاب الذين تم اختيارهم للفريق مناسبين ، و اذا كانت الإجابة (لا) فلماذا؟

نعم

11- هل جميع المستخدمين من الموظفين و الطلاب علموا بأن المؤسسة تسعى للحصول ؟ و اذا كانت الإجابة بنعم، فكم عدد الذين كان لديهم فكرة عن ماهية ISO27k على شهادة منهم؟ ISO27k شهادة

no

12- فى رأيك، هل معظم المؤسسات التى تتضمن جميع انواع المستخدمين ، من الموظفين ISO او الطلاب، اكثر وعيا بأهمية تأمين تكنولوجيا المعلومات بعد الحصول على شهادة 27k ؟

نعم

13- كيف تقوم مؤسستك بالتأكد من وعى موظفيها بتأمين المعلومات؟

as per the security incident number and compliance level among users

نشكركم على وقتكم الذى منحتموه لأكمال هذا الإستبيان، فإجاباتكم ستساعد فى تنمية الوعى فى مجال أمن المعلومات مساعدة كبيرة داخل مؤسسات المملكة العربية السعودية

ISO interview with Imam University information security management

مقابلة شخصية

ان هدف هذه المقابلة الشخصية هو المساعدة فى جمع البيانات المتعلقة بأمن المعلومات. ستساعد نتائج هذه المقابلة فى تنمية الوعى بأمن المعلومات فى المؤسسات فى المملكة العربية السعودية و لهذا فإننا نقدر مشاركتك و مساعدتك:

1- هل حصلت مؤسستك على شهادة، أو فى طريقها للحصول عليها ISO 27k؟

- نعم
- لا

2- ما هى الخطوات التى اتبعتها للحصول على ISO 27k؟

(على أربع مراحل ISMS بتطوير نظام أمن المعلومات (ISO 27k) تم الحصول على مستمرة و معتمدة وهي:

- التخطيط
- التنفيذ
- التأكد
- المراجعة

3- كيف تم اختيار اعضاء فريق ISO 27k الخاص بالمؤسسة التعليمية التى تعمل لديها؟

- الدرجة العلمية
 - درجة البكالوريوس
 - درجة الماجستير
 - درجة الدكتوراه
- المهارات التى تشعر انها مهمة فى اختيار من يقومون بمراجعة الحسابات
- المنصب
 - ادارة تكنولوجيا المعلومات
 - فريق دعم تكنولوجيا المعلومات

- الإدارة
- فريق أكاديمى
- طالب

4- هل لعب ممثلى المستخدمين من مختلف الأنواع دورا فى فريق ISO 27k الخاص بك؟

- نعم
- لا

5- هل هناك الأكاديميين فى فريق ISO 27k؟

- نعم
- لا

6- هل يوجد اداريين فى فريق ISO 27k؟

- نعم
- لا

7- هل كان هناك من الطلاب فى فريق ISO27k؟

- نعم
- لا

8- ماهى نسبة جميع انواع المستخدمين من الموظفين و الطلاب المشاركة فى فريق ISO27k ؟

الموظفين: حوالي 70%

أعضاء هيئة التدريس: حوالي 30%

9- ماهى نسبة المشاركين من الإناث فى فريق ISO27k؟

كان هناك دور (غير مباشر) لموظفات تقنية المعلومات لبعض متطلبات شعادة الأيزو و أنظمة حماية أجهزة الموظفين. , مثل التوعية الأمنية ISO27001:2013

10- هل تعتقد بأن المستخدمين من الموظفين و الطلاب الذين تم اختيارهم للفريق مناسبين ، و اذا كانت الإجابة (لا) فلماذا؟

أما الفريق المشارك فتم اختيارهم و ترتيب اجتماعات مجدولة قبل البدء وحتى نعم. الحصول على الشهادة

11- هل جميع المستخدمين من الموظفين و الطلاب علموا بأن المؤسسة تسعى للحصول ؟ و اذا كانت الإجابة بنعم، فكم عدد الذين كان لديهم فكرة عن ماهية ISO27k على شهادة منهم؟ ISO27k شهادة

تم إعلام جميع منسوبي الجامعة بعد الحصول على الشهادة (حوالي 14 ألف موظف وعضو هيئة تدريس).

12- فى رأيك، هل معظم المؤسسات التى تتضمن جميع انواع المستخدمين ، من الموظفين ISO او الطلاب، اكثر و عيا بأهمية تأمين تكنولوجيا المعلومات بعد الحصول على شهادة 27k ؟

بالطبع أصبحوا أكثر وعي، خاصة بعد تدشين مشروع برنامج التوعية بأمن المعلومات باستخدام قنوات و وسائل مختلفة.

13- كيف تقوم مؤسستك بالتأكد من وعى موظفيها بتأمين المعلومات؟

تدشين مشروع برنامج التوعية بأمن المعلومات. المشروع مستمر طوال السنة ويستخدم قنوات و وسائل مختلفة ويخدم جميع منسوبي الجامعة من موظفين وأعضاء هيئة تدريس وكذلك طلاب، رابط البرنامج:

<https://infosec-aware.imamu.edu.sa>

نشكركم على وقتكم الذى منحتموه لأكمال هذا الإستبيان، فإجاباتكم ستساعد فى تنمية الوعى فى مجال أمن المعلومات مساعدة كبيرة داخل مؤسسات المملكة العربية السعودية

Translation of the two ISO interviews

PNU Interview

The purpose of this interview is to help gather information in relation to the security of information. The findings from this interview will help to improve information security awareness in Saudi Arabian organisations; therefore your assistance is greatly appreciated in the participation.

1. Has your organisation got, or is it in the process of getting ISO 27k accreditation?

Yes in the process of getting it

No

2. What steps did you follow to get ISO 27k accreditation?

Complete execution plan has been prepared starting gap analysis, then fulfilling whatever gap found, then recheck (redo gap analysis) then plan & do internal audit and finally continual improve the maturity

3. How did you choose your ISO 27k team members?

- **Education degree**

Bachelor degree

Master degree

PhD degree

- **Skills that you perceive to be important in choosing those to be involved in the audit**

- **Position held**

IT Administration

IT Support Staff

Management

Academic staff

Student

4. Did representatives of all types of user play a part in your ISO 27k team?

Yes

No

5. Were there any academic users in the ISO 27k team?

Yes

No

6. Were there any administrative users in the ISO 27k team?

Yes

No

7. Were there any student users in the ISO 27k team?

Yes

No

8. What proportion of all types of user participant were there in the ISO 27k team?

0% academics and 0% students

9. What proportion of female participants were there in the ISO 27k team?

non

10. Do you believe that the users chosen for the team were appropriate, if not why not?

yes

11. Is all type of users, employees and students knew that there had been ISO accreditation? If so, how many of them have any idea what ISO accreditation is?

no

12. In your opinion, are most of the organisation, including all type of users, employees and students, more aware of the importance of the IT security after getting the ISO 27k accreditation?

yes

13. How does your organisation ensure information security awareness among employees?

as per the security incident number and compliance level among users

Thank you for taking the time to complete this questionnaire, your responses will help to significantly improve the information security awareness in Saudi Arabian organisations.

Imam ISO Interview

The purpose of this interview is to help gather information in relation to the security of information. The findings from this interview will help to improve information security awareness in Saudi Arabian organisations; therefore your assistance is greatly appreciated in the participation.

14. Has your organisation got, or is it in the process of getting ISO 27k accreditation?

Yes

No

15. What steps did you follow to get ISO 27k accreditation?

Developing information security system (ISMS) in four continuous stages:

- Plan
- Do
- Check
- Act

16. How did you choose your ISO 27k team members?

- Education degree

Bachelor degree

Master degree

PhD degree

- Skills that you perceive to be important in choosing those to be involved in the audit

- Position held

IT Administration

IT Support Staff

Management

Academic staff

Student

17. Did representatives of all types of user play a part in your ISO 27k team?

Yes

No

18. Were there any academic users in the ISO 27k team?

Yes

No

19. Were there any administrative users in the ISO 27k team?

Yes

No

20. Were there any student users in the ISO 27k team?

Yes

No

21. What proportion of all types of user participant were there in the ISO 27k team?

70% administrators and staff

30% academic

22. What proportion of female participants were there in the ISO 27k team?

Indirect participation of IT female staff as part of the awareness program

23. Do you believe that the users chosen for the team were appropriate, if not why not?

yes, the team members were chosen and arranged scheduled meetings before starting getting ISO27k accreditation

24. Is all type of users, employees and students knew that there had been ISO accreditation? If so, how many of them have any idea what ISO accreditation is?

Yes, 14000 of employees including academics and staffs have been informed just after getting ISO27K

25. In your opinion, are most of the organisation, including all type of users, employees and students, more aware of the importance of the IT security after getting the ISO 27k accreditation?

Yes, especially after inauguration of the information security awareness programme through different communication channels

26. How does your organisation ensure information security awareness among employees?

Inauguration of the information security awareness programme through different communication channels and this programme is continued during the year

<https://infosec-aware.imamu.edu.sa>

Thank you for taking the time to complete this questionnaire, your responses will help to significantly improve the information security awareness in Saudi

Appendix C

Employee Security Awareness Survey

Adopted from Trenton Bond trent.bond@gmail.com Admin - Version 1.3

Information Security Awareness survey used to Determine Risk

This survey consists of 24 questions. Some of the question responses in this survey indicate strong awareness and good security practices while others indicate weak awareness, negligent behaviour, or high-risk activities. Based on these differences, each question response in this survey (except for the first question) has been assigned a risk value (1-5). "One" is the lowest risk value and "five" is the highest risk value. When the results of the survey have been collected, they can be used to determine the overall risk score or risk level of the organization.

1. For each of the 24 questions, multiply each question response risk value (1-5) by the number of times it was chosen by the survey takers.

<response risk value> X <the number of times chosen> = <response total>

2. Add up all of the response totals for a survey cumulative response total.

3. Divide the survey cumulative response total by the number of survey takers to calculate the survey (or organization's) risk score.

<cumulative response total> / <number of survey takers> = Organization's Risk Score

4. Using the risk score, check the "Risk Levels" table below for the organization's general risk rating.

Risk Levels

Risk level	Description
Low (25 – 39)	Users are aware of good security principles and threats, have been properly trained, and comply with all organizational security standards and policies.
Elevated (40 – 60)	Users have already been trained on organizational security standards and policies, they are aware of threats, but may not follow good security principles and controls.
Moderate (61 – 81)	Users are aware of threats and know they should follow good security principles and controls, but need training on organizational security standards and policies. They also may not know how to identify or report a security event.
Significant (82 – 96)	Users are not aware of good security principles or threats nor are they aware of or compliant with organizational security standards and policies.
High (97 – 110)	Users are not aware of threats and disregard known security standards and policies or do not comply. They engage in activities or practices that are easily attacked and exploited.

Survey Minimum Risk Score = 25

Survey Maximum Risk Score = 110

1. What is your position within the university?

- a. Management
- b. Support Staff
- c. Academic / Lecturer
- d. Student

Other, please specify:

Logic Note: Did not apply risk values to positions because they should all be equally security aware.

2. How secure do you feel your computer is?

- a. Very secure (3)
- b. Secure (1)
- c. Not secure (5)
- d. I do not know how secure it is (4)

Logic Note: Users who feel their computer is not very secure may be right and the issue should be escalated to the responsible party. However, the user may be less likely to handle sensitive data or conduct risky transactions with it, which would lower the impact of compromise slightly.

Users who feel their computer is very secure may be right and so the device poses little vulnerability risk to the organizations. However, the user may be more likely to handle sensitive data or conduct risky transactions with it, which would increase the impact of compromise. Cautious but aware users who chose “Secure” seemed like a good middle ground to strive for.

3. Is the firewall on your computer enabled?

- a. Yes, it is enabled. (1)
- b. No, it is not enabled. (5)
- c. I know what a firewall is but I do not know if it is enabled. (3)
- d. I do not know what a firewall is. (4)

Logic Note: Users who chose “C” are not informed and pose a significant risk for obvious reasons. Users who choose “B” are even a higher risk as they know what a firewall is and the protection it would provide; yet do not have it enabled.

4. Is anti-virus software currently installed, updated and enabled on your computer?

- a. Yes it is. (1)
- b. No it is not. (5)
- c. I do not know how to tell. (4)
- d. I do not know what anti-virus software is. (5)

Logic Note: Users who choose “B” may be indicative of users who are aware of what “anti-virus” is and the protection it provides, yet do not run or update it. This behaviour may also

indicate the user is risk tolerant and is more likely to improperly handle sensitive data or conduct risk transactions.

Users who choose “C” pose a significant risk because they are aware of what “anti-virus” is, but unaware of how to tell whether or not it is running. Users who choose “D” pose a high risk because they are unaware of what “anti-virus” is and unaware of how to tell whether or not it is running.

5. Do you know what an email scam is and how to identify one?

- a. Yes I do. (1)
- b. No, I know what an email scam is but I don’t know how to identify one (3)
- c. No, I do not know what an email scam is. (4)

Logic Note: Users who are aware of how to identify an email scam are less likely to fall victim lowering risk.

6. Does the university have policies available on which websites you can access relating to website security?

- a. No, there are no policies, I can visit whatever websites I want while at work. (4)
- b. Yes, there are policies limiting what websites I can and cannot visit while at work, (2) but I do not know the policies.
- c. Yes, there are policies and I know and understand them. (1)

Logic Note: Users who choose “B” are protected by corporate filtering solutions, but are an elevated risk because they are unaware of the policies.

Users who choose “A” pose a significant risk because they can visit whatever site they want including potentially malicious sites.

7. Does the university have policies on how and what you can and cannot use email for?

- a. No, there are no policies, I can send whatever emails I want to whomever I want while at work. (4)
- b. Yes, there are policies limiting what emails I can and cannot send while at work, but I do not know the policies. (2)
- c. Yes, there are policies and I know and understand them. (1)
- d. I do not know if there are any policies on what I can use email for.(3)

Logic Note: Users who choose “B” are protected by corporate filtering solutions, but are an elevated risk because they are unaware of the policies.

Users who choose “A” pose a significant risk because they can visit whatever site they want including potentially malicious sites.

8. Is instant messaging allowed in your university?

- a. Yes, I can use it with anyone. (1)
- b. Yes, but I can only use it with other university employees(1)
- c. No, instant messaging is not allowed. (2)
- d. I do not know. (2)

Logic Note: Users who choose “A” or “B” are indicative of users that are aware of organizational policy regardless of disposition. Users who choose “D” are not aware of or perhaps a policy does not exist elevating the risk.

9. Can you use your own personal devices, such as your mobile phone, to store or transfer confidential university information

- a. Yes I can. (5)
- b. No I cannot. (1)
- c. I do not know. (4)

Logic Note: Users who choose “A” represent a high risk to the organization because there is little if any control over the processing, transmitting, or storing of sensitive data on personal devices.

Users who choose “C” pose a significant risk because at minimum they are unaware of whether or not it is allowed, and they are more likely to handle confidential information on personal devices without knowing.

10. Does the university have an information security team?

- a. Yes, we have an information security team. (1)
- b. No, we do not have an information security team. (4)
- c. I do not know. (3)

Logic Note: Users who chose “C” are not informed and pose a risk for obvious reasons. Users who choose “B” when there really is a security team could represent an even higher risk to the organization because they believe they are aware but are really misinformed.

11. Do you know who to contact in case you are hacked or if your computer is infected?
- a. Yes, I know who to contact. (1)
 - b. No, I do not know who to contact. (5)

Logic Note: Users who do not know who to contact when their PC is compromised pose a significant risk because they are likely to continue to use the device, potentially exposing the organization to further compromise or breach.

12. Do you know how to tell if your computer is hacked or infected?
- a. Yes, I know. (1)
 - b. No, I do not know. (4)

Logic Note: Users who do not know what potential symptoms to look for are more likely to continue to use a compromised device, potentially exposing the organization to further compromise or breach.

13. How careful are you when you open an attachment in email?
- a. I do not open attachments. (1)
 - b. I always make sure it is from a person I know and I am expecting the email. (1)
 - c. As long as I know the person or company that sent me the attachment I open it. (3)
 - d. There is nothing wrong with opening attachments. (5)

Logic Note: Users who choose “B” could be tricked into opening malicious attachments from spoofed sources that look like they came from recognizable persons or companies.

Users who choose “C” pose a significant risk to the organization because they are unaware of the threat, vulnerability or impact if they open a malicious attachment. Cautious and aware users will choose “a”.

14. Do you know what an email phishing attack is?

- a. Yes, I do. (1)
- b. No, I do not. (5)

Logic Note: Users who are aware of how to identify phishing are less likely to fall victim lowering risk.

15. Do you think that your computer has no value to hackers, so no one would target it?

- a. Yes I do. (5)
- b. No, I do not (1)

Logic Note: Users who choose "A" pose a significant risk to the organization because they are unaware of the threat and impact if their computer is compromised.

16. If you delete a file from your computer or USB stick, that information can no longer be recovered.

- a. True (4)
- b. False (1)

Logic Note: Users who choose "A" could represent a significant risk to the organization because they believe they are aware but are really misinformed and likely do not dispose of sensitive electronic documents properly.

17. Have you ever found a virus on your computer at work?

- a. Yes, it has been infected before. (4)
- b. No, it has never been infected. (2)
- c. I know what a virus is but I do not know if it has ever been infected. (3)
- d. I do not know what a virus is. (4)

Logic Note: Users who are unaware of malware threat pose a significant risk to an organization and would likely not know how or when to report it.

Users who indicate they are aware of malware threat but still have had infected work computers also pose a significant risk. Their activities and/or behaviours, while at work, may have led to the infections (sites they visit, links they click, etc.). However, the risk is slightly lowered because users who have been infected in the past are usually more security aware.

18. Have you ever given your work password to a co-worker or someone else?
- a. Yes (5)
 - b. No 1)

Logic Note: Users who are willing to share their work password are highly susceptible to social engineering or internal threats. The easiest way to get a password is to ask.

19. Has your manager or anyone else you know at work ever asked you for your password?
- a. Yes, they have (5)
 - b. No, they have not. (1)

Logic Note: Organizations where it is common and accepted for others to ask users for their passwords is more likely to be successfully attacked with social engineering.

20. Is your computer configured for the security to be automatically updated?
- a. Yes, it is. (1)
 - b. No, it is not. (5)
 - c. I do not know. (3)

Logic Note: Users who chose "C" are not informed and pose a risk for obvious reasons. Users who choose "B" are even a higher risk as they know what "automatic updates" means and the protection it would provide; yet do not have it configured.

21. Have you downloaded and installed software on your computer at work?
- a. Yes I have. (2)
 - b. No I have not. (1)

Logic Note: Users who choose “A” pose a higher risk to the organization than those who choose “B” because they are more likely to download malicious software and infect a work computer.

21. Do you use the same passwords for your work accounts as you do for your personal accounts at home, such as Facebook, Twitter or your personal email accounts?

- a. Yes I do for many personal accounts. (4)
- b. Yes I do, but only for the following accounts: (2)
- c. No I do not. (1)

Logic Note: When third party accounts are compromised, users who use the same password on work as personal accounts are much more vulnerable to password attacks and guessing.

22. How often do you take information from work and use your computer at home to work on it?

- a. Almost every day. (5)
- b. At least once a week. (4)
- c. At least once a month. (2)
- d. Never (1)

Logic Note: Users who answer “A”, “B”, or “C” pose an increasing risk of data loss to organizations based on increasing frequency and the use of a home personal computer.

23. Have you logged into work accounts using public computers, such as from a library, cyber cafe or hotel lobby?

- a. Yes, I have done so many times. (4)
- b. Yes, but only on rare occasions (4)
- c. No, I have never done so. (1)

Logic Note: Users who access work accounts from public computers are more likely to have their credentials or corporate data stolen if these devices are insecure or compromised. This would also indicate the user is not aware of the potential risks of doing so.

Data analysis for prior assessment

Table 8.1 Q2 shows that small percentage (4%) of the participants from both universities thought their personal computer is very secure. 36% of both universities participants do not know how secure are their personal computer (Figure 8.2).

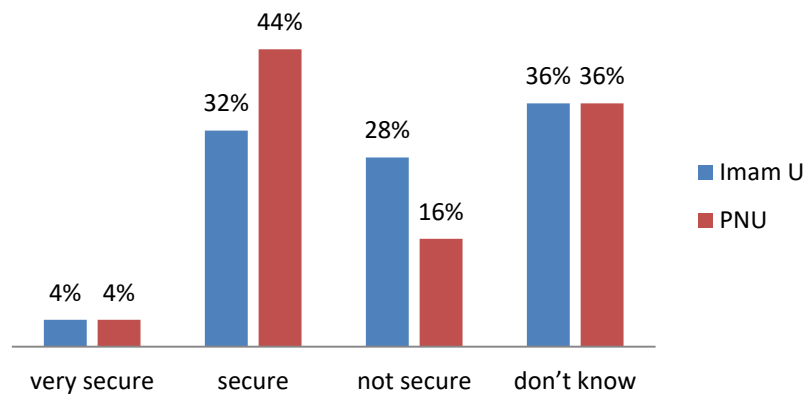


Figure 8.2: security of personal computer

Table 8.1 Q3 shows that 18% of PNU participants and 20% of Imam U knew what a firewall is and think that it is enabled on their computer. Whereas 74% of PNU participants and 60% of Imam U don not know and do not know what is a firewall (Figure 8.3).

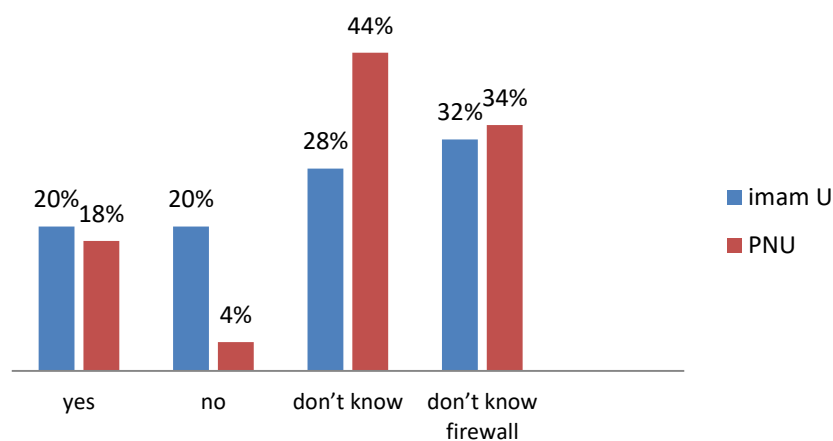


Figure 8.3: Is the firewall on your computer enabled?

Table 8.1 Q4 shows that 28% of PNU participants and 48% of Imam U knew that anti-virus software installed, updated and enabled on their computers. Whereas 68% of PNU participants and 32% of Imam U don not know and do not know what is anti-virus software (Figure 8.4).

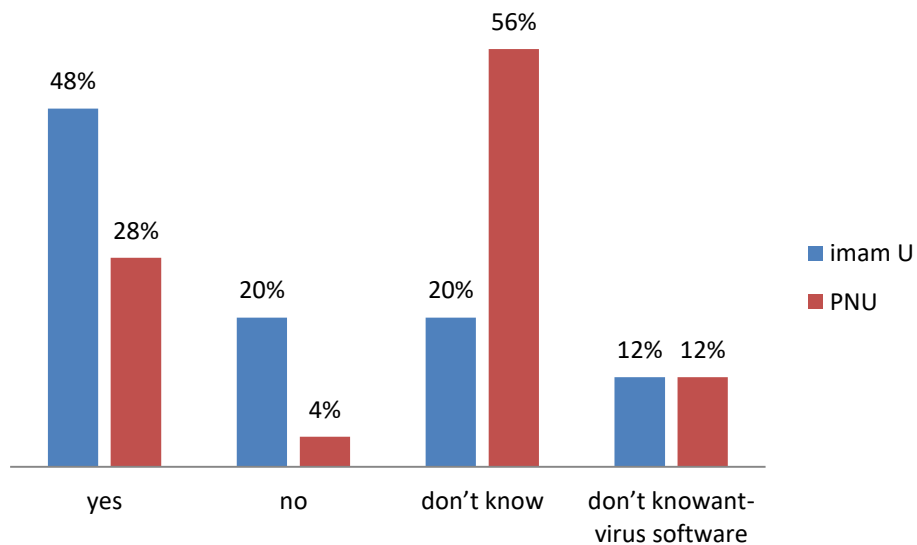


Figure 8.4: Is anti-virus software installed, updated and enabled on your computer?

Table 8.1 Q5 shows that only 18% of PNU participants and 8% of Imam U knew that what an email scam is and how to identify one. Whereas 82% of PNU participants and 92% of Imam U don not know and do not know what an email scam is and how to identify one (Figure 8.5).

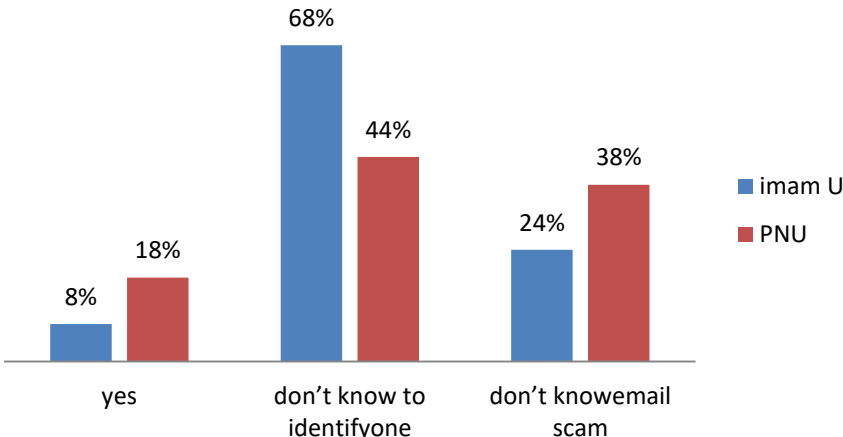


Figure 8.5: Do you know what an email scam is and how to identify one?

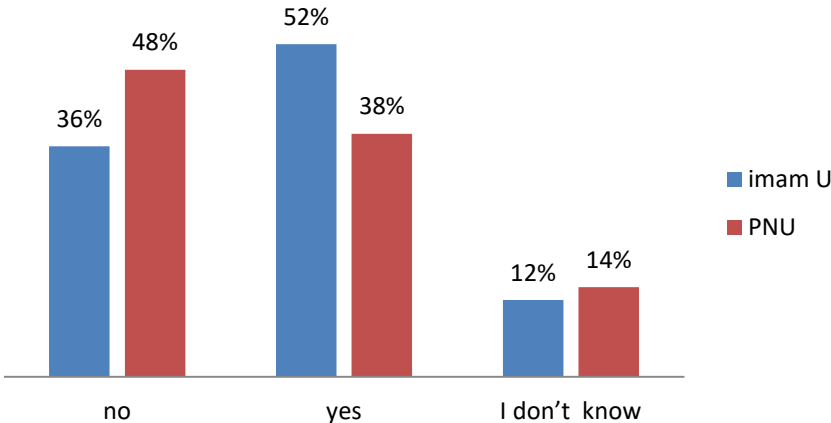


Figure 8.6: The University has policies available on website security that can be accessed

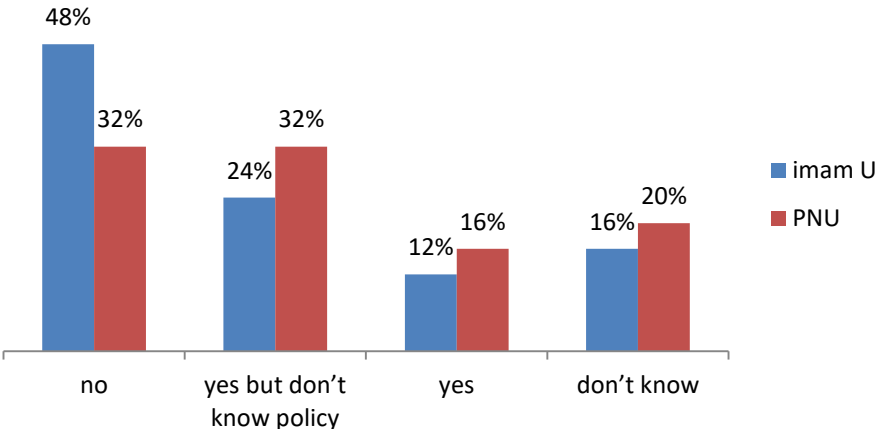


Figure 8.7: The University have policies on how and what can and cannot use email for

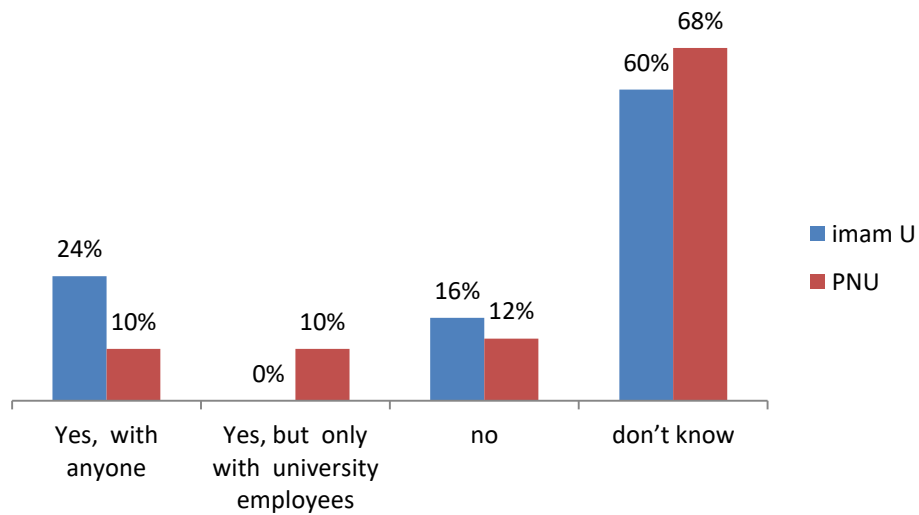


Figure 8.8: instant messaging is allowed in university

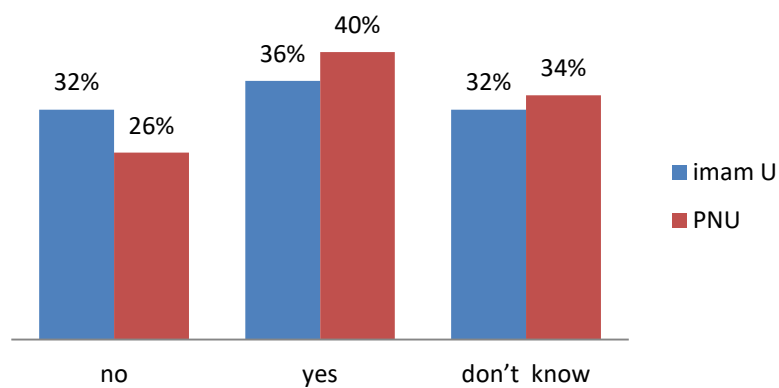


Figure 8.9: Use of personal devices to store or transfer confidential university information

According to the survey result approximately 70% of both universities participants did not know the people in charge of the information security, see Figure 8.11.

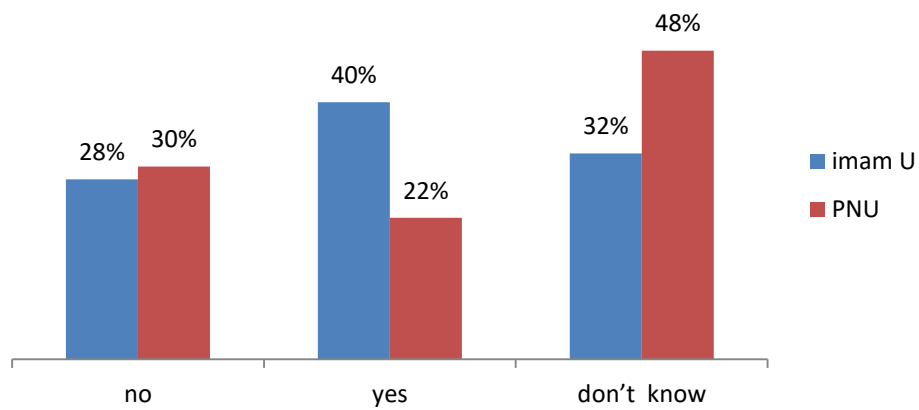


Figure 8.11: Does the university have an information security team?

Moreover about 72% from ImamU participants and 62% from PNU participants did not know who to report threats, see Figure 8.12.

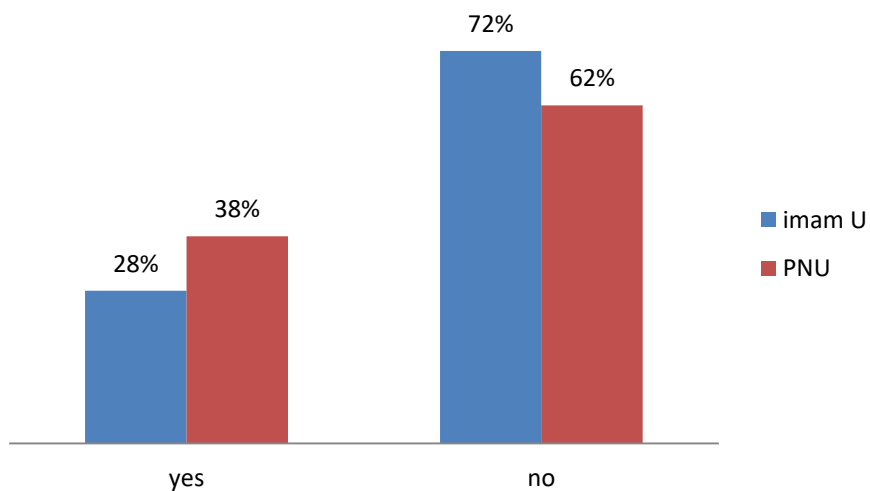


Figure 8.12: Do you know who to contact in case you are hacked or if your computer is infected?

Moreover about 72% from ImamU participants and 78% from PNU participants did not know what an email scam was and they did not know how to identify one, see Figure 8.13.

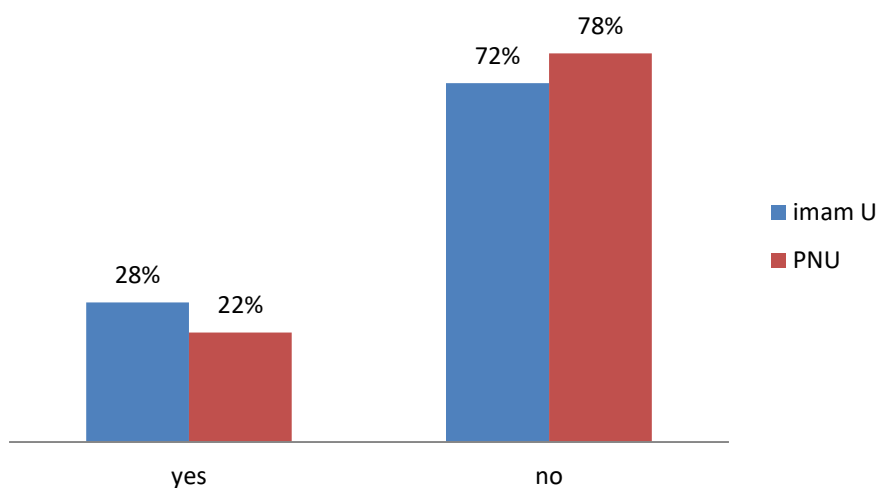


Figure 8.13: Do you know what an email scam is and how to identify one?

Figure 8.13 show that 72 % of ImamU participants and 78 of PNU participants did not know what an email scam is and how to identify one. Although according to the newly developed team member, PNU information security department had sent emails to all users to block scam email without telling them what a scam email is.

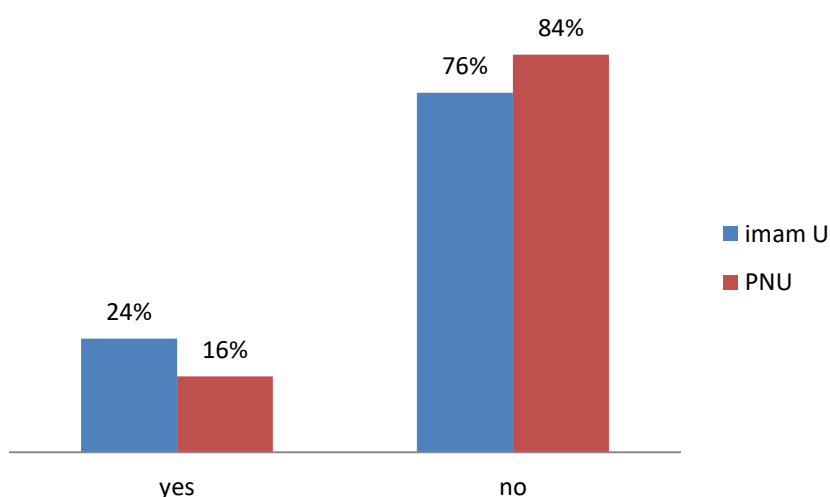


Figure 8.14: Do you know what an email phishing attack is?

Moreover about 76% of ImamU participants and 84% of PNU participants did not know what an email phishing was and they did not know an email phishing attack, see Figure 8.14.

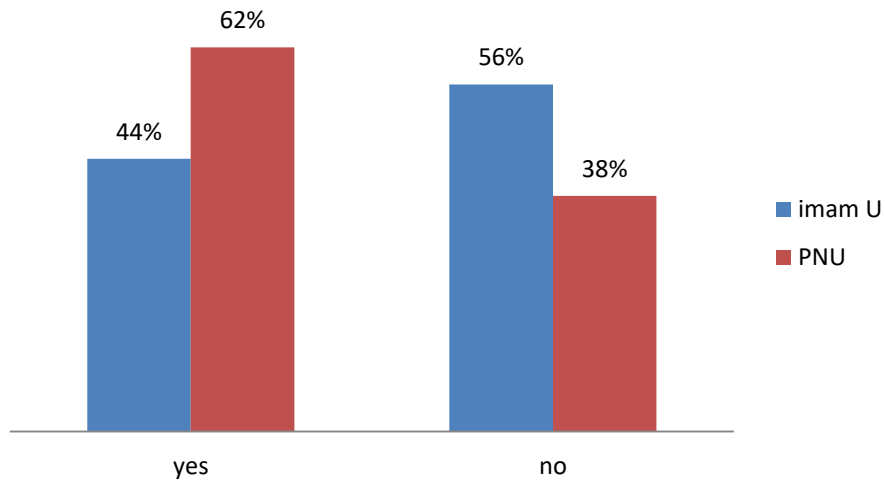


Figure 8.15: Does work computer has no value to hackers, so no one would target it?

Moreover about 56% of ImamU participants and 38% of PNU participants thought that their work computer has no value to hackers, so no one would target it, see Figure 8.15.

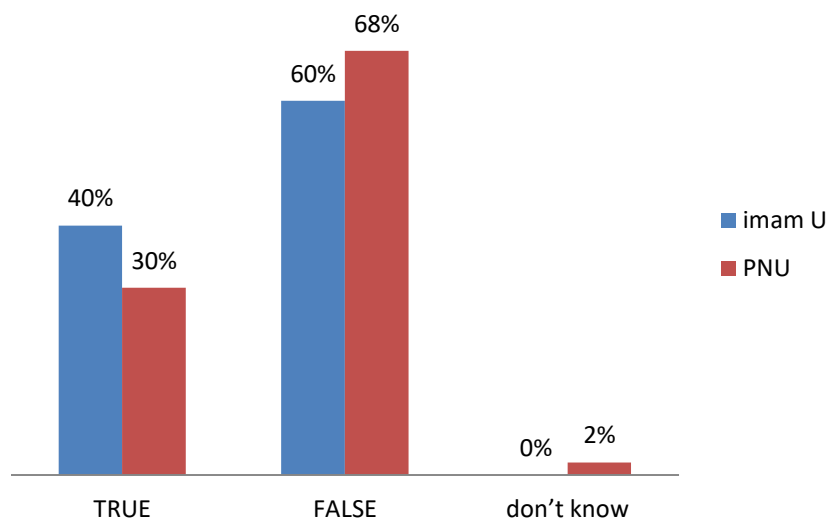


Figure 8.16: A Deleted file from a computer or USB stick can no longer be recovered

Figure 8.16 shows about 40% of ImamU participants and 30% of PNU participants thought if they deleted file from a computer or USB stick can no longer be recovered. It also shows about 60% of ImamU participants and 68% of PNU participants thought if they deleted file from a computer or USB stick can be recovered.

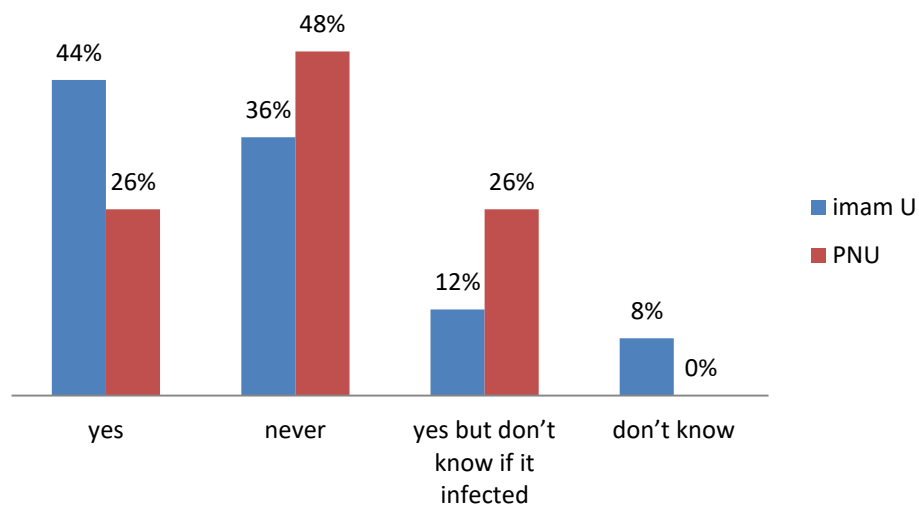


Figure 8.17: Found a virus on work computer

Figure 8.17 shows that 56% of ImamU participants and 52% of PNU participants thought that they had found a virus on their computer at work.

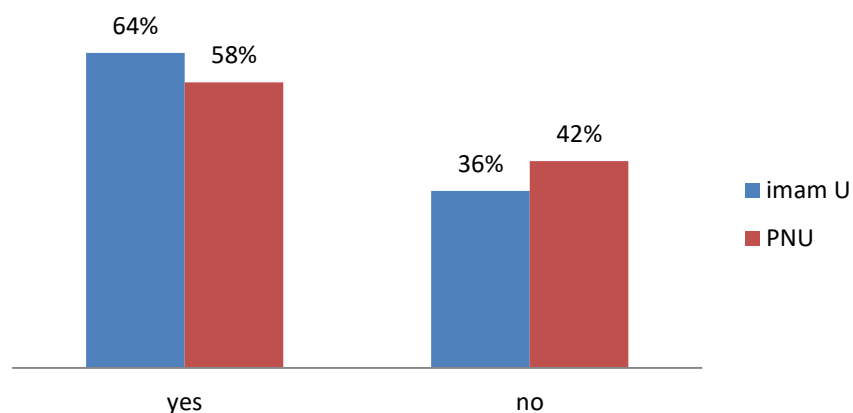


Figure 8.18: Share work password with a co-worker or someone else

Figure 8.18 shows that employees were not aware of the risk related to share their password with others such as co-worker (64% of ImamU participants and 58% of PNU participants).

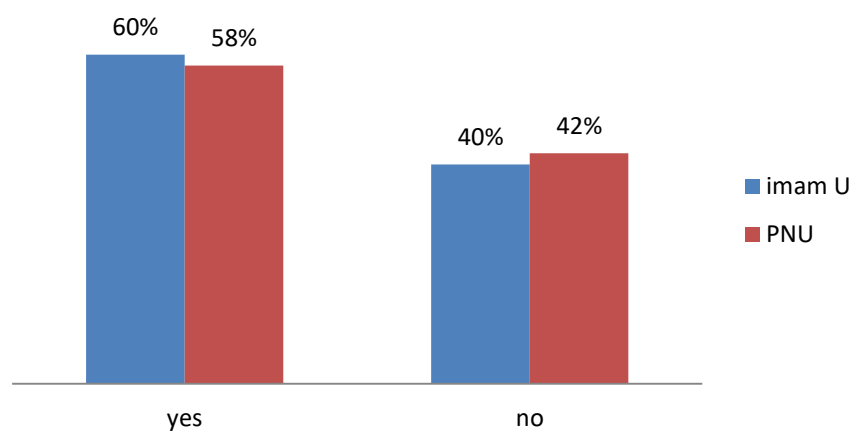


Figure 8.19: Give work password to manager if asked

Figure 8.19 shows that employees were also not aware of the risk related to given managers their password. Participants from both universities (60% of ImamU participants and 58% of PNU participants) agreed that they would their manager their password if asked.

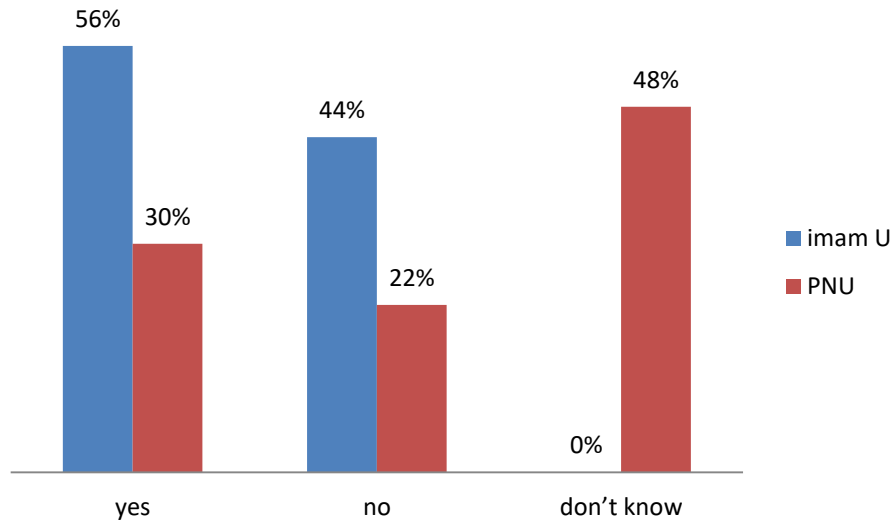


Figure 8.20: Work computer configured for the security to be automatically updated

Figure 8.20 shows that some of the participants thought that their computers were not automatically updated to be configured for the security (44% for ImamU and 22% for PNU). Most of the PNU participants (48%) did not know if their work computer automatically updated to be configured for the security.

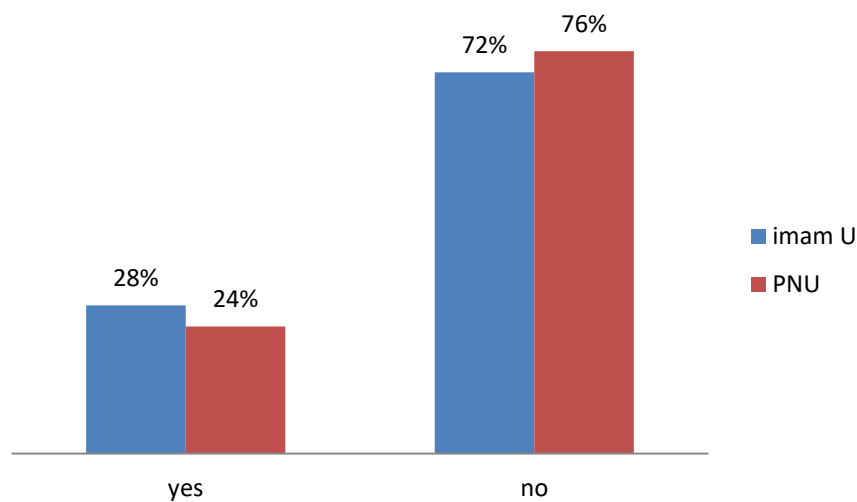


Figure 8.21: Download and install software on computer at work

Figure 8.21 shows that some participants had downloaded and installed software on their computers at work (28% for ImamU and 24% for PNU). Although the percentage is low but

downloading or installing software without the university permission is very risky and can threaten the entire information system.

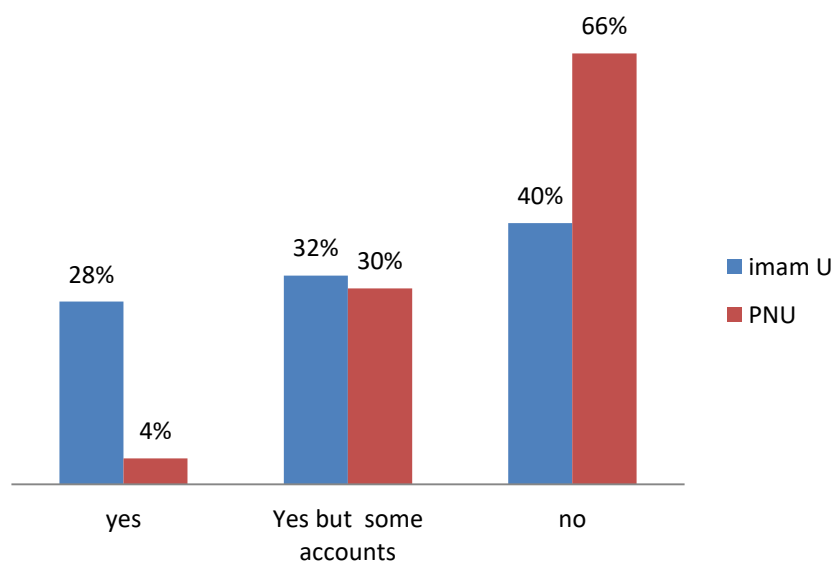


Figure 8.22: Use the same passwords for work accounts and personal accounts at home, such as Facebook, Twitter or personal email accounts

Figure 8.22 shows that some participants used the same passwords for work accounts and personal accounts at home, such as Facebook, Twitter or personal email accounts (60% for ImamU and 34% for PNU).

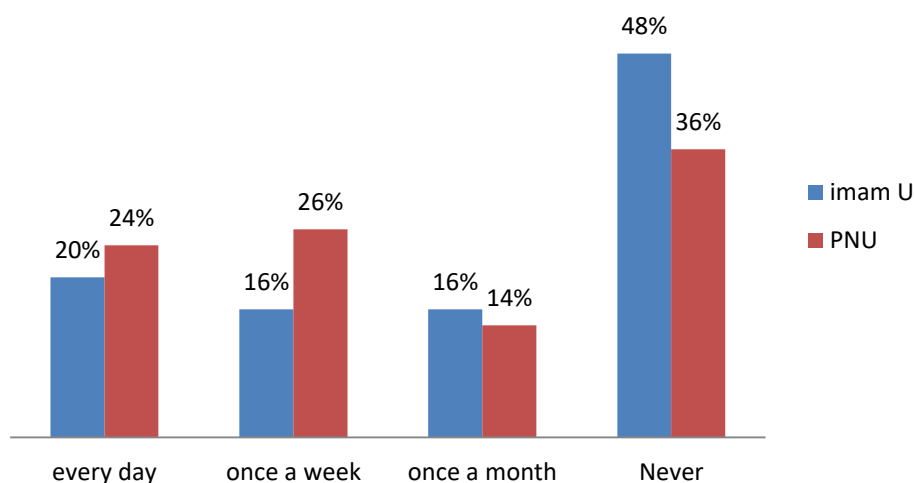


Figure 8.23: How often do you take information from work and use your computer at home to work on it?

Figure 8.23 shows that 20% of ImamU participants and 24% of PNU participants take information from work and use their computer at home to work on it every day, 16% of ImamU participants and 26% of PNU participants take information from work and use their computer at home to work on it at least once a week, 16% of ImamU participants and 14% of PNU participants take information from work and use their computer at home to work on it at least once a month and 48% of ImamU participants and 36% of PNU participants never information from work and use their computer at home to work on it.

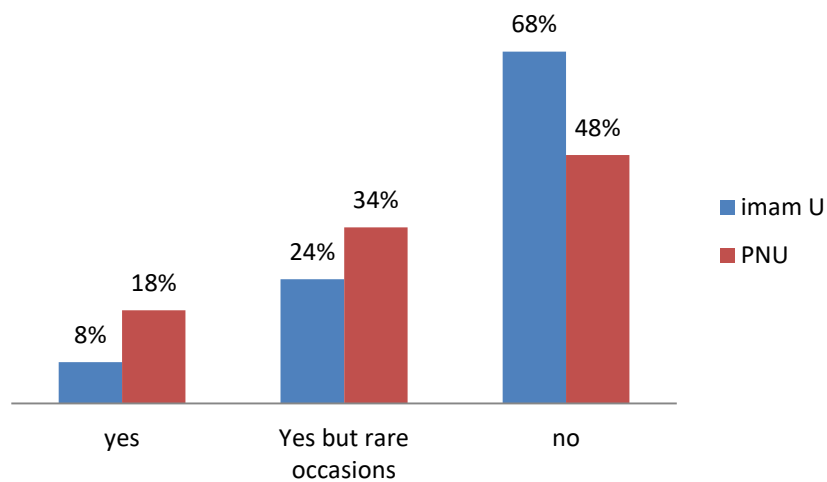


Figure 8.24: Logging into work accounts using public computers, such as from a library, cyber cafe or hotel lobby

Figure 8.24 shows that 8% of ImamU participants and 18% of PNU participants logged into work accounts using public computers, such as from a library, cyber cafe or hotel lobby, 24% of ImamU participants and 34% of PNU participants, in rare occasion, logged into work accounts using public computers, such as from a library, cyber cafe or hotel lobby and 68% of ImamU participants and 48% of PNU participants never logged into work accounts using public computers, such as from a library, cyber cafe or hotel lobby.

Appendix D

Example of tables filled by students

Computer issues

1-Student name: Tamara Majed

Section: 4i1

Definitions:

Information assets cover not only information (data, voice, video and paper) but also where it is stored and the system and equipment that process them. Information assets, whether electronic or hardcopy, are all university computers, such as workstations, personal computers and laptops, and electronic resources, such as networks, printers, communication facilities and remote facilities.

A threat is an event or act which has the potential to harm an information system through unauthorised access, destruction, disclosure, modification of data, or denial of a service.

Risk is a condition that contributes to display harm or danger.

Some of computer problems (issues) are:

- If a computer is slow
- If a computer displays unusual messages
- If a computer runs out of disk space
- If a computer crashes
- If a computer receives bounced back emails
- If a password doesn't work anymore
- If you received suspicious emails from unknown or known person/company

- Overheating

- Lockups and freezes

*If you experience more problems please add them to the list above

Table 1: Recording information assets

Asset	Type (workstation/ laptop/ mobile)	Software type	Asset Location	User position	Problem faced	Risk rate	Frequent occurrence	effect
Password to login to my account	laptop	Email	The email wasn't working well	I open it in the university It wasted my time spending to retry putting the password while I was sure it's correct	It has wasted my time trying to fix it and I had an exam online so I was late	Low	It happened one time	I wasn't sure about my accounts privacy and I started to doubt if a hacker break into my account!!
Transfer between language	Laptop and mobile	Application (from website Google) which is PNU	Website (Google) which is PNU	Trying to put the correct ID in the required language but it still not correct and it takes time	The website wasn't working well because of the difference in languages and it was hard to put the ID and it remain incorrect	Low	It happened one time	It was hard because working with technics and solve it but I had to work on the problem and try to fix it

Table 2: Listing threats

Threat	Type	rate	Frequency of occurrence	reported	fixed
Virus	Email which wasn't able to log in	Low	Once a year or less	I sent an email to the UCC to fix my email from the virus	They had fix my email from the virus and pick up the problem I faced

Table 3: Threat rating

Threat rate	Frequency of occurrence
Low	Once a year or less
Medium	At least two a year
High	At least once a month

2- Student name: ابراهيم عبدالكريم الفوازSection: 4i1**Table 1: Recording information assets**

Asset	Type (workstation / laptop/mobile)	Software type	Asset Location	User position	Problem faced	Risk rate	Frequent occurrence	effect
Student account	Laptop / phones	chrome	blackboard server	Cannot use the website	Can't access her account	low	Once a year	Not able to see any updates from the educators such as: announcement, grades, etc.

Table 2: Listing threats

Threat	Type	rate	Frequency of occurrence	reported	fixed
System shutdown	denial of a service	medium	Two times in a month		Yes

Table 3: Threat rating

Threat rate	Frequency of occurrence
Low	Once a year or less
Medium	At least two a year
High	At least once a month

3-Student name: khulud alshammariSection: 4I3**Table 1: Recording information assets**

Asset	Type (workstation / laptop/ mobile)	Software type	Asset Location	User position	Problem faced	Risk rate	Frequent occurrence	Effect
1- System Academic	laptop	website	change the password on my academic system, and after a while I opened my account through old password and account opening! It opens my academic system has become through two of your old and new password	Academic system opened in the house	The problem I faced it became my Academic account opens through two of the password and the possible cause breach my account	Low	Once a year or less	This problem possible impact on my academic and exposed to penetrate because it is possible enter it through two password
2- Email university	laptop / mobile	Email	Very slow to access messages and upload	Academic system opened in the House and the university	Slow download and get messages cause not to read the messages sent from the university or important messages until late	Medium	At least two a year	Slow download and get messages cause not to read the messages sent from the university or important messages until late

Table 2: Listing threats

Threat	Type	Rate	Frequency of occurrence	reported	fixed
1- System Academic	Disruption and delays in service	Low	Once a year or less	yes	yes
2-Email university	Disruption and delays in service	Medium	At least two a year	yes	yes

Table 3: Threat rating

Threat rate	Frequency of occurrence
Low	Once a year or less
Medium	At least two a year
High	At least once a month

4- Student name: **Shahad alqarni**Section: **4i3****Table 1: Recording information assets**

Asset	Type (workstation/ laptop/mobile)	Software type	Asset Location	User position	Problem faced	Risk rate	Frequent occurrence	effect
The site where the pressure upon deletion and addition.	laptop	PNU	Home	Student	If there is an error on page Or page not found	Once a year or less	Often repeated	Delay the registration materials

Table 2: Listing threats

Threat	Type	rate	Frequency of occurrence	reported	fixed
Deviations in quality of service	software	Medium	Once a year or less	No reported	No

Table 3: Threat rating

Threat rate	Frequency of occurrence
Low	Once a year or less
Medium	At least two a year
High	At least once a month

Appendix E

Information security policies for the information system department at PNU

Document Title	Information security Policy for Information System Department
Version Number	1.0
Approved by	The Information system Department Management
Document Classification	open
Effective date	05/04/2017
Review date	05/05/2017
Author	Information system Department (Hend Alkahtani)

1.0 Introduction

The information system department collaborates with PNU information security management with its documented information security policy that best fit its end users, employees and students. The developed information security policy is available to all end users either as:

- a hardcopy distributed to all employees
- Softcopy made available in the organisation website

Users' needs influence the developed information security policy documentation and any other documentation activities, such as the writing style, the way in which it is presented and the distribution of the document (Höne and Eloff, 2003). It is:

- Made available to all employees
- Easy to use
- Easy to read
- Written in a language that most of the users understand
- Use a readable text and a font size.

1.1 Authorised Access Policy

All users should be informed of their authorised access policy and rights.

- Covers all the identification and access rights such as: access rights
 - One identifier for each user
 - Each computer has a unique password
 - Each user had unique password

- Enforce password requirement (see next subsection).
 - Sharing computer, identification or password is not acceptable at all levels to control trusting culture.
 - Accessing other employee account is not acceptable and is subject to disciplinary actions
 - Unused account must be disabled.
- User failure to comply with this policy is subject to disciplinary actions.

1.2 Password policy

Information system users need to be directed in:

- How to choose a password. There must be a password policy in how to choose a strong password.
- How to protect a password. Users at all level of organisation must be aware of the risk of sharing or revealing their password with other users.
- How to use a documented password policy.
- Password policy must be presented to all users either as a hand in or sent via email, PNU website and any other social media.

Password requirement such as:

- Password must be changed upon first logon (enforced by the IT system)
- New password must be completely different than the old password (enforced by the IT system).
- Password must not be in a written in a sticky note or stored in a cabinet near the employee computer system.

- Password should be changed at regular intervals (every university semester, every three months)
- Password must be complex and not easy to guess.
- Account lockout after a number of unsuccessful consecutive logon attempts

End users make critical information security errors therefore the suggested solutions are:

- Prevent password sharing between employees and management formally either by sending a warning emails to all employees or verbally during department meeting.
- Develop a formal information problem reporting form that must be signed by the head of the management in a college such as the Dean of the School. This form has the name of the employee, the type of problem faced, the frequency of occurrence and the effect and the damage of that problem.
- A follow up role assigned to the team member as part of their job to monitor and make sure the problem is taken seriously and fixed as fast as possible. A problem that is not fixed should be reported back by the team leader to the Dean and the problem issue is reported again.
- Create an information security culture among employees.
 - Notify all type of employees of any recent development of the university information security mission
 - Request employee involvement in any recent development of the university mission. Distribute table 7.4 (listing threats) to help employees recording their feedback.
 - Use email more alerts when any information security risk or threat accrued or reported
 - Use workshops and seminars to all type of users when any information security risk or threat accrued or reported

1.3 System user access roles policy

System users must know his/her access roles by having:

- A form for creating a new account to each user with his/her privileges and restriction listed and should be completed approved by:
 - o The account user
 - o The user supervisor
 - o Owner of the information system
- A copy of the form is giving to the user, either via email or regular mail to the user, and another copy stored in the user file.
- A form for termination an account for user who leaves the information system due to changing or leaving the organisation and should be completed also approved by the user, supervisor and owner of information.
- Termination of an account must occur immediately after form approved.

1.4 The information system auditors

The information system auditors need to:

- Check if there are criteria for acceptable risk and classify the risks according to this classification. Otherwise it is necessary to first create the criteria for acceptable risk.
- Contribute end users in auditing the information system to make sure that:
 - All types of computer, system configuration, and application software are handled, used, and upgraded according to operation standards, regulations, and policies.
 - All services are undertaken according to operation standards, regulations, and policies

- Recognise and record information system threats. Use the Table 1.1 to recognise and report.

Table 1.1: Recording and reporting information assets problems

Asset	Type	Location	User Position	Problem faced	Frequent occurrence	Risk rate	effect	reported	fixed

- Classify threats according to the risk associated with it using Table 1.2:

Table 1.2: Risk rating

Risk rate	Frequency of occurrence
Low	Once a year or less
Medium	At least once a semester
High	At least once a month

- Recognise, classify, assess and report risk
- Help in developing information security policy
- Choose the appropriate actions to manage risks such as:
 - Applying treatment to reduce the risk
 - Accepting the risk
 - Finding work-rounds to avoid the risk
 - Transferring the risk to third parties.
- Repeat the risk assessments and classification annually or as required during a system's upgrading or maintenances.

1.5 Computers and workstations physical secure policy

- Secure university computers by activating the security card access control or any proper physical security access controls.
- All workstations are kept in a room with a lock door.

1.6 Copying data policy

- The policies must be as detailed as possible to ensure all employees follow them to the letter.
- Restrict the use of removable and portable memories.
- Taking a copy of information assets outside the work area is not allowed and subject to a sanction.
- Acknowledge all type of information system users of all the sanctions related to misuse of data which include copying university data and taking data outside work areas in a removable memory (section 1.10).

1.7 Retention and disposal policy

- The policy must be as detailed as possible to ensure all employees follow them to the letter and must covers:
 - A fixed time period for disposal of old information, e.g. end of a next semester.
 - A special storage or a cabinet to keep the old information
 - The way the old information destroyed.

- A fix time period for disposal of old hardware. Usually the average lifetime of hardware would be between 4-6 years.
- The need for a proper disposal policy to ensure all information is removed from a computer since deleting files from a computer does not destroy the information which can often be recovered. There are a number of ways do not work to dispose information from old hardware such as:
 - Deleting files only removes part but not all information even if information deleted from the trash it can be retrieve
 - Reformatting disks. Formatting makes it hard to retrieve data but not impossible. The information can be recovered in part or in whole.
 - Encrypting disks or files only hide information from view just as the password if the password is weak it will be expose to other so is the encrypting method almost all encryption method can be cracked with time and effort
- There are a number of better ways that could work to dispose information from old hardware as in:
 - Wiping the hard drive (overwriting) is one of the effective ways of destroying information by writing random data over the original information. This way obliterates original information therefore it cannot be recovered. There are a number of software tools to overwrite every bit and byte of original information.
 - Physical destroying of the hard disks

By using proper disposal policy to ensure all information is removed from a computer, the computer can be reused in two ways:

- Recycling the old hardware to have safe environment.
- The formatted old hardware can be donated to others in need either locally or to different countries.

1.8 Exchange information policy

- The end users need to know:
 - What a suspicious email may look like
 - What it may contain
 - What is the possible damage, risk and threat associated with it
 - How and why they must be reported
- The message should be distributed, not only via email, but also through the use of other social media, such as WhatsApp, and, not only once a year, but at the beginning of a semester and every time knowledge-intensive organisation encountered a threat.

1.9 Information security physical controls policy:

- Secure knowledge-intensive organisation's computers by activating the security card access control or any proper physical security access controls.
- Keep all workstations in a room with a door lock.
- If the knowledge-intensive organisation's data is particularly sensitive, or there is a significant risk of access by unauthorised personnel, then a CCTV installation covering the knowledge-intensive organisation's computers should be considered. If a CCTV system is already installed, then steps should be taken to ensure it is switched on and monitored. If the CCTV covers areas which are primarily used by females then to safeguard privacy and gender sensitivities, CCTV cameras covering

areas used by females should be monitored by female security staff. For example, in PNU, a CCTV system is installed but it is not switched on and working. The CCTV needs to be made fully functional. Furthermore as most CCTV cameras will monitor computers used by the female staff and students, it is important that these cameras are monitored by suitably trained female security staff.

- Install a fire alarm system. If a fire alarm system is already installed, then tests should be taken to ensure it is switched on and working.
- Install physical access control devices. If physical access control devices are installed such as PNU card access devices, then tests should be taken to ensure they are active and working.

1.10 Related Laws and Regulations

The university must Present the disciplinary action for policy and reference it to a law or an act such as:

- Saudi Arabia Ministry of Communication and Information Technology (MCIT) Acts and Regulation: Anti-Cyber Crime Law:
 - <http://www.mcit.gov.sa/Ar/AboutMcit/Regulations/Pages/CriminalLaws.aspxpdf>
- Saudi Arabia Ministry of Higher Education and university regulations
 - <https://www.moe.gov.sa/en/HigherEducation/PrivateHigherEducation/Pages/RulesandRegulations.aspx>
- Adopted and promulgated western legislation:
 - UK Data Protection Act 1998 (DPA 1998)
 - <http://www.legislation.gov.uk/ukpga/1998/29/data.pdf>
 - UK Computer Misuse Act 1990 (CMA 1990)
 - https://www.unodc.org/res/cld/document/gbr/1977/computer-misuse-act-1990.html/Computer_Misuse_Act_1990.pdf

- Human rights laws, such as ‘The Universal Declaration of Human Rights’ developed by the United Nations.
 - http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf