Implementation, Management And Dissemination Of Information Security: An Organisational Perspective Of Financial Institutions

A thesis submitted for the degree of Doctor of Philosophy

By

Abdullah Masfer Alhayani

School of Information Systems, Computing and Mathematics

Brunel University

May 2013

Dedication

I would to dedicated this thesis to my late father (GOD bless his soul and my lovely mother GOD bless her soul too). She the driver force behind my life by her continouse prayer for me.

(And lower unto them the wing of submission and humility through mercy, and say: “My Lord! Bastow on them Your Mercy as they did bring me up when i was a child.”)

Acknowledgement

I dedicate my special thank to my supervisor Dr. Georege Ghinea, for his contiouse, endless help and support thourghout my PhD research programme even in his private time and to my family for their patient and support.

Publications

The following papers still under review as a direct result o the research discussed in this thesis:

Under Review

1. Alhayani, A & Ghinea, G "The Significance of Developing Information System Security in Saudi Arabian Financial Institutions: An Analysis of Interview with Mangers”

2. Alhayani, A & Ghinea, G "Information System Security, Threats, and Needs for Improvement: Assessment of Data Obtained from Saudi Financial Organisations"

“Implementation, management and dissemination of information security: An organisational perspective of financial institutions”

ABSTRACT

The objective of this thesis is to investigate the significant perceived security threats against information security systems (ISS) for information systems (IS) in Saudi organisations. An empirical survey using a self-administered questionnaire has been carried out to achieve this objective. The survey results revealed that almost half of the responded Saudi organisations have suffered financial losses due to internal and external IS security breaches. The statistical results further revealed that accidental and intentional entry of bad data; accidental destruction of data by employees; employees' sharing of passwords; introduction of computer viruses to IS; suppression and destruction of output; unauthorised document visibility; and directing prints and distributed information to people who are not entitled to receive are the most significant perceived security threats to IS in Saudi organisations. Accordingly, it is recommended to strengthen the security controls over the above weakened security areas and to enhance the awareness of IS security issues among Saudi companies to achieve better protection to their IS.

ABSTRACT 2

CHAPTER ONE: INTRODUCTION 7

1.1 OBJECTIVE & AIMS 7

1.2 BACKGROUND 8

1.2.1 E-BUSINESS SYSTEMS DEVELOPMENT AND MAINTENANCE 10

1.2.2 THREATS ANALYSIS AND RISK MANAGEMENT 10

1.3 RESEARCH QUESTIONS 11

1.4 RESEARCH SCOPE AND EVALUATION 12

1.5 SUMMARY 12

CHAPTER TWO: LITERATURE REVIEW 13

2.1 Introduction 13

2.1.1 Introduction to Saudi Arabian Conditions 14

2.1.2 Information Security Standard ISO 17799 14

2.2 Basic Security Policies 15

2.2.2 Physical, Environmental and Personal Security 19

2.2.3 Communications and Operations Security 20

2.2.4 Access Control 21

2.3 Employee Compliance 22

2.3.1 Introduction and Early Literature 22

2.3.3 Security Case Studies 25

2.3.4 Theory of Reasoned Action, Protection Motivation Theory, and other Theories 29

2.3.6 Global Information Security Survey 31

2.4 Security Infrastructure 32

2.4.1 Algorithms and Cryptographs 33

2.4.2 Setting up a PKI 36

2.4 Elements of Security Infrastructure 40

2.4.1 Secure Sockets Layer/Transport Layer Security 40

2.4.2 Mobile Computing, Mobile Code and Intelligent Agents 41

2.5 Technological Compliance: Common Criteria 42

2.6 Systems Analysis 42

2.6.1 BS 7799-Related Issues 43

2.7 Asset Classification and Control 45

2.7.1 Continuity Planning 45

2.7.2 Auditing 46

2.8 Legal Issues 47

2.8.1 Intellectual Property Rights 47

2.8.2 Privacy Rights 48

2.8.3 Providers Rights and Responsibilities 49

2.9 Inter-organzational Issues 49

2.9.1 Introduction and Coordination of Security Activities 49

2.9.2 General Interdependency 50

2.9.3 Trust Issues 51

2.10 Financial Institutions and Information Systems Security *52*

2.10.1 Introduction 52

2.10.2 Financial Security Threats 52

2.10.3 Financial Security Developments 53

2.10.4 Financial Developments and Risks 57

2.11 Worldwide Context 58

2.11.1 Demand for Strategies in Information Systems Security 58

2.12 Recent Developments in IS Security Strategy 62

2.13 Summary 67

Chapter 3: Methodology 69

3.1 Introduction 69

3.2 Significance of Research 70

3.3 Phases of Research 73

3.3.1 Phase 1: Selection of Research Direction and Rationale for the Research Design 73

3.3.2 Phase 2: Creation of Research Questions and Hypotheses 79

3.3.3 Phase 3: Selection of Sampling Techniques and Sampling 85

3.3.4 Phase 4a: Questionnaire Survey Development 87

3.3.5 Phase 4b: Interviews 93

3.3.6 Phase 5: Pilot Study 94

3.3.7 Phase 6: Primary Data Recording and Instrumentation Distribution 95

3.3.8 Phase 7: Data Analysis 98

3.4 Secondary Research and Data 99

3.5 Validity and Reliability 100

3.6 Research Ethics 100

3.7 Limitations of Study 101

3.8 Summary 102

Chapter 4: Description of Context/Case 103

4.1 Saudi Arabian Context 103

4.1.2 Key Saudi Arabian Conditions 103

4.1.3 Present Demand for Improved Strategies in Saudi Information Systems Security 104

4.1.4 Developments Contributing to or Affecting Present Context in Saudi Arabia 106

4.1.5 Incomplete Elements of Implementation in Saudi Arabia 109

4.1.6 Other Aspects of Existing Threats 111

4.1.7 ISO 27000 Compliance 112

4.2 Saudi Banking Industry and Significance of Sampled Organisations 114

4.3 Conclusion 115

Chapter 5: Results and Analysis 116

5.1 Introduction 116

5.2 Pilot Study and Distribution 116

5.2.1 Demographic and Misc. Information 117

5.3 Hypotheses 120

5.4 Questionnaire Results 121

5.4.1 Questions 1-6: Threats and IS Development 122

5.4.2 Questions 7-13: Policies and Procedures 125

5.4.3 Questions 14-17: Security Threats 129

5.4.4 Questions 18-23: Ethics, Focus, and Improvements 131

5.4.5 Questions 24-27: Training, Devotion of Efforts, and Adequacy of Technology 134

5.4.6 Questions 28-30: The Importance of Information Systems, Information System Security, and Information System Security Policy 137

5.4.7 Supplemental Data: Organisations, Employee Quantities, and Size of IT/IS Departments (completed by researcher) 138

5.4.8 Basic Implications of Results in Relation to Literature 140

5.5 Interview Results and Analyses 142

5.6 Chapter Summary and Closing Remarks 161

Chapter 6: Recommendations 162

6.1 Introduction 162

6.2 Fundamental Areas of Recommendation 162

6.3 Addressing Saudi Arabia's Developing Need for Security 166

6.4 Policy Recommendations Regarding Employees and Questionnaire Topics 170

6.5 Policy Recommendations Regarding Managers and Interview Topics 177

6.6 Summary and Implications to Stakeholders 179

Chapter 7: Evaluation of Stakeholder Recommendations 183

7.1 Introduction 183

7.2 Stakeholder Recommendations 184

7.2.1 Sampling 184

7.2.2 Instrumentation 185

7.2.3 Results 188

7.3 Evaluation 197

7.3.1 Introduction 197

7.3.2 Stakeholder relations 197

7.3.3 Management 198

7.3.4 Combined evaluations 199

7.4 Summary 202

Chapter 8: Discussion, Conclusions, and Final Recommendations 203

8.1 Introduction 203

8.2 Discussion 203

8.3 Conclusions 211

8.4 Limitations of Study 218

8.5 Recommendations for Future Research and Development 219

8.5.1 Areas in need of change: Potential for progressive development or research 219

8.5.2 Tailoring policy 220

8.5.3 Saudi Arabia and further research 221

8.6 Closing Commentary 221

REFERENCES 223

Appendices 239

Appendix A: Questionnaire 239

Appendix B: Interview Transcripts 242

INFORMATION SYSTEMS SECURITY

CHAPTER ONE: INTRODUCTION

1.1 OBJECTIVE & AIMS

The aim of this study is to identify demands and potential for improvement in information security. More specifically to identify threats to information security in financial institutions in Saudi Arabia. To this end, the corresponding objectives are to :

1. Identify how such threats to information security are unique to the banking industry,
2. Identify the factors that influence employees' willingness to following information security (IS) policies and procedures industry
3. Examine the personal ethics of the employees as they relate to adherence to policies or in other words for determination if employees are honest in their dealing,
4. Examine the current modes of presentation for information security (IS) policy to determine if these affect the employee's willingness to follow them
5. Assess the importance of organisational characteristics that may affect employee compliance with policies
6. Develop and design a set of guidelines for Saudi banking institutions that will enable them to establish more effective information security systems, policies and procedures

1.2 BACKGROUND

The rapid change in information technology, the widespread of user-friendly systems and the great desire of organisations to acquire and implement up-to-date computerised systems and software have made computers much easier to be used and enabled accounting tasks to be accomplished much faster and more accurate than hitherto.

On the other hand, this advanced technology has also created significant risks related to ensuring the security and integrity of information system (IS). The technology, in many cases, has been developed faster than the advancement in control practices and has not been combined with similar development of the employees' knowledge, skills, awareness, and compliance. Every day, there is potential in accounting and financial operations for computer related data errors, incorrect financial information, violation of internal controls, thefts, burglaries, fires and sabotage. Organisations should be aware with the potential security threats that might challenge their IS and implement the relevant security controls to prevent, detect and correct such security breaches. Although considerable efforts have been made by practising accountants to reduce the vulnerability of IS to such events, it is argued that an increased effort is still required (Abu-Musa, 2001 and 2003).

Furthermore, security of information systems (IS) is becoming a part of core business processes in every organisation. Companies are faced with contradictory requirements to deal with open systems on the one hand and assure high protection standards on the other. Appropriate treatment of related issues is far from trivial and requires a wide spectrum of knowledge, ranging from technology and organisation to legislation. There are various approaches in the literature, some of them being almost exclusively technical, e.g. (Stallings, 1999), some of them hardly mentioning security issues, e.g. (Harmon, 2001); some of them covering mainly human factors in organisational issues, e.g. (Wysocki, 1997), and some of them mentioning only legal issues, e.g. (Powers, 2001). Therefore, a coherent conceptual model is needed to manage E-business systems security effectively by deploying existing approaches in a balanced way. Accordingly, this thesis addresses these topics through integration of relevant areas, and it bridges the gaps between practitioners of various profiles that are involved in IS security.

To protect information, an organisation has to start with the identification of threats related to business assets. Based on threats analysis, a layered multi-plane approach is proposed. The first plane is focused on interactions, starting with security mechanisms and therefore deploying security services which are linked to human-machine interactions. Finally, human interactions have to be covered. In parallel, to make things operational, it is necessary to address another perspective, which includes technological, organisational and legislative planes (Figure 1).The detailed methodology, based on the above model, is presented in this thesis with diagrams. These diagrams state inputs, processes and outputs, which capture necessary business activities for management of IS security. They are explained in the text, which includes the background knowledge that is necessary to understand related issues.

The chapter is organised as follows. In the next section, systems development and maintenance is covered, which includes threats analysis, security infrastructure, public key infrastructure and additional elements of security infrastructure. It addresses the practitioner's dilemmas about costs, outsourcing, complementary and substitutive technologies. In the third section, security policy is being evaluated. It concentrates on human resources management issues with addressing of organisational and legislative issues, including continuity planning, auditing and inter-organisational issues.

1.2.1 E-BUSINESS SYSTEMS DEVELOPMENT AND MAINTENANCE

It is the starting point for E-business systems development and maintenance that is covered in the next section.

1.2.2 THREATS ANALYSIS AND RISK MANAGEMENT

Threats are the starting point of E-business systems security and the procedure goes as follows (Broder, 2000; Raepple, 2001; Arce, 2002):

1. Make a complete record of organisation' s assets and resources.
2. Identify threats by taking motivation of a potential attacker and the human factor into account. Avoid common assumptions that only bright and knowledgeable people can exploit security bugs, and that attackers are always motivated by illegal tendencies.
3. For each threat in Step 2 define its possibility E(x).
4. Determine damage costs D(x) related to each threat.
5. Evaluate risks by calculating expected damage — D(x)*E(x).
6. Define an action plan by setting priorities, where investment for preventing threats should not exceed damage costs.
7. Decide for arrangements with insurance companies to complement the organisation's own measures and to compensate damage in worst-case scenarios (Figure 3).

One should not overlook the fact that threats also include non-operational IT infrastructure because of improper design that leads to overload and technical failures.

Finally, expertise should not be limited just to computer-related issues, but also to general business risks, e.g. costs caused by interrupted operations. Although the procedure looks straightforward, threats analysis is not a trivial task. The main problem is to determine E(x). Due to the nature of the security business, a large number of attempts remain undiscovered and getting accurate figures is close to impossible. Therefore, an organisation should use various sources: its own data, data collected by other professional organisations and data obtained by hired system attackers. A promising approach is to deploy techniques that are used to stimulate innovation processes (Likar, 2001) by focusing on security threats.

1.3 RESEARCH QUESTIONS

Research questions addressed in the research of this study include those as follows:

(1) What are primary threats affecting information security in financial institutions within Saudi Arabia?

(2) How are these threats unique to this sector?

(3) What policies and procedures are currently in place?

(4) How well do employees follow information security policies and procedures?

(5) What factors affect the willingness of employees to comply with policies and procedures?

(6) How do personal ethics affect compliance with policies and procedure?

(7) How do various institutional factors impact employees' willingness to comply with policies and procedures?

(8) Are there aspects of the current information security policies or procedures that make it difficult for employees to comply?

(9) How do overall organisational characteristic affect the successful execution of information security success?

(10) What improvements can be made to increase effectiveness of information security operations?

1.4 RESEARCH SCOPE AND EVALUATION

The research presented is not technical in nature, and rather addresses important issues in management, auditing, and issues related to quality; the scope of the research deals with these areas only, but applied in a manner intended to help bring awareness and encourage changes in information security.

The work applies the research objectives and instrumentation towards the development of recommendations, combined with those having been published in literature, and present a discussion of potential solutions, recommendations for the future direction of research, other relevant implications, and limitations. The capacity to do this is considered the successful completion of the research objectives, and the shortcomings of the paper are to be addressed through recommendations for continuing (and improved) studies in the topic areas.

1.5 SUMMARY

Summarising the chapter, it is evident that researchers have commonly found problems in Saudi Arabian institutions, while the research aims to assess multiple aspects of this problem while addressing the research objectives. The following chapter provides an extensive review of literature before moving to a chapter better detailing the methodology applied for data recording and analysis.

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

The following literature review discusses Saudi Arabia, information security, systems, and management in a variety of contexts. The objective of this review is to lay a solid foundation for the study outlined in the following chapter. The study will be designed on the assumptions of the theories of this review, the considerations of discussions will use it as a foundational for recommendations, and other aspects of the analysis will relate back to it.

Moreover, Althaneer and Nelson state that information security and IS management are essential parts of the ICT infrastructure required to support the development of the Saudi Arabia economy (2009). A lack of a mature approach to information security management could cause significant damage to Saudi organisations and the national economy. To address this, the Saudi government has encouraged the establishment of secure environments in both sectors (public and private). It has also established ICT infrastructures to increase the productivity and performance of organisations and individuals in Saudi Arabia. As a result, adopting an IS culture and practices within Saudi organisations is a major challenge to be dealt with to protect their economic assets from attacks and intruders (Althaneer and Nelson, 2009).

The following subsections provide a review of Saudi Arabian conditions, basic security policies, access control, development, theory of reasoning, global relevance, security infrastructure, asset classification, inter-organisation issues, and operations and regulations in financial institutions.

2.1.1 Introduction to Saudi Arabian Conditions

Saudi Arabia is reported to be a developing country; however it is stated that "*Despite this status, Saudi Arabia is the largest economy in the Middle East, comprising 25% of the Arab world's GDP. Previous plans drove ICT development between 1990 and 2000 and emphasised the improvement of education, financial, legal and technical skills to create private sector employment opportunities for Saudi citisens*" (Althaneer and Nelson, 2009). It is reported that a National Communications and IT Plan (NCITP) was developed in 2005 as part of the 8th economic development plan. Two components make up the NCITP: (1) A five-year plan for Communications and IT in the country; and (2) A long-term perspective for Communications and IT in the country (Althaneer and Nelson, 2009).

2.1.2 Information Security Standard ISO 17799

ISO 17799, though not a formal requirement, is becoming the standard of information security across businesses. Its role has become increasingly important to success in business and the selection of security frameworks (Myler and Broadbent, 2006). The standard establishes guidelines and principles for developing, integrating, enhancing, and otherwise using information security management.

ISO was initially developed in 1989 as a code of practice for users (and derivative of BS 7799), and would not become a code of practice for information security management for another six years (Carlson, 2001). The code was expanded in 1998, revised the following year, and continues to be refined as needed. Its basic structure consists of 11 security control clauses, encompassing the areas of security policy, organisation information security, asset management, human resources security, physical and environmental security, communications and operations management, access control, information systems acquisition, information security incident management, business continuity management, and compliance (Myler and Broadbent, 2006; Carlson, 2001).

ISO 17799 is not technologically driven nor a technical standard, however it is a widely recognised standard for best practices.

2.2 Basic Security Policies

Security policies serve as the basis for development for additional developments within an organisation, while they naturally serve as the foundation for employee regulations and managerial action. Numerous researchers have considered strategic developments and potential for improvements on this topic.

In addition, Alfawaz, Nelson, and Mohannak (2009) reported that the importance of issues that are non-technical has received little attention, since most studies are quantitative studies that fail to consider the role of human factors (including those of individual choice and behavior. The role of organisational factors such as national and organisational culture, environment, and levels of information security awareness have also been little studied in their relation to their affect on information security in the organisation. The work of Vroom and von Solms (2004) is stated to have shown that these determinants are critical in organisational information security management.

More recent developments have attempted to better consider the behavioural aspects of security protocol and management. The work of Dhillon *et al.* (2007) states that "*computer crime committed by internal employees is essentially a rational act that may result from internal or* *external factors*" (Alfawaz, Nelson, and Mohannak, 2010). It is asserted by Dhillion *et al*. (2007) cited in Alfawaz, Nelson, and Mohannak, 2010) that "*behavioural security holds the key to successful information system security management*." (Alfawaz, Nelson, and Mohannak, 2010). It is significant that the risk posed by data by insiders should be monitored and managed carefully. This risk is stated to take two forms: (1) the risk posed by malicious insiders who deliberately leak sensitive data for personal or financial gain or other criminal purposes; and (2) the risk from insiders who intentionally expose data (Alfawaz, Nelson, and Mohannak, 2010).

Later, the work of Alnatheer and Nelson (2009) entitled: "*A Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context*" states that "*...An examination of Information Security (IS) and Information Security Management (ISM) research in Saudi Arabia has shown the need for more rigorous studies focusing on the implementation and adoption processes involved with IS culture and practices*" *(*Alnatheer and Nelson, 2009, pp.67). Alnatheer and Nelson (2000) state that information security can be defined as "*the prevention of and recovery from, unauthorised or undesirable destruction, modification, disclosure, or use of information and information resources, whether accidental or intentional*." Information security involves three basic services as: i) confidentiality of sensitive information, which is concerned with preventing disclosure of information to unauthorised users, ii) integrity, which is concerned with ensuring data cannot be modified without authorisations, and iii) availability, which is concerned with ensuring information must be available to authorised users when they require them (Althaneer and Nelson, 2009).

Meanwhile, the legal and regulatory framework and environment in regards to ICT is still under development. International practices for information system security (ISS) are stated to be based upon the "*combined experiences of several influential international companies concerning the way in which they manage their information security*." (Althaneer and Nelson, 2009) ISM standards are utilised in the establishment and maintenance of a secure environment for information as well as for assist senior management in monitoring and controlling their security and in minimisation of any business risk that is residual in nature and for making sure that security fulfill the corporate, customer and legal requirements in an ongoing manner (Althaneer and Nelson, 2009). The code of practice gives recommendations on information security management to those responsible for initiating, implementing or maintaining an organisation's security. Initially, there has to be a person (information security manager) or a body (information security group) that is responsible for establishment, maintenance and review of security policy. Security policy has to be reviewed independently, whether internally or preferably, by an external specialised organisation.

The contention of Alfawaz, Nelson, and Mohannak (2010) is that a culture "*that encourages ethical conduct and commitment to compliance with information security requirements is a desirable organisational attribute.*" This was earlier affirmed in the research of (Chia *et al*. (2002, Ruighaver *et al*., 2007), Schlienger and Teufel, 2002, 2003; Zakaria and Gani, 2003; Zakaria, 2004) who all indicate that organisations are required to take *"...affirmative steps to create an environment where security is "everyone's responsibility" and doing the right thing is the norm*." (Alfawaz, Nelson, and Mohannak, 2010).

2.2.1 Security Technology and Breaches

Even technologically superior solutions will be in vain without complementary organisational aspects, because many successful attacks have nothing to do with sophisticated kinds of technological attack (Anderson, 1994). Thus, risk management should address human resource management through organisational and legislative issues.

In addition, the security policy is defined by procedures that set out an organisation's approach to managing security. It is vital that this policy is based on management commitment. The policy document should include the definition of information security, basic terms, its objectives and scope, brief explanations of principles, standards and compliance requirements, a definition of responsibilities for information security management and references to documentation that supports the policy. The basic standard in this area is BS 7799 (BSI, 1999), which has recently been accepted as an international standard (ISO, 2000). It is recommended that organisations follow closely this standard as the main methodology for establishing security policy.

Information security breaches are known to cause harm that is irreparable and which shuts down business computers; such destructive processes can ultimately result in the loss of data, potential revenue, the possibly leaking of confidential information from the organisation, and even making the organisation "*vulnerable to legal and regulatory problems and bad publicity.*" (Siponen, Mahmood and Pahnila, 2009, p.1) Siponen, Mahmood and Pahnila (2009) report that the majority of organisations have more than one information security breach each year. In addition, it is reported that additional studies on information security research reveal that 91% of organisations' own employees fail frequently to adhere to information security policies which only paves the path for security breaches to occur.

The work of Schlienger and Teufel (2003) and Zakaria Jarupunphol and Gani (2003) as well as Vroom and von Solms (2004) indicates that it is "*imperative that the organisational culture reflects a positive attitude toward information security in the entire organisation*" (Althaneer and

Nelson, 2009). It is stated that there is no sure and solid agreement on the definition of the '*security culture*' or what precisely constitutes '*security culture*'. Information Security Management factors are examined in the work of Althaneer and Nelson who state that the four specific areas examined are those of, corporate citizenship, legal regulatory environment, corporate governance, cultural factors (2009). Naturally, the employee and employee policies are critical factors in any organisational culture, while there has been an abundance of literature concerning employee compliance.

Reviewing the nature of security breaches that occurred in different parts of the world, Dhillon (1999) argued that many of the security losses resulting from computer-related fraud could be avoided if financial institutions adopted a more pragmatic approach in dealing with such incidents; as well as adopting a balanced approach of security controls which place equal emphasis on technical, formal and informal interventions to their computerised systems. The results of Dhillon's study (1999) suggested that implementing controls, as identified in a security policy, would indeed deter computer misuses. Committing computer fraud by insiders is recognised as a severe problem which could be difficult to prevent especially when it blends with legitimate transactions.

2.2.2 Physical, Environmental and Personal Security

Cryptographic mechanisms only reduce the need for physical protection, but they cannot eliminate it. Thus, physical and environmental security has to be addressed carefully. This kind of protection should include issues about clear-desk policy, locking of sensitive information, logging off the system, prevention of unauthorised photocopying, immediate clearance of sensitive information from printer, appropriate use of passwords etc. In order to prevent unauthorised access, secure areas have to be defined. Physical entry controls should include supervision of visitors, recording of their entry and departure, and providing visitors with instructions. Moreover, they should also wear some form of visible identification. Securing offices, rooms and facilities should consider possibilities of theft, dust, excessive vibration, electrical interference, electromagnetic radiation, proper cabling and maintenance, fire, flood, smoke, explosions and other forms of natural and man-made disasters. Facilities should be located in a way that prevents public access, buildings should give a minimum indication of their purpose, and support equipment (faxes, photocopiers) ought to be sited properly. Further, protected windows and slam shut doors should be considered, suitable intrusion detection systems and alarms should be in place, as well as smart card-based control throughout the building. Hazardous materials, fallback equipment and back-up media should be stored at a safe distance. Working in secure areas has to be properly related to working in delivery and loading areas. The basis of security in every organisation is informed, educated, and loyal employees. This is the most paramount factor for minimisation of human error, misuse, fraud and theft (Althaneer and Nelson, 2009).

2.2.3 Communications and Operations Security

Special attention has to be paid to internal communications and operations; operating procedures should be documented and every change formally approved. Segregation of duties is one of the main principles to reduce the risk of system misuse. Certain groups of procedures that might be easily overlooked, but may present a significant threat, are:

- Sufficient attention is not paid to event logs, especially their integrity and regular analysis, which are essential for detecting suspicious behavior and for cases of legal dispute.

• Media management is considered sufficiently (transport of media, its exchange and disposal), e.g. high security measures are conducted within an organisation, but neglected when transporting back-up copies to a remote location.

• Minor operations are overlooked: clocks are not synchronised, equipment is left unattended, automatic time-out procedures are not implemented, software is not upgraded on time, mobile phones are used for sensitive communication in public places, passwords are poorly managed, faxes are sent to wrong numbers, etc.

• Equipment that is used off-premises; management should authorise every such use and this equipment should not be unattended, and additional adequate insurance cover for such equipment should be considered (Althaneer and Nelson, 2009).

2.2.4 Access Control

The introduction of networked and Web-centric information systems requires a security policy that clearly defines the use of network services, necessary user and node authentication, physical segregation of networks, enforced paths for services, and filtering and limitation of connection time for high-risk applications. Regarding data access within an organisation, it is advisable to manage information propagation using the Bell—La Padulla model (Bell, 1973) with its ‘no write down’ and ‘no read up’ principle. This principle assures that sensitive information can only propagate horizontally and upwards, so there is no leakage of confidential information; it is especially suitable for hierarchical organisations. Regarding an important technological threat to access controls, steganography should be mentioned (Katzenbeisser, 1999).

2.3 Employee Compliance

2.3.1 Introduction and Early Literature

Employee complaince has been considered from many angles for decades by notable theorists. It is noted that the work of Fishbein and Ajzen (1975) presents the theory of reasoned action (TRA) which seeks to explain "*that an individual's behaviour or action is determined by his or her intention to perform such behaviour*." (Alfawaz, Nelson, and Mohannak, 2010, pp.53) Therefore, TRA "*considers that behavior is determined by intention – which is in turn influenced by the individual's attitude towards performing that behavior, and subjective norms (social pressures to perform the behaviour)"* (Alfawaz, Nelson, and Mohannak, 2010). The theory of reasoned action and its extension the Theory of Planned Behavior (TPB) in the work of Ajzen (1985) is stated to have been applied in various studies regarding information security issues and specifically in risk perception, and security-related behaviour. Each of these theories is stated to suggest that 'ease of use' is a critical factor that affects the behaviours of humans.

2.3.2 Security and Modes of Behaviour

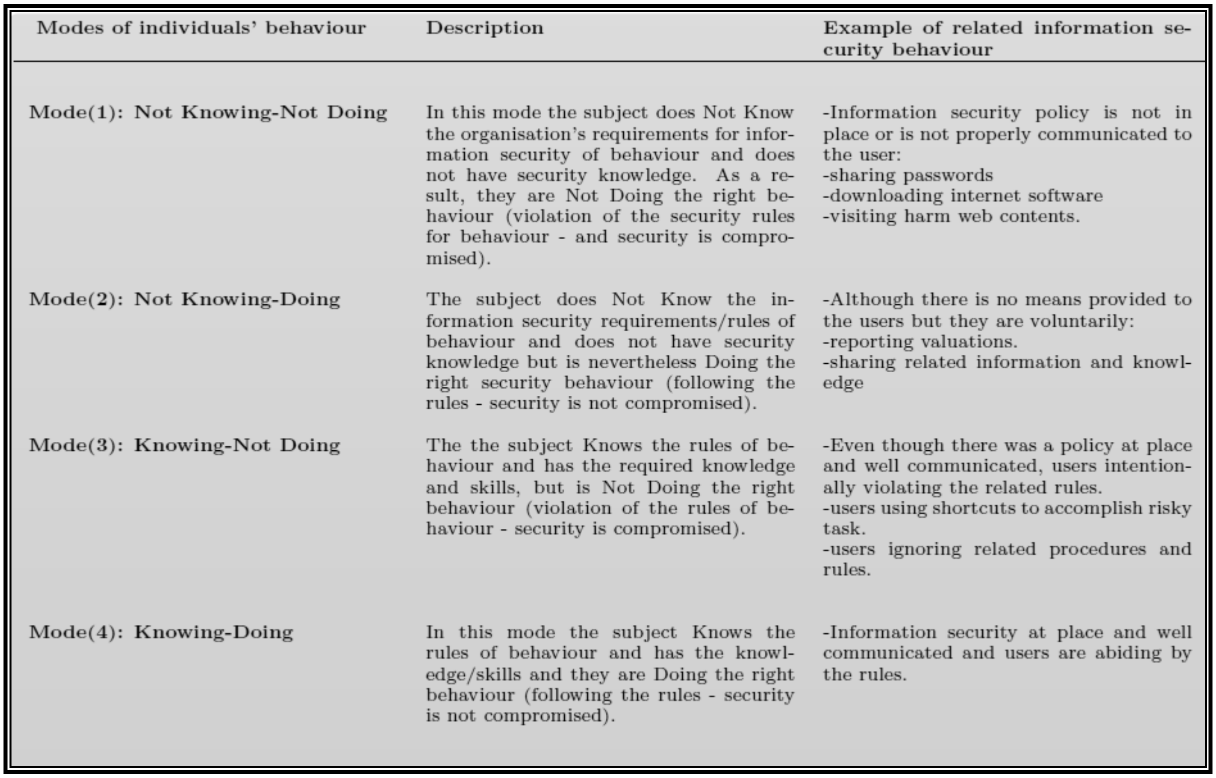
The work of Siponen (2000) states findings that the issues associated with 'ease of use' of security solutions "*has not been well addressed in the security literature*" (Alfawaz, Nelson, and Mohannak, 2010). While earlier research has indicated that several factors are critical to information security policy adherence and user awareness, most of these studies have failed to address the influence of national and/or organisation culture to employees attitudes, beliefs and behaviors, or to the interactions between individuals and their context (Alfawaz, Nelson, and Mohannak, 2010). Alfawaz, Nelson, and Mohannak (2010) also state that, on the basis of the individual’s acknowledgement of the security rules and possession of the required skills for performing certain actions, they identify four modes to categorise individual security behaviours. These comprise: (1) knowing-doing mode; (2) knowing-not doing mode; (3) not knowing-not doing mode; and (4) not-knowing doing mode (2010). Each of these modes are defined as Mode 1, Mode 2, Mode 3, and Mode 4. With this, the authors defined the categories.

Mode (1)- Not Knowing-Not Doing: In this mode, which falls into the upper right corner of the model of information security behaviour modes, the subject does Not Know the organisation’s requirements for information security of behavior and does not have security knowledge. As a result, they are Not Doing the right behaviour (violation of the security rules for behaviour - and security is compromised);

Mode (2)- Not Knowing-Doing: This second mode falls into the upper left corner of the model. The subject does Not Know the information security requirements/rules of behaviour and does not have security knowledge but is nevertheless Doing the right security behaviour (following the rules - security is not compromised);

Mode (3)- Knowing-Not Doing: In this third mode, which takes the lower left corner of the model, the subject Knows the rules of behaviour and has the required knowledge and skills, but is Not Doing the right behaviour (violation of the rules of behaviour security is compromised);

Mode (4)- Knowing- Doing: In this mode, which takes the lower right corner of the model, the subject Knows the rules of behaviour and has the knowledge/skills and they are Doing the right behaviour (following the rules - security is not compromised) (Alfawaz, Nelson, and Mohannak, 2010). Figure 1 below provides a description of modes of behavior.



Modes of individuals' behaviour	Description	Example of related information security behaviour
Mode(1): Not Knowing-Not Doing	In this mode the subject does Not Know the organisation's requirements for information security of behaviour and does not have security knowledge. As a result, they are Not Doing the right behaviour (violation of the security rules for behaviour - and security is compromised).	-Information security policy is not in place or is not properly communicated to the user: -sharing passwords -downloading internet software -visiting harm web contents.
Mode(2): Not Knowing-Doing	The subject does Not Know the information security requirements/rules of behaviour and does not have security knowledge but is nevertheless Doing the right security behaviour (following the rules - security is not compromised).	-Although there is no means provided to the users but they are voluntarily: -reporting valuations. -sharing related information and knowledge
Mode(3): Knowing-Not Doing	The the subject Knows the rules of behaviour and has the required knowledge and skills, but is Not Doing the right behaviour (violation of the rules of behaviour - security is compromised).	-Even though there was a policy at place and well communicated, users intentionally violating the related rules. -users using shortcuts to accomplish risky task. -users ignoring related procedures and rules.
Mode(4): Knowing-Doing	In this mode the subject Knows the rules of behaviour and has the knowledge/skills and they are Doing the right behaviour (following the rules - security is not compromised).	-Information security at place and well communicated and users are abiding by the rules.

Figure 1: (Alfawaz, Nelson, and Mohannak, 2010)

Other work has considered the effectiveness of awareness and the consequences of non-compliance. The work of Deloitte, Touche, and Tohmatsu (2005) state that approximately "*45% of global organisations are not sensitive their employees in respect of possible information security threats, and this lack of information security awareness could well lead to compromised information within the organisation*" (cited in: Althaneer and Nelson, 2009). The work of Siponen, Mahmood and Pahnila (2009) states that employees who are careless and fail to follow information security policies "*constitute a serious threat to their organisation*" (p.1). Siponen, Mahmood and Pahnila (2009) further report the results of their own field survey, for the purpose of providing an understanding of which factors assist in the compliance of employees with security policies, and showed that the visibility of practices and normal expectations of peers offer a solid foundation toward employees that are compliant with the policies; beyond this, the research found that when employees see the vulnerability of their organisation in relation to security threats, and once they understand these threats, they are more likely to be driven to be compliant with policies.

2.3.3 Security Case Studies

The work of Alfawaz, Nelson, and Mohannak (2010) entitled: "*Information Security Culture: A Behaviour Compliance Conceptual Framework*" states that understanding the complex and sometimes unknown traits of organisational employees that have a role with security activities. It is related that studies have demonstrated that "*non-technical issues are at least as important as technical issues in safeguarding an organisation's sensitive information*" (Alfawaz, Nelson, and Mohannak, 2010, p.2).

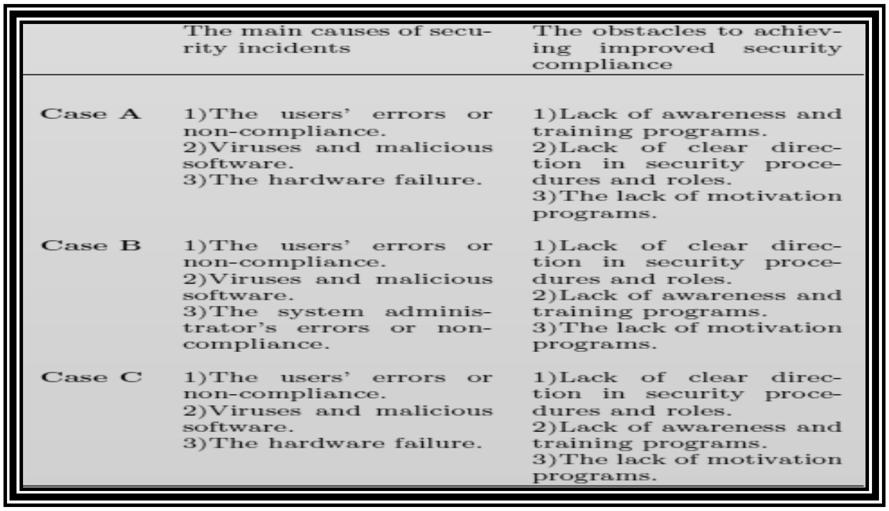
Alfawaz, Nelson, and Mohannak (2010) report findings from three exploratory case studies that were reported to be conducted in organisations in Saudi Arabia. The organisations studies and reported on are as follows:

> **Case A** – a private organisation with more than 5,000 employees;
>
> **Case B** – participants from public organisations; and
>
> **Case C** – a non-profit organisation which employs approximately 3,600 people in Saudi Arabia. (Alfawaz, Nelson, and Mohannak, 2010)

Sources of data for interviews are stated to have included senior managers, information security managers, functional managers, IT specialists, and IT users in each of the case study organisations.

Furthermore, participants from all three organisations were asked to identify three primary causes of security incidents and the barriers to achieving improved IS security compliance in their organisation. It is reported that the interview data from the three cases demonstrated that *"behavioural issues associated with users' security compliance behavior were the most common of all concerns*" (Alfawaz, Nelson, and Mohannak, 2010).

Issues were stated to include password sharing, using shortcuts, downloading Internet software, surfing potentially harmful content, ignoring relevant procedure, not sharing information and knowledge relevant to information security practices, not reporting security violations, and not enforcing security related rules (Alfawaz, Nelson, and Mohannak, 2010). Figure 2 below shows cases and obstacles to improving compliance in security.



	The main causes of security incidents	The obstacles to achieving improved security compliance
Case A	1)The users' errors or non-compliance. 2)Viruses and malicious software. 3)The hardware failure.	1)Lack of awareness and training programs. 2)Lack of clear direction in security procedures and roles. 3)The lack of motivation programs.
Case B	1)The users' errors or non-compliance. 2)Viruses and malicious software. 3)The system administrator's errors or non-compliance.	1)Lack of clear direction in security procedures and roles. 2)Lack of awareness and training programs. 3)The lack of motivation programs.
Case C	1)The users' errors or non-compliance. 2)Viruses and malicious software. 3)The hardware failure.	1)Lack of clear direction in security procedures and roles. 2)Lack of awareness and training programs. 3)The lack of motivation programs.

Figure 2: The Primary Causes of Security Incidents and Obstaclesto achieving Improved Security Compliance (Alfawaz, Nelson, and Mohannak, 2010)

The following figure (Figure 3) illustrates the relation of the information security issues to each of the four modes used for assessment in the study of Alfawaz, Nelson, and Mohannak (2010).

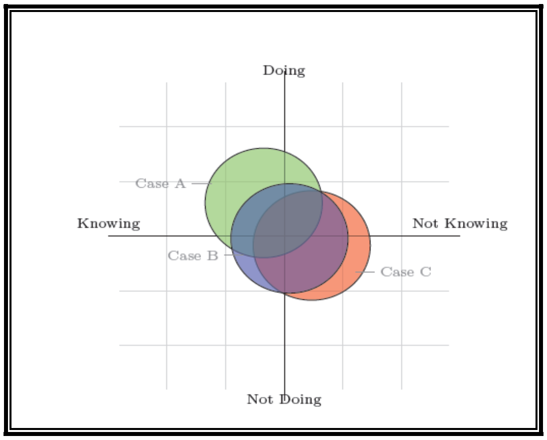
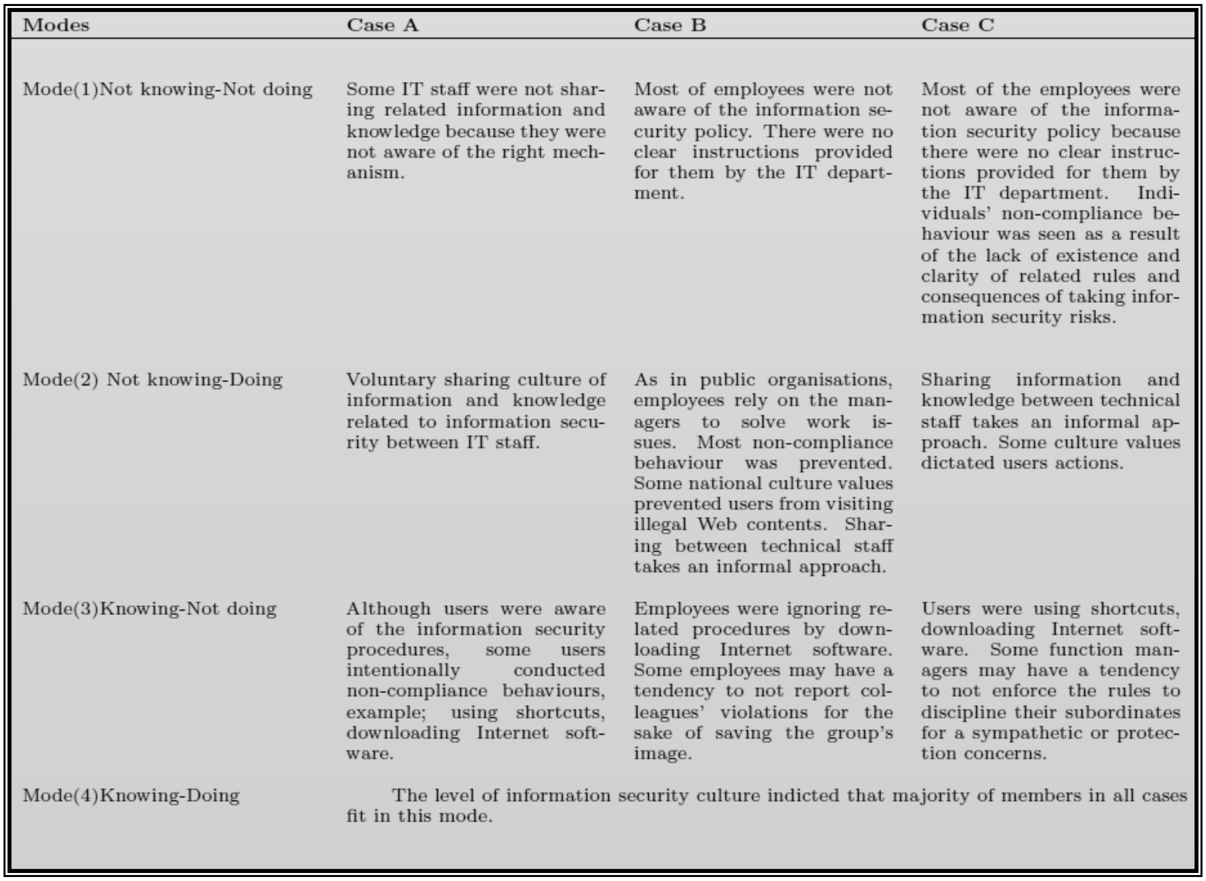


Figure 3: Information Security Behaviour Modes (Alfawaz, Nelson, and Mohannak, 2010)

Additional analysis conducted by Alfawaz, Nelson, and Mohannak (2010) resulted in the findings shown in the following figure (Figure 4) which states the reason why these issues were present in each organisation.



Modes	Case A	Case B	Case C
Mode(1)Not knowing-Not doing	Some IT staff were not sharing related information and knowledge because they were not aware of the right mechanism.	Most of employees were not aware of the information security policy. There were no clear instructions provided for them by the IT department.	Most of the employees were not aware of the information security policy because there were no clear instructions provided for them by the IT department. Individuals' non-compliance behaviour was seen as a result of the lack of existence and clarity of related rules and consequences of taking information security risks.
Mode(2) Not knowing-Doing	Voluntary sharing culture of information and knowledge related to information security between IT staff.	As in public organisations, employees rely on the managers to solve work issues. Most non-compliance behaviour was prevented. Some national culture values prevented users from visiting illegal Web contents. Sharing between technical staff takes an informal approach.	Sharing information and knowledge between technical staff takes an informal approach. Some culture values dictated users actions.
Mode(3)Knowing-Not doing	Although users were aware of the information security procedures, some users intentionally conducted non-compliance behaviours, example; using shortcuts, downloading Internet software.	Employees were ignoring related procedures by downloading Internet software. Some employees may have a tendency to not report colleagues' violations for the sake of saving the group's image.	Users were using shortcuts, downloading Internet software. Some function managers may have a tendency to not enforce the rules to discipline their subordinates for a sympathetic or protection concerns.
Mode(4)Knowing-Doing	The level of information security culture indicted that majority of members in all cases fit in this mode.		

Figure 4: Modes of Individuals' Behaviour of Information Security Culture

Source: Alfawaz, Nelson, and Mohannak (2010)

Alfawaz, Nelson, and Mohannak (2010) state that the most important of all factors that their study identified were those of top management commitment, the level of training and IT skills, security awareness programs, organisational IT structures, the appointment of information security managers, type of motivation system utilised, and the existence of information security standards (Alfawaz, Nelson, and Mohannak, 2010). Meanwhile, other determinants were further related to the national culture's influence on values in decision making, compliance, risk taking, sharing culture, collaboration, enforcement, reporting, and communications. (Alfawaz, Nelson, and Mohannak, 2010). These findings are therefore stated to be consistent with the perspectives that an individual's decision to be compliant with security requirements in not a function of knowledge and skills or their perception of how the cost benefit of behavior described in economic theories; additionally, it is important for them to consider how these aspects affect employee practices to achieve an information security culture (Alfawaz, Nelson, and Mohannak, 2010).

Moreover, a stated inherent complexity in contemporary organisations indicates that organisations will be inclusive of individuals that do not share a view of IS and who are expected anyway to participate in the security culture of that specific organisation. It is related that these disparate views "*may be attributed to the different assumptions, attitudes and values towards the information system implementation and use processes held by each employee*" (Alfawaz, Nelson, and Mohannak, 2010). In addition, it is reported that variation may be due to "*rapid* *technological advances bringing about an increase in the range of tools used for conducting unauthorised behaviors*" (Alfawaz, Nelson, and Mohannak, 2010). Furthermore, it is noted that it is the assumption of most employees that their organisation's information security is not their responsibility and that the IT staff are those responsible for organisation information security.

In order to address this situation in organisations there have been various suggestions made to assist the compliance of employees with information security policies; however there have been critiques which noted serious weaknesses in the approaches that presently exist and remarked that these approaches are lacking in empirical evidence on the effectiveness of these used in practice. Siponen, Mahmood and Pahnila (2009) state that since there is a lack of empirically validated information for practitioners, it is critical that researchers continue to study employee compliance and non-compliance trends through field research; additionally, in order to comprehend why employees can be carefully about following security policies and the factors that are important toward employees' compliance (p.1).

2.3.4 Theory of Reasoned Action, Protection Motivation Theory, and other Theories

The survey instrument used in the study of Siponen, Mahmood and Pahnila (2009) is reported to have been developed on the basis of a theoretical model that was developed from using behavioral theories including the **'**Theory of Reasoned Action' and the 'Protection Motivation Theory' (2009, p.1). It is reported that since the compliance of employees with information security policies *"...is ultimately a psychological phenomenon; we find these theories useful in understanding how organisations can help their employees comply with these security policies*" (Siponen, Mahmood and Pahnila, 2009, p.1). Siponen, Mahmood and Pahnila state additionally that they show how these theories can be useful in offering a new insight into what can motivate employees toward compliance.

Not only do underlying principle beliefs, values, and assumptions drive the behaviour of users of information security, but also complications arise due to the rate of change occurring in the information system environment and particularly in relation to security threats, therefore making it ill-advised to assume that the knowledge and skills of the individual will be up to date and that the behaviour of the individual will remain as would be expected. The stated challenge is the determination of the aspects of the organisation's environment that serve to facilitate and enable "*sustainable approaches to information security adherence*" (Alfawaz, Nelson, and Mohannak, 2010).

Additionally, Althaneer and Nelson point out that the literature on information security reveals that IS is still in early stages of development, as issues are still being found, conceptualized, and explored; here, culture has affected the formation of security measures like national security legislation. Meanwhile, security culture affects social and cultural issues as well as ethical measures in improving security operations, and thus, security culture is advised to support all types of organisational activities so that it is viewed as a natural part of daily activities for all employees (p. 6). Establishment of an organisational information security culture is critically necessary for effective information security.

2.3.5 Influence of National Culture on Policy

National cultural factors in Saudi Arabia are stated to have a tendency to be obstacles that can affect the adoption of IS cultural and practices in organisations. Althaneer and Nelson (2009) state that the theme of corporate citizenship is concerned with how employees gain an understanding of appropriate IS culture and practice through awareness raising and training programs. The notion of corporate citizenship is applied at three levels: (1) national; (2) organisational; and (3) individual (Althaneer and Nelson, 2009). Security and training and awareness programs are stated to be a "*fundamental component of effective information security strategy"* and these programs can assist the organisations in minimising some of the damage caused by misused or misinterpreted application procedures" (Althaneer and Nelson, 2009).

2.3.6 Global Information Security Survey

It is reported that a global information security survey report of 450 information security officers and IT directors demonstrated that "*less than 50 percent of employees had received information security awareness training programs*" (Althaneer and Nelson, 2009). In addition, it is reported that a 2002 security awareness index survey conducted by Pentasafe Security Technologies Inc published a report that was based on results from an online survey strategically designed to assess organisational awareness of information security (from 1350 employees in 583 companies) (Althaneer and Nelson, 2009). Findings of the survey included the following facts:

(1) 66% of security managers think that information security awareness is inadequate or dangerously inadequate,

(2) 50% of employees have never received formal information security training,

(3) 10% of employees have never read their company security policy, and

(4) 25% of employees have not read their security policy in the last two years (Security Awareness Index Survey, 2002, cited in: Althaneer and Nelson, 2009)

The work Koskosas (2009) states that while there have been various IS security approaches developed that serve to minimise security threats such as risk assessments, evaluations, and checklists; practitioners' interest has turned on social and organisational factors that may have an influence on IS security development and management. Moreover, Siponen *et al*. (2007) advanced a new model that explains employees' adherence to IS policies and found that threat appraisal, self efficacy and response efficacy have an important effect on intention to comply with information security policies. Koskosas (2009) also conducted a study among banks and states findings which compiled the conclusions from three studies, to find that goal setting was a key component of business activity agendas.

2.4 Security Infrastructure

OSI standards (ISO, 1995a) form the technological basis of security for contemporary networked E-business systems. The main representatives of symmetric cryptographic algorithms today are Triple-DES (NIST, 1999) and AES/Rijndael (Foti, 2001). Among asymmetric algorithms, RSA (RSA Labs, 2002) is a major player, while for devices with low processing capabilities like smart cards, elliptic curve-based systems are used, e.g. ECDSA (ANSI, 1998). Secure Hash Algorithm or SHA-1 (Eastlake, 2001) is an emerging standard among one-way hash functions.

2.4.1 Algorithms and Cryptographs

Cryptographic algorithms are needed to transform plaintext into ciphertext and vice versa. As a rough rule, researchers had assumed that hackers will be matched with ongoing technology, while organisations will be able to able to keep up with best practices, but newer research has shown how these projections did not come to pass in Saudi Arabia (Althaneer and Nelson, 2009; Fumy, 2000). For elliptic curve (EC)-based systems, keys can be significantly shorter — having RSA encryption with 768 bits long keys, a comparable strength can be achieved with approx. 128 bits for EC-based system, while 2 K bits of RSA gives strength that is roughly comparable to 200 EC bits. Moreover, symmetric algorithms use the same keys for encryption and decryption, while asymmetric ones use one key for encryption and another for decryption. Only the owner knows the first key, called a private key, whilst the second one can be communicated to anyone and is called a public key. When the owner of a private key encrypts a message, anyone knowing the corresponding public key can decrypt it. Consequently, the recipient can be assured of a message's origin and integrity and this is the basis for digital signature. Additionally, when a message is encrypted with a certain public key, only the owner of the corresponding private key can decrypt it to access the contents.

These properties of asymmetric mechanisms constitute the basis of modern security services. However, there are drawbacks; the first is computational complexity. These algorithms are significantly slower compared to symmetric algorithms of a similar strength. Secondly, in order for a user to know that a particular public key indeed belongs to the person claimed, a trusted third party called certification authority (CA) has to be introduced. CA issues a certificate that is a digitally signed electronic document, which assures binding between an entity and the corresponding public key. A certificate can be verified by anyone knowing CA's public key. However, every cryptographic document has a limited life span because of growing processing power and it may happen that the old key becomes insufficiently long sooner than expected. Besides, a private key may be compromised. Finally, a user may be using a certificate in a way that he/she was not supposed to. Thus, each CA maintains a certificate revocation list (CRL) that should be checked every time a certificate is used.

Protocols that use cryptographic primitives are called cryptographic protocols. They are used to implement security services, which are:

- authentication that provides for the authentication of the communicating peer entity
- confidentiality that protects the data from unauthorised disclosure
- integrity that detects any modification, insertion or deletion of data
- access control that provides against unauthorised use of resources
- non-repudiation that provides the recipient with the proof of origin and the sender with a proof of delivery, where false denying of the message content is prevented
- auditing that enables administrative recording of events for detection of suspicious activities, analysis of successful breaches and evidence for resolving legal disputes (ITU, 2000).

To provide authentication, asymmetric algorithms are used, because of their low key-management complexity. Due to computational complexity, symmetric algorithms are used for protecting sessions once entities have been authenticated. However, certificates have to be introduced in this scenario. The ultimate certificate and certificate revocation list specification for a business environment is the X.509 standard, version 3 (ITU, 2000). The main certificate fields are serial number, issuer (i.e. trusted third party), subject (i.e. an owner of a public key), the public key itself, validity and signature of a certificate. Before using a public key, the validity of a certificate has to be checked against the corresponding CRL. These checks currently have to be done manually, which is very frequently neglected in today's E-business environments. Regarding security policies (discussed in more detail in the following sections), it should be evident to a user of a certificate in what context a certain public key may be used. For example, an employee may not be allowed to sign contracts above a certain amount.

Distribution of public keys is done through a global distributed directory. The most frequently proposed system for this purpose is the X.500 directory (ITU, 1997c). Protocols to access its content (certificates, CRLs) are directory access protocol or DAP (ITU, 1997c) and lightweight directory access protocol or LDAP (ITU, 1997c). The so called Registration Authority (RA) that identifies users and submits certificate requests to CA, serves as an interface between the user and CA. In addition, a synchronised time base system is needed for proper operations. All these elements, together with appropriate procedures, form a so-called public key infrastructure (PKI).

Furthermore, other regulations in cryptography have been developed to address key issues. Cryptography has become a common practice in the business environment, as governments have recognised the importance of securing online business. At the international level, the basis for use of cryptography is presented in OECD Cryptography Guidelines (OECD, 1997). They are strongly in favour of privacy — the fundamental right of individuals to privacy (including secrecy of communications and protection of personal data) should be respected. These guidelines also state that cryptographic methods should be trustworthy in order to generate confidence. They should be developed in response to the needs, demands and responsibilities of users and governments, where users should have a right to choose any cryptographic method, subject to applicable law. Further, the liability of individuals and entities that offer cryptographic services, or hold or access cryptographic keys, should be clearly stated.

In recent years, relevant national regulations are becoming increasingly liberal to stimulate E-business processes. However, it is always significant to check the cryptography usage situation on a case-by-case basis. There might be restrictions on import and export of crypto products as well as their use. An extensive survey on regulation of cryptography can be found in (Koops, 2001).

2.4.2 Setting up a PKI

Implementation of a PKI should address a wide variety of issues:

- Operational procedures — registration, initialisation, certification, key generation, key recovery and compromise, key update and expiry, cross-certification, and revocation.
- Supporting protocols — operational and management protocols, time stamping.
- Staff-related issues — education and training.
- Hardware and software-related issues — flexibility, scalability, ease of use, costs, interoperability and standardisation.
- Consultancy for specific issues — name space management, certificate paths, trust models, etc.

The central point in establishing PKI is the CA (Figure 5). It all starts with issuing a certificate to a physically identified user who knows the corresponding private key. Malicious actions by CA operators should be minimised as much as possible. Therefore, it is a common practice that a user generates a key pair to ensure that a private key is known only to him/her. However, many threats still exist that should be minimised (Roe, 1993). Figure 5 below shows setting up a public key infrastructure.

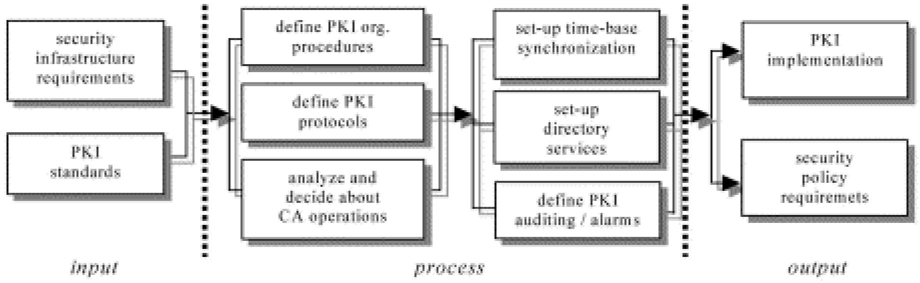

security infrastructure requirements
PKI standards
define PKI org. procedures
define PKI protocols
analyze and decide about CA operations
set-up time-base synchronization
set-up directory services
define PKI auditing / alarms
PKI implementation
security policy requiremets
input
process
output

Figure 5: Setting-up a Public Key Infrastructure (Roe, 1993).

- loss of confidentiality of private keys, including compromise of local key storage, interception during transmission from key storage unit to the processing unit, and compromise of the key generation process
- modification of data, which includes modification of certificate contents and modification of attributes prior being packaged in a certificate
- masquerade, which should consider both parties, users and CAs
- false repudiation, which includes the user denying requesting a certificate or requesting a certificate revocation
- misuse of privilege, which includes CA issuing incorrect certificates or revocation lists

In the past, trust models used to be an important topic that addressed questions like what kind of CAs would exist, what their relationships would be, etc. Efforts were made to standardise these models by introducing so called policy CAs and organisational CAs. However, after years of operations of established commercial CAs it is evident that they operate as isolated certification islands — there is almost no cross-certification.

Moreover, procedures for initial key exchange have to be defined before certificates can be issued. Initially, a user physically contacts the RA, where he/she is identified on the basis of a valid document and signs a request. The subsequent procedure may vary and it is defined locally. In the Web environment, a common business practice goes as follows. The CA maintains a Web server that supports the SSL protocol (Freier, 1996) and has installed the CA's certificate. A user, who has enrolled at RA, is sent two secret strings through two different channels, e.g. email and ordinary mail. After obtaining these strings, a user connects to the server through the browser, which automatically activates SSL, and establishes a secure session. Based on the data about the CA's certificate a user can be assured of being connected to the CA's server — usually this is done by checking key fields and a fingerprint of a certificate (a fingerprint can be obtained at RA during initial registration). Afterwards a confidential exchange of subsequent data, along with integrity, is enabled. After checking the CA's certificate, a user enters his/her personal data and secret sequence strings, which authenticate the user to the server. Then the server triggers a browser to produce a key pair and a public key is transmitted over the network for signing. When the certificate is produced, a user can download it to his/her computer, as every certificate is a public document. Once a certificate is signed, it is necessary to provide means to revoke it. For this purpose, procedures for revocation have to be defined and CRLs have to be maintained in accordance with (ITU, 2000). In the case of compromised private key, the following procedure can be done over the network — a user makes a request for revocation with the serial number of a certificate and signs it with a compromised private key.

CAs may be expected to stay in business for a long period. Therefore, they should define procedures for changing their keys (Aresenault *et al.*, 2002). Most commonly, existing digital documents will have to be re-signed, together with their old signatures using new keys. Other procedures should include operations for employees and physical access to the CA's computing resources. Educational and training requirements also have to be considered seriously.

PKI standardisation efforts started in the first half of 90s and these issues are now very complex. PKI standards that are mainly concerned with technological part of operations are defined by Internet Engineering Task Force. As an introductory reading to the wide variety of IETF PKI standards, PKI roadmap is recommended (Aresenault *et al*., 2002). It addresses and references in detail the related approaches and methodologies mentioned above.

2.4.3 When to Outsource PKI Operations

CA operations are very sensitive and require significant knowledge, manpower and financial investments; it is vital to evaluate the total costs of ownership. The first decision that needs to be made concerns outsourcing these operations.

The structure of costs then has to be defined precisely. These costs can be grouped into six main categories (Aberdeen Group, 1998):

- PKI systems: user and server certificate fees, certificate hardware and software platforms, CA and directory software.
- Client software: client software acquisition and distribution.
- Maintenance: hardware, software, disaster recovery systems.
- Services: PKI design and planning, installation and configuration, integration and testing, training, root key notarisation, cryptography health checks, audit and certification, disaster recovery services, secured facilities and procedures for logical and physical protection.

- Staffing: start up engineering costs, integration and testing, project rollout, project management, info-systems administration, certificate repository and maintenance, PKI procedures, help desk, training, security monitoring and audit.
- Risk management: transaction insurance, financial and legal liability assistance.

2.4 Elements of Security Infrastructure

2.4.1 Secure Sockets Layer/Transport Layer Security

SSL protocol was developed by Netscape as a common security layer for a variety of application protocols, with emphasis on Web services. It is positioned just below the application level. It provides authentication, confidentiality and integrity with a possibility to negotiate crypto primitives and encryption keys. Authentication includes server authentication by default and, optionally, client authentication. The session is initiated by a client and in a response a server sends its certificate and cryptographic preferences. The client then generates the master key, which is encrypted with the server's public key and returned to the server. Using its private key, the server recovers the master key and returns to the client the message encrypted with this master key. This is the basic phase, which can optionally be extended with authentication of a client, which is analogous to the basic phase with roles of client and server exchanged. At this stage, entities are authenticated and subsequent messages are encrypted with a symmetric algorithm that uses session keys derived from a master key and this provides confidentiality. A successor of SSL is TLS (Dierks, 1999) but although they are close relatives, TLS is not compatible with SSL.

2.4.2 Mobile Computing, Mobile Code and Intelligent Agents

PKI is a problem for the wireless world. It requires extensive computation for certificates and CRLs and it further narrows the available throughput (Miller, 2001). Appropriate standards that would enable a wide-scale secure deployment are yet to come, but the principles of secure operations are similar to those for fixed devices.

Furthermore, mobile code and mobile agents present a fundamentally new approach. They pass from one processing environment to another and they use the computing resources of the host. Agents are supposed to act on behalf of their users, e.g. finding the best offers, bidding at auctions, etc. Therefore, their security is crucial. Typical threats include uncontrolled read and write access to core agent services and information (e.g. agent directory services), privacy and integrity of messages and message transport services, and denial of services. Moreover, such code operates in partly predictable environments and has to be protected from malicious hosts. This introduces two new generic threats, which are code peeping and code modification through false computation (a promising method for their prevention is mobile cryptography but it is at a research phase (Sander, 1998). Speaking generally, security issues in this area have yet to be resolved (FIPA, 2001).

Firewalls are specialised computer systems, which are used primarily for access control (Cheswick and Bellovin, 1994). They operate on the border between the corporate's network and the Internet, where all traffic must pass through the firewall. Only authorised traffic is allowed to pass, which is defined by the security policy. This makes security management much easier, as the firewall presents one central point for auditing and alarms for outside attacks. It blocks potentially vulnerable services and provides additional useful features like local network hiding through address translation. All local addresses are mapped in the outgoing packets, thus making it harder for attackers to obtain appropriate data for successful attacks. Besides, firewalls can provide proxy software that receives and pre-processes requests before passing them on. Firewalls can even host exposed server software like HTTP daemons. The main limitation of classical firewalls is their inability to prevent tunneling attacks, e.g. virus attacks and Trojan horses. Of course, firewalls cannot protect against bypassing attacks, e.g. internal modem pools (Stallings, 1999).

2.5 Technological Compliance: Common Criteria

Joint harmonisation efforts are underway within ISO, called Common Criteria for Information Technology Security Evaluation — CC (ISO, 1999). However, harmonisation has not been a major focus in Saudi Arabia, or in many developing countries for that matter (Althaneer and Nelson, 2009). CC defines requirements that products have to fulfill from the security point of view and they present a base for comparing various security evaluations. Consumers can determine if a certain product is secure enough for the intended use, developers can determine desired security properties and declare them in a standardised way, and evaluators can verify them.

2.6 Systems Analysis

Exploiting vulnerabilities of poorly verified code is the main reason for denial of service attacks and their prevention is becoming critical. This is achieved with a use of formal techniques, which have to be taken into account at the process of analysis and design. Such techniques include the Unified Modeling Language (UML) (OMG, 2001), the Z language (Spivey, 1989) and BAN logic (Burrows *et al.*, 1990) .

2.6.1 BS 7799-Related Issues

BS 7799 consists of two parts. The first part describes the code of practice for information security management, while the second gives a specification for information security management systems. We will concentrate on the code of practice, which explicitly states the main areas that have to be addressed in order to produce a sound security policy (BSI, 1999) (Figure 6):

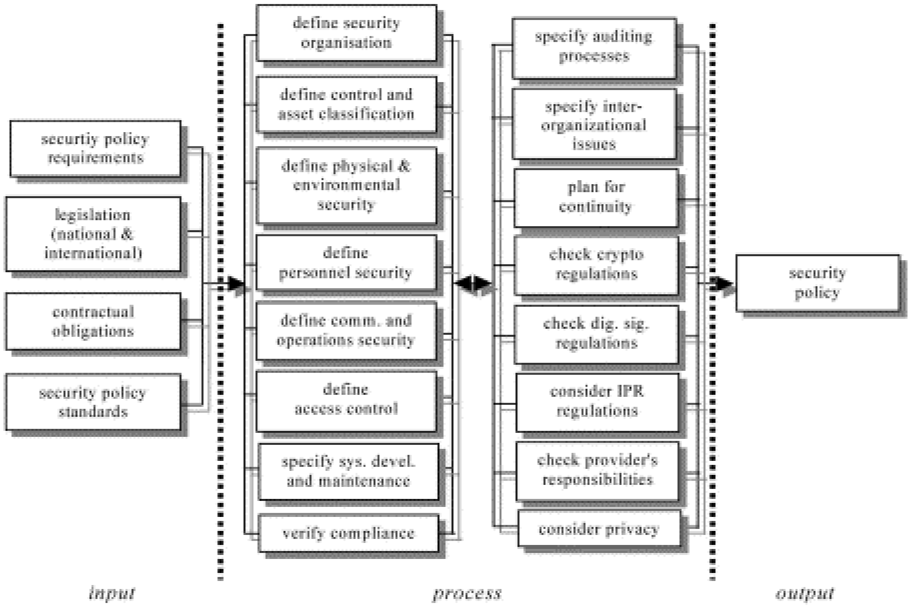

securtiy policy requirements
legislation (national & international)
contractual obligations
security policy standards
define security organisation
define control and asset classification
define physical & environmental security
define personnel security
define comm. and operations security
define access control
specify sys. devel. and maintenance
verify compliance
specify auditing processes
specify inter-organizational issues
plan for continuity
check crypto regulations
check dig. sig. regulations
consider IPR regulations
check provider's responsibilities
consider privacy
security policy
input
process
output

Figure 6. Risk Management based on BS 7799.

Figure 6 can be considered in terms of high, middle, and lower heirarchies, and what was and can be learned from this. At the upper levels of this kind of division are the macroscopic functions, the lower levels the microscopic, and the middle the processes connecting them. Changing the figure to this perspective allows analysts to consider the operations as a whole and how they related to each other on these key three levels, while the following descriptions are important concepts in information security. These concepts are still important in the present day.

- Security organisation: information security infrastructure, security of third party access, outsourcing.
- Asset classification and control: accountability for assets, information classification.
- Personnel security: security in job definition and resourcing, user training, responding to security incidents and malfunctions.
- Physical and environmental security: secure areas, equipment security, general controls.
- Communications and operations management: operational procedures and responsibilities, system planning and acceptance, protection against malicious software, housekeeping, network management, media handling and security, exchange of information and software.
- Access control: business requirement for access control, user access management, user responsibilities, network access control, operating system access control, application access control, monitoring systems access and use, mobile computing and teleworking.
- Systems development and maintenance: security requirements of systems, security in application systems, cryptographic controls, security of system files, security in development and support processes.
- Business continuity management: aspects of business continuity management.
- Compliance: compliance with legal requirements, reviews of security and technical compliance, system audit and considerations.

The main tasks behind the above-mentioned areas are briefly given in the following subsections with emphasis on activities that may be easily overlooked or underestimated.

2.7 Asset Classification and Control

The responsible entity identifies all assets and allocates further responsibilities to members of the organisation through the definition of clear and documented processes, taking into account authorisation procedures for use of information processing facilities. Inventory access should include:

- information assets, which means databases, other files, system documentation, manuals, training material, operational procedures, continuity plans, archived information
- software assets, which means applications, operating systems, development tools
- physical assets, which means servers, clients, mainframes, terminals, notebooks, modems, routers, faxes, data media, power supplies, air conditioning, furniture and accommodation.

Each asset has to be classified and labeled accordingly. These labels should reflect how critical information is in terms of its confidentiality, integrity and availability; however, overly complex schemes should be avoided. For each classification, handling procedures should be defined (in the case of data this includes copying, storage, transmission in electronic format or by spoken word, and destruction). Of course, all procedures are defined in line with threats analysis, so that the costs incurred do not exceed the value of resource being protected.

2.7.1 Continuity Planning

Business continuity planning (BCP) is a crucial issue and it has to be covered carefully (Devargas, 1999). After a serious disaster many businesses recover with difficulty, e.g. in the case of a major fire in the UK, over 80% of businesses never recover, despite insurance arrangements, which effectively cover 30–50% of losses (Devargas, 1999). Thus, continuity planning should be an integral part of security policy. BCP starts with threats identification, asset valuation and determination of likelihood of incidence.

2.7.2 Auditing

As information security management in e-business systems becomes common practice, standards for auditing are becoming increasingly important. It is vital for management to consult proactively and to advise on IT security. There are two mainstream auditing methodologies for IS. The first is based on BS 7799 standards. Information Systems Audit and Control Foundation (ISACF) has defined a complementary approach and this group of auditing standards is called Control Objectives for Information and Related Technology or COBIT (COBIT SC, 1998). COBIT is more of a general nature. It is oriented towards understanding and managing business risks that are associated with implementation of new technologies. In other words, it bridges gaps between business risks, control needs and technical issues, by providing good practices to structure and manage activities. These activities are related to business objectives and they are structured into four domains: planning/ organisation, acquisition/implementation, delivery/support, and monitoring. Each of these domains consists of processes that have to be performed and there are 34 such processes, e.g. from definition of a strategic IT plan to independent monitoring. Using these processes, two additional views are covered: information criteria (quality, fiduciary, security) and resources (people, applications, technology, facilities, data).

2.8 Legal Issues

Certification service providers should comply with Data Protection Directive (EU, 1995) with regards to processing of personal data and their free movement: these data may be collected only directly from the subject or after explicit consent of the subject, and may not be used for any other purpose.

Many countries have already defined their national legislations and their implementations are frequently based on the above-mentioned models. A comprehensive reference to relevant legislation can be found in (Baker and McKenzie, 2002). It includes international directives, enacted and pending regulation with summaries and related resources.

2.8.1 Intellectual Property Rights

Intellectual property rights (IPR) cover copyrights, patents, design rights and trademarks (for introduction see (WIPO, 2000)). Copyright infringement can result in serious consequences, even criminal prosecution. Traditional legal systems for intellectual property protection are based on sovereignty and territoriality. The global network challenges these issues significantly. From the security point of view and for the majority of businesses, copyright issues apply mainly to software. Thus, organisations should have a published copyright compliance statements, defined procedures for acquisition, installation and use of new software products, registers of copyrighted assets with proof and evidence of ownership and procedures to control compliance with licensing agreements (BSI, 1999). Regarding patents, for the majority of users they may apply only to algorithms, e.g. in the US. From a wider security perspective, design rights and trademarks have to be considered in relation with Web services. Page designers should avoid using elements of proprietary literary and artistic works, while administrators should take care to prevent meta-tags that may violate trademarks. Trademark issues have also to be considered when registering domain names. Finally, an organisation has to consider even such IPR issues like agreements with developers and designers of their website to prevent claims that they own the rights of that work.

2.8.2 Privacy Rights

On the international level, the base for privacy rights is the OECD Privacy Guidelines (OECD, 1998). These recommendations put forward the following principles: transparency regarding the collection of personal data, transparency regarding the use of personal data, and control of personal data and access to it by the individual. Privacy rights have can be addressed from two perspectives: internal and external entities.

With regards to external entities, websites should have a privacy statement, explicitly expressing the organisation's online privacy policy. US Federal Trade Commission recommends four practice principles that should be addressed: notice, choice, access, and security (Dreben and Werbach, 1999). Similarly, the EU Data Protection Directive (EU, 1995), discussed below, requires processing of personal data only upon an individual's specific, informed, and unambiguous consent. With regards to privacy issues for employees, workplace monitoring, retrieving and storing of employees' communications has to be addressed. Organisations must decide what policies they wish to adopt concerning use and disclosure of electronic mail sent and received by their employees (Dichter and Burkhardt, 2001). Web surfing policies should be put in place as well. Although these policies will vary among companies and jurisdictions, the following issues should be considered: employee privacy rights, the disclosure of confidential information, the rights of third parties to obtain access to company records, the company’s need to manage resources, the right of unions to access company employees via email.

2.8.3 Providers Rights and Responsibilities

Additional problems are related to service provisioning (Dreben, 1999). The possibility for clients to post content on an organisation’s website has to be seriously analysed, as the organisation may be responsible for infringements and offensive or harassment messages stored on its site. In general, two main acts, (EU, 2000) in the EU and (US Congress, 1998) in the US, do not state a responsibility of a provider for content; if the provider is not aware of it or if the provider does not remove illegal content after being informed about it.

EU service providers should follow closely the Directive on Privacy and Electronic Communications (EU, 2002), which supplements Data Protection Directive. It covers relations between subscribers and service providers.

Spyware, cookies and similar technologies can be used, but only for legitimate purposes, with the knowledge of users concerned. Therefore, users have to be informed about such use, and have to have a possibility to refuse these techniques. It is generally advised to obtain users consent by any appropriate method, e.g. by ticking a box on a website.

2.9 Inter-organzational Issues

2.9.1 Introduction and Coordination of Security Activities

Successful management of e-business security requires coordination between organisations with reporting of incidents and coordination of counter measures. These activities started at the end of the 1980s with establishment of so called computer emergency response teams. Many national governmental, industrial and educational emergency response teams now exist. In the US the main one is CERT Coordination Center, located at Carnegie Mellon University. These teams provide technical assistance and coordinate responses to security compromises through coordination, technical documents and training courses. They further coordinate their work at the international level within the Forum of Incident Response and Security Teams (FIRST). Following their activities is necessary, especially for on-time upgrades of compromised software components. Contacts should be maintained with response teams, and also with law enforcement authorities, regulatory bodies and service providers to ensure responsiveness in case of a security incident.

2.9.2 General Interdependency

Security policy according to BS 7799 is mainly organisation-centric. However, it is becoming increasingly important to think also in wide inter-organisational terms. There are growing trends to consider global dimensions. According to (Hunker, 2002), there are five critical dimensions, which are mainly yet to be resolved: measuring system risk and resiliency, managing and understanding interdependencies, overcoming barriers to technological change, selecting appropriate forms of infrastructure governance, developing efficient incentive structures, and adopting an integrated systems perspective.

Although Hunker addresses all critical infrastructures and not just the Internet, the paper is relevant since it has a considerable bearing on Internet security. Regarding system risk, there is no definitive and quantifiable risk measurement to underpin risk mitigation strategies. Regarding interdependencies, each organisation is linked to billions of users in the Internet, which is a highly complex, non-linear system, especially as it inherently includes human factors. Modeling this point of view is a very difficult task, and research in this area is very much in its early stages. Hanker also stresses the importance of barriers to technological change, as advances in technology can often prevent threats, but the inertia of existing systems is mainly based on required investment and it is an open question how and whom to force to perform such transitions, and who should pay for them. The basis is certainly some kind of societal consensus in laws and public policy. This is linked to the problem of governance of the Internet infrastructure, which is currently governed loosely only by the IETF, which decides about acceptable technological solutions in an open manner. To establish efficient incentive structures, the following is suggested: market forces, regulations, liability and contracts, voluntary standards, best practices, insurance, public disclosure, reputation and procurement.

2.9.3 Trust Issues

Rapidly growing trends in collaborative and cooperative business relationships expose trust. Fundamental questions are (DeMaio, 2002): can I trust entities and infrastructures on which I depend? Can involved organisations trust me? Together, can we trust our common infrastructure and processes? In order to achieve trust, an e-Trust initiative has been started, where each participant willingly continuously demonstrates that he/she is acting openly, honestly, following the rules and being controlled appropriately (DeMaio, 2002). This demonstration comes in various forms and it is managed by Information Systems Security Certification Consortium, which is a non-profit consortium for training and certification of information security professionals.

2.10 Financial Institutions and Information Systems Security

2.10.1 Introduction

Reviewing the literature concerned with evaluating the security of computerised information systems reveals the paucity of available studies in that particular area of research. One reason is that the security of IS is a relatively new research area. The main objectives of previous studies under this category have been to list the security threats that might threaten computerised information systems in an financial institution; to explore the significance of such perceived security threats in the real world; and to investigate their occurrence and potential losses in different financial institutions.

2.10.2 Financial Security Threats

One of the most important studies in this area was carried out by Loch *et al.* (1992), while Althaneer and Nelson (2009) show that not many policy improvements have occurred in Saudi Arabia or in the Middle East since this time. The researchers conducted a survey to explore the perception of Management Information Systems Executives regarding the security threats in microcomputer, mainframe computer, and network environments. The researchers developed a list of twelve security threats and empirically examined them. The results indicated that natural disasters; employee accidental actions (entry of bad data and destruction of data); inadequate control over media; and unauthorised access to IS by hackers had been ranked among the top security threats. These results confirmed the experts' claims that the greatest threats come from inside financial institutions.

Moreover, since accounting information system security has become one of the major concerns for information system auditor, Davis (1996) tried to discover the current status of the security issue in practice. Davis conducted a survey using the questionnaire, "*Threats to Accounting Information Systems Security Survey*" which was adapted from Loch *et al*. (1992), in replication of their work. The results of Davis' survey (1996) indicated that information systems auditors recognised that different computing environments have different relative levels of security risks. This has been confirmed in more recent studies as shown in the Saudi section, with 2009 and 2010 studies showing that have experienced similar problems while their technological and organisational development have been lagging (Althaneer and Nelson, 2009).

The results of Davis' (1996) study also reported that employees' accidental entry of "bad" data and the accidental destruction of data, as well as the introduction of computer viruses, were considered to be the three top threats in a microcomputer environment. However, unauthorised access to data and/or system by employees, accidental entry of "bad" data by employees and poor segregation of information system duties were rated as the major threats to the minicomputer environment. Concerning the mainframe computer environment, accidental entry of "bad" data by employees, natural disaster, and unauthorised access to data and/or system by employees were perceived as the main threats, while unauthorised access to data and/or system by both outsider (hackers) and insiders (employees), and technology advances faster than control practice were said to be the most important threats in network computer environment.

2.10.3 Financial Security Developments

Ryan and Bordoloi (1997) explored how companies moving from a mainframe to a client/server environment evaluated and took security measures to protect against potential security threats. The results of Ryan and Bordoloi's (1997) study revealed that the most significant security threats were: accidental destruction of data by employees; accidental entry of erroneous data by employees; intentional destruction of data by employees; intentional entry of erroneous data by employees; loss due to inadequate backups or log files; natural disaster: fire, flood, loss of power, etc; and single point of failure.

Henry (1997) conducted a survey to determine the nature of the accounting systems and security in use. The results of Henry's survey indicated that 80.3 percent of the companies backed-up their accounting systems. 74.4 percent of the companies secured their accounting system with passwords, but only 42.7 percent utilised protection from viruses. Physical security and authorisation for changes to the system were employed by less than 40 percent of the respondents. The survey results also showed that only 15 companies used encryption for their accounting data, which was a surprising result, considering the number of companies utilising some form of communication hardware. Almost 45 percent of the sample underwent some sort of audit of IS data.

In 1998, Hood and Yang studied the impact of banking information systems security on banking in China in comparison to the UK. The survey results revealed that all respondents believe that management was aware of security but none believed that their banks had taken enough action to reduce the risks and losses. The most common reason for this was the lack of financial and human resources. Furthermore, all four banks surveyed claimed to have a security policy, but only one was formally stated. Human security threats were perceived as the most important security threats in the Chinese banking sector, especially in the form of malicious attack from outsiders.

Siponen (2000) introduced a conceptual foundation for financial institutional information security awareness program to minimise the end-user errors and to enhance the effectiveness of implemented security controls. Siponen (2000) argued that information security techniques or procedures would lose their real usefulness if they were misused; misinterpreted; not used or not properly implemented by end-users.

In related work, Hermanson et al. (2000) carried out an exploratory survey using a questionnaire to understand how financial institutions are addressing their IT risks and to examine evaluations of IT risks performed by internal auditors in their financial institutions. The results of the study revealed that internal auditors focus primarily on traditional IT risks and controls, such as IT asset safeguarding, application processing, and data integrity, privacy, and security.

Subsequently, Abu-Musa (2001) carried out a survey to investigate security threats of IS in the Egyptian banking sector (EBS). The entire population (66 banks) of the EBS was surveyed using a self-administered questionnaire which included nineteen IS security threats. The statistical results of the study revealed that accidental entry of bad data by employees, accidental destruction of data by employees; introduction of computer viruses to the system, natural and human-made disasters, employees' sharing of passwords and misdirecting prints and distributing information to people not entitled to receive them are the most perceived significant security threats to IS in the EBS. The IS security threats list suggested by Abu-Musa (2001) and Althaneer and Nelson (2009) will be adopted and used in the current study to investigate the significant perceived security threats challenging IS is Saudi environment.

In other research, Coffin and Patilis (2001) studied the role of internal auditors in evaluating the security controls of protecting sensitive data in IS in financial institutions such as banks, securities firms, and insurance. The researchers argued that internal auditing could significantly help financial institutions in determining and evaluating the implemented security controls surrounding the collection, use and access to customer information as well as compliance with applicable regulations. White and Pearson (2001) surveyed over two hundred USA companies to investigate the security controls of personal use of computers, controlling e-mail accounts, and securing company data. The results of the study reinforced the need for better security control in the majority of surveyed companies. The results also revealed that many corporations began to use computer technology before implementing appropriate safeguards; and the majority of the company's safeguards continue to be lacking.

Warren (2002) carried out a survey to investigate the security practices of computerised information systems in three countries: Australia; UK and USA. The paper attempted to evaluate security practices from different perspectives and to investigate whether the security practices are varied from one country to another. The results of survey revealed that:

- In Australia, poor levels of computer security were found among Australian financial institutions. Many of the security problems were identified due to poor security procedures being implemented. The results also indicated that 45 percent of financial institutions did not budget for computer security.
- In the UK, 42 percent of financial institutions did not have an information security policy.The findings also revealed that 49 per cent of financial institutions listed budget constraints as being an issue in implementing computer security.

In the USA, meanwhile theft of information and financial fraud caused the most financial damage. However, differences in the levels of IS abuses carried out by internal and external individuals were not significant. The paper suggested that USA security practices seem to be more effective than those of Australia or the UK.

2.10.4 Financial Developments and Risks

Wright and Wright (2002) conducted an exploratory study to obtain an understanding of unique risks associated with the implementation and operation of Enterprise Resource Planning (ERP) systems using a semi-structured interview approach. The results suggested that major firms use process audit techniques, as opposed to validation testing (i.e., they do not rely on tests of output) when hired to provide assurance on the risks for an ERP system.

As mentioned many times, Saudi Arabia is behind in their IS and security developments, making older literature more relevant to the nation than it is to nations with more development in this area. The National Institute of Standards and Technology (2003) in USA issued its initial publication draft titled "*Standards for Security Categorisation of Federal Information and Information Systems*". This publication establishes three potential levels of risk (low, moderate, and high) for each of the stated security objectives (confidentiality, integrity, and availability) relevant to securing computerised information systems. The proposed levels of risk are more heavily weighted toward the impact of risk on the security of IS and the potential magnitude of harm that the loss of confidentiality, integrity, or availability would have on agency operations (including mission, functions, image or reputation), agency assets, or individuals (data privacy).

The United States General Accounting Office (GAO) (2003) performed a review at the Financial Management Service (FMS) during the period from October 2002 to June 2003 to investigate whether FMS: (1) conducted a comprehensive security risk assessment and (2) documented and implemented appropriate security measures and controls for the system's protection. The results of GAO' review (2003) revealed that although FMS and the Federal Reserve had implemented numerous of security controls to protect their computing resources, risks were not sufficiently assessed, and numerous security control weaknesses were identified. Accordingly, immediate actions to correct the weaknesses to promptly address new security threats and risks as they emerge to IS were highly recommended.

More recently, Hunton *et al*. (2005) carried out an experiment study to understand, assess and examine the extent to which financial auditors and information systems (IS) audit specialists recognise differences in the nature and unique business and audit risks associated with enterprise resource planning (ERP) systems, as compared to traditional computerised (non-ERP) systems. The research findings revealed that financial auditors were significantly less concerned than IS audit specialists with the following heightened risks of the ERP environment in the experimental case: business interruption, network security, database security, application security, process interdependency, and overall control risk. Moreover, financial auditors did not recognise the heightened risks of a seeded control weakness as well as reluctance to seek consultation of IS audit specialists. However, IS audit specialists were less confident in financial auditors' abilities to recognise unique risks posed by ERP systems. The findings suggest a lack of understanding and consideration of unique ERP risks by financial auditors, which could have deleterious effects on audit quality.

2.11 Worldwide Context

2.11.1 Demand for Strategies in Information Systems Security

Strategies to improve information systems (IS) security may involve many individual or combined factors ranging from improved software and applications, improved hardware, improved usage of existing technology, awareness of threats and strategic design, or even improved organisational cultures and training which facilitate enhanced security. According to Zurich (2008), information security has a major role in enterprise since it relies on information flow, and guaranteeing confidences in the integrity and accuracy of the information is just are significant as restricting (unapproved) access to information. Most security breaches are asserted to be due to "*internal employees, industrial espionage by competitors, hackers, organised crime, and even foreign governments. Information security does not just mean controlling computer access, but also physical access to secured areas such as data centres"* (p. 1). Professional data management is deeply integrated with IS security, while the goal of professional data management is to decide how to share and secure electronic information. Naturally, both electronic and paper base records must be properly secured from potential external and internal threats alike, creating the need for two fundamentally different systems. While IS security may use the same principles as documentation security, IS security development must be continually mindful of changing variables. These variables include internal processes, technology, and the evolution of external threats. External threats may change with technology as it is available to the public, while evolving trends in both tools used in security threats and trends in attacks may play a role in the need for security evolution. According to Zurich, IT is a double edged sword since most of the modern companies are reliant on it; this means it cannot be avoided, demanding continuous attention, improvements, training, etc. to remain competitive and capable of meeting all of the customers' demands; the author also stated that "*there are many ways to go about developing these plans...An effective information security plan considers people, policy, and the technology in developing and implementing the plan. The plan itself needs to be realistic and flexible to accommodate the needs of various business units*" (2008, p. 5).

There are four primary steps to reaching security goals in IS, including the investigation of the security in place within the IS infrastructure, the analysis of technical practices in place (including encryptions, policies, organisational culture, and other practices and aspects), comparisons between security requirements and business security needs, and insisting awareness or actions improve for all data security and data sharing processes. Analysing the security of IS infrastructure may include the evaluation of security domains, the assessment or testing of firewall types (including applications and circuit gateways), assessing or designing firewall filters (including transport or tunnel mode), and assessing or designing intrusion detection systems (including applications or networks). Once these assessments have been made, or some changes have been made where known to be necessary, policies may be considered in further detail so that specialists can deduce the next or final courses of action prior to safely resuming standard operations (Stamps, 2006; Wells, 2007).

Furthermore, analysing IS security policies may involve the consideration of which individuals or groups are allowed to access variety categories of information, and this often involves security levels or specific classifications for information. With this, policies may have express consideration for reading data, writing data, appending data, and deleting data. Security requirements for employees, business, and all external factors must take proper care in planning and execution, a proper mix of technology, and strategic design for infrastructure. The roles of individuals can be optimised according to theoretical concepts in security and the objectives of the company (the following section considers additional strategic development concepts as they have been applied in recent years), while Grance, Hash, and Stevens (2004) wrote that many people can have a role in IS, but the names with vary across organisations, depending on their unique demands. Beyond this the authors stated that not all participants will have a role in all activities, and that "*the determination of which participants need to be consulted in each phase is as unique to the organisation as the development. With any development, it is important to involve the information security program manager and information system security officer*

(ISSO) as early as possible; preferably in the initiation phase" (p. 3). (The initiation phase is described in detail in the following section, and in terms of optimising strategy and expert recommendations).

Moreover, awareness in data security and sharing demands strategic management conducted so that both people and policies are properly focused on demands and aspects at hand. This may include security attacks, threats, development, or any general or specific category. According to White (2009), organisations generally lack the levels of awareness required to maintain security protocol aligned with threats (and therefore best practices in security). Any acceptable use policy (AUP) should be updated amid the developments of security and awareness policies, while all actions should be conducted thoroughly both routinely (for awareness purposes) and as needed due to threats, technology, or policy. Awareness has a major impact on developing policy in terms of hardware, software, employees, and other major aspects of a functioning organisation, while the direct and indirect impact of changes may make critical differences for attacks or threats. Legislation often plays a role in both the potential for security improvements or security attacks, and it may also require that an organisation immediately adjust security protocol or IS infrastructure.

Naturally, changes in IS infrastructure, whether they be the result of changing operating systems, changing applications, different hardware, or different policies, create a demand for different security (Stamps, 2006). The Data Protection Act of 1998 was one of the most major and influential catalysts of changes for both IS and security in the information technology age; it is therefore an example of how changes may impact this area in response to legislation in the future. The Data Protection Act includes eight principles for information handling that have become the foundation for modern best practices in IS and IS security. These principles are concerned with fair and lawful processing, processing for limited purposes, adequate (and relevant) without being excessive, accuracy, not keeping for longer than necessary, processing in line with rights, international transfers, and other areas. More specifically, these principles state that personal data should be fairly and lawfully processed, shall not be processed in any manner incompatible with lawful purposes, shall be adequate and relevant, shall be accurate and up to date, shall not be kept longer than demanded by all defined purposes, shall be processed in accordance with the rights of data subjects, that data shall be subject to appropriate technical and organisational measures and that personal data shall not be transferred outside the nation unless that country assures appropriate protection (in according with rights and freedom of information topics relevant to the data) (The National Archives, 2010).

The demand for IS security has been evident in numerous examples in addition to the major attack described above, while threats and attacks exist across the spectrum of topics described above in addition to other potential areas. The following section discusses major aspects of IS security as they have been considered in recent literature, with emphasis on the evolution of security and implications for the future.

2.12 Recent Developments in IS Security Strategy

The National Institute of Standards and Technology (NIST) in the United States recently published a comprehensive series of recommendations for IS security, with an emphasis on incorporating security across all phases of an information system development life cycle (SDLC) (Grance, Hash, and Stevens, 2004). Such recommendations form the basis of strategic development and best practices for any organisation wishing to improve security while implementing cost effective solutions for security control. Both the adoption of SDLC and the consideration of implementation techniques regarding IS security requirements across the phases in SDLC serve to improve IS security strategic development. The five primary stages in SDLC include initiation, acquisition and development, implementation, operations and maintenance, and disposition. According to Grance, Hash, and Stevens (2004), "*An organisation will either use the general SDLC described in this document or will have developed a tailored SDLC that meets their specific needs. In either case, NIST recommends that organisations incorporate the associated IT security steps of this general SDLC into their development process*" (p. iv).

As mentioned, the various stages of the SDLC contain additional elements important for optimising strategy and security. In the initiation phase, the most important aspects are security categorisation and preliminary risk assessment. Meanwhile, in the acquisition and development phase, the most important elements are risk assessment, security functional requirements analysis, security assurance requirements analysis, cost considerations and reporting, security planning, security control development, developmental security test and evaluation, and other planning components. Next in the implementation phase, organisations should consider strategic processes in terms of inspection and acceptance, system integration, security certification, and security accreditation. In the operations and maintenance phase, information security specialists should be mindful of configuration management and control as well as constant monitoring. Lastly, in the disposition phase, users should consider information preservation, media sanitisation, and hardware and software disposal (Grance, Hash, and Stevens, 2004).

In addition, Wells (2007) considered the IS security strategies in terms of technology and theoretical defence. In attempting to discern the ideal solution to IS infrastructure security, Wells (2007) recommends a combination of extending infrastructure security, defining security solutions in terms of organisational objectives, and defining processes for optimising security within the specific characteristics of an organisation. In the past decade, IS security across numerous organisations was faced with issues regarding internet firewalls, as the once predominantly reliable solutions slowly because insufficient against security attacks and threats.

Incomplete security solutions are as much of a problem as ineffective security solutions, while security threats and attacks commonly find a loophole in systems comparably as often as they find a way though an existing security measure (Bellamy, Perri, and Raab, 2005; Stamp, 2006; Straub, D., Goodman, S., and Baskerville, 2008). The optimisation of IS security involves balancing both protection as risk as to counter both the defence against attacks as well as vulnerability to general threats. In the case of the firewall defence instrument, the nature of the incomplete solution can be described in terms of abilities and restrictions; firewalls are generally the use of software in terms of hardware characteristics, and thus have a hard-coded functionality set (Wells, 2007). This is thus an example (similar to many other instruments), of an instrument designed for a specific type of processing that neglects consideration of specific threats, and is therefore an incomplete solution. Firewalls are designed for high throughput and provide only a limited profile for precise attacks to security; firewalls limit the potential access from external sources in terms of attempted connections or services, however, they are nonetheless an example of an incomplete solution.

As mentioned, incompleteness is a common problem in an increasing amount of instrumentation, and thus should be considered as a conceptual necessity in improving IS security in general. Virtual private networks (VPNs), security sockets layers (SSLs), and demilitarised zones (DMZ) have also been found incomplete. While VPNs allow remote users (or networks) to enter an internal network via encrypted tunnels, they both facilitate privacy for the data as it travels through unsecured internet space as well as the reduction of the internal network’s security because they allow potentially infected systems to have indiscriminate access (Wells, 2007;

Stamp, 2006). Meanwhile, SSL encrypts HTTP data in another manner which adds a certain level of privacy rather than security, although the encrypted data may pass through any network space or application while avoiding inspection (and detection) of malware. Lastly, DMZs are networks within the gateway while outside the network, and are incomplete solutions because they isolate systems to an extent but servers' dual porting provides access to resources within the internal network in a manner which may jeopardise the solution of the entire DMZ (Wells, 2007). Clearly, incomplete solutions are common, and this conceptual approach to developing strategy may give rise to a methodological and systematic optimisation of instrumentation, networks, infrastructure, processes, and overall operation.

More recently, other analysts have provided information that is useful for consideration in this work, showing how best practices continue to evolve in both procedure and technology, having implications for organizations or entire regions adopting a "good enough" approach (or waiting until there is a problem before seeking a solution to their security vulnerabilities). Teller Vision (2013) provided a list of recommendations for modern organizations, although it may be unrealistic for institutions in developing countries to become this modern in a sole transitional phase. According to Teller Vision (2013), organizations are advised to consider that spending on new technology alone is not sufficient for protecting information, that data disruption attacks can lead to destructive attacks, that nation states and threat actors are becoming more sophisticated (this is especially relevant to organizations in developing nations who may not realize that they are falling behind), that legislation can change industry standards in ways that may change the nature of threats, that predictive threat intelligence analytics can create more effective risk management capacity, vendor risk management is becoming more important and relevant for financial services, cyber risk should still be dealt with at the board level (versus other levels), firms should to adjust to the ‘boundless network’ concept while ensuring appropriate investments are made in training, both identity and access management are becoming critical security controls, and that the financial services industry is becoming increasingly reliant on cyber benchmarking. It seems that this is well beyond the efforts made in Saudi Arabian analyses, or is recorded in literature, but the research attempts to determine the extent of developments in actual institutions.

In other literature, Sandilya (2012) examined the execution of IT projects in banks, while the research had implications for ongoing coordination challenges and the need for continuous system updating amid the many changing variables in such organizations. French (2012) examining security in e-banking specifically, on the rise with considerable vulnerability concerns in developing nations, and reported that the improvements in safeguards against security threats has been been paralleled by usability issues and decreased security practices from the institution’s customers. Daud, Mamud, and Aziz (2011) studied consumer perception of information security in e-banking, surveying 330 customers, finding that confidentiality and privacy are most likely to have an impact on consumer perception of security.

Kumar, Agrawal, and Chauhan (2013) discussed modern technological changes and demands, stating that “the widespread use of electronic documents makes the security of top secret documents critical for banking. Confidential financial and customer data require stringent user and security protocols. When unauthorized persons gain access to sensitive data, it can dilute the brand, result in loss of business and erode the confidence of customers. Banks can uphold security by adopting a robust policy to prevent breach of security and unauthorized access” (p. 16). This last statement is in line with the assertions from earlier literature, but the variables and associated demands involve change, while some organizations may not be able to keep up with the pace of these changes. Kumar, Agawal, and Chauhan (2013) also reported on a new technology that is expected to be implemented for security increases in developing nations and organizations that can afford it, explaining that biometric sensors will be able to better authenticate users when the technology is more cost-effective for these kinds of uses. Similarly, Rao et al. (2012) discussed newer technology and applicability in the banking sector, reporting that cryptography has improved, and quantum cryptography can be used to offer more secure communiations. The research team also stated that "Cryptography provides following merits establishment of a secure connection which can prevent attacks such as eavesdropping, man-in-the-middle and replay. Applications of cryptography include computer passwords, bank account passwords, ATM machines, etc. However there are many other classical cryptography ways for securing ones particular data but they are currently unsafe and they cannot detect the existence of passive attacks such as eavesdropping, man-in-the-middle and replay" (p. 1540). With this, they recommended that conventional cryptography be combined with quantum cryptography for maximum benefits.

2.13 Summary

Security threats and attacks commonly find a loophole in systems comparably as often as they find a way through an existing security measure. Threats and attacks can forcibly penetrate systems while loopholes have been found in firewalls, DMZ, VPNs, and SSL in recent years. Incomplete solutions are common; while a conceptual approach to developing strategy can give rise to a methodological albeit precise improvement of IS security instrumentation, networks, infrastructure, processes, and overall organisational operation. Information security is presently at the crossroads of four diverging poles of interest, while management teams must make informed decisions as IT staff serve the system, auditors control the system, and users use the system. Meanwhile, security professionals must be mindful of the incompleteness of even modern tools, while research and implementation efforts should be conducted periodically as well as when needed to ensure that vulnerabilities due to incompleteness do not give rise to breaches. Numerous methods of attack have plagued information security specialists in recent years, while the threat evolves alongside the changing uses of developing technology. As mentioned, Saudi Arabia’s vulnerability is potentially even greater than that of the average nation’s risk.

The research inquiries reveal additional significance in the study. This effort is to consider ten items total across the primary inquiry of present conditions in Saudi IS. As mentioned, these areas include the primary threats affecting IS in financial institutions, whether the threats are unique to the sector, the current policies and procedures for these areas, employees and ability to follow relevant policy, factors affecting willingness, the role of personal ethics and the aforementioned compliance, the impact of institutional factors of compliance, the presence and nature of factors restricting compliance, the role of organisational traits in overall IS effectiveness, and the potential for generally improving IS. In addition to the previously described significance of either supporting literature (and thus further expanding the existing academic knowledge base) or closing research gaps while revealing the reality of these processes in terms of unique modern conditions, this study has additional significance resulting from the nature of the inquiries. As all of this literature has shown, in addition to Saudi Arabia having a gap in literature focusing on the specific conditions and obstacles facing the individual country, the nation is ‘behind’ in development, and the study attempts to fill this gap with a study targeting these areas while providing an original data set.

Chapter 3: Methodology

3.1 Introduction

This chapter discusses the details of the research and analysis methodology, and through this, the framework for addressing the research inquiries is considered. The research direction is outlined in fine detail, the significance of the research is prioritised while emphasising the relationships to context (and the importance of the organisational and environmental) characteristics, and data sources are demonstrated. Moreover, the primary and secondary sources are described in terms of their many components; two main instruments are used for the primary data source, while the secondary research supplementing this effort will compliment both the literature and the results. Concurrently, the secondary research will be somewhat reliant on the results of the data analysis, as the researcher will seek to best support and discuss the findings alongside recent statistics and literature by tailoring such research to the implications and nature of the findings from the primary research.

The first major communicative action to be undertaken in this research effort is the pilot study. Once this has been strategically designed, administered to the target audience, and carried out, the researcher will analyse the results for practicality. Next, interviews and a (potentially modified) questionnaire will be administered to employees and managers playing some IS roles within Saudi financial institutions. As mentioned, although generalised supplementary research will be carried out during primary research administration, gathering, and analysis, additional research will be conducted following the analysis (to best address the specific issues raised relevant to the results). Thus, both primary and secondary data sources and research will play substantial roles in formulating conclusions, recommendations, and topics for continued research.

This chapter describes the rationale behind the specific strategic organisation employed in this research effort. The areas of methodology considered (in terms of the pilot study, primary data sources, and secondary data sources) include sampling techniques, the sample size of the pilot study and of the primary data, the design and implementation of questionnaires (including organisational theory and distribution techniques), the design and implementation of interviews, and the resources to be used and considered for the supplementary secondary data sources. Following the description of these areas, which will constitute the bulk of the chapter; additional sections will describe the post-compilation stage of data analysis, research ethics, and validity and reliability. These sections will further relate theory to strategic design, while also revealing the potential and limitations of the analysis and results. The data analysis section will contain a description of techniques to be employed in generating useful quantitative figures, explain the nature of qualitative elements in analysis, and describe the development of displaying data while blending observation (including relationships, correlations, and particularly significant or implicative findings) and discussion. The validity and reliability section will explain any potential limitations, biases, or other similarly influence factors, while the research ethics section will explain important issues such as confidentiality, the awareness and freedom of respondents, and academic policies.

3.2 Significance of Research

From the literature published across the past recent decades, it can be shown that many studies conducted have not commonly made a clear distinction between security threats and the inadequacy of security controls (Loch *et al.*, 1992; Davis, 1997; Henry, 1997; Ryan and Bordoloi, 1997). These earlier studies treated ineffective security (including inadequate controls) as security threats. As an example, the lack of inadequacy of some security controls, such as inadequate control over media, poor control over manual handling on input and output, poor segregation of information systems and duties, poor segregation of accounting duties, inadequate control over storage media, inadequate audit trial, the inadequacy of log-on procedures, loss of data through insufficient backup procedures or logging files, uncontrolled read and update access, uncontrolled user privileges, and weak physical controls were all regarded as security threats; naturally this is incorrect application as insufficient measures only constitute a threat potential from internal action, not the presence of the external threat as it exists. Although the potential of existing threats can be amplified in this regard, the threat is not defined by the inadequacies of the aforementioned measures. The justification for treating these areas as threats was based on specific definitions, while considering the ongoing existence of the financial institution. The researchers included these elements in their survey while reporting them as substantially relevant to technology and information security best practices (Ryan and Bordoloi, 1997). More recent analyses have considered these same conceptual areas with regards to newer technology, however there has been little research targeted at closing the conceptual gap; a study of closing this gap in Saudi Arabia is therefore significant.

Nearly all of the previous studies in the IS security threats research area have been implemented in developed countries; and according to the author's knowledge, no empirical research has examined comprehensive IS security threats in Saudi Arabia. It is believed that conducting the current study in a developing country, Saudi Arabia, could thus yield significant results and bridge the gap in this research area. In the current study, security threats and controls have been carefully distinguished. A selected number of precise (conceptual) security threats to IS are derived from previous studies (Loch *et al.*, 1992; Davis, 1996 and 1997; FFIEC, 1996; and Henry, 1997). In addition, the following IS security threats are included in the proposed security list to be empirically examined for the first time is Saudi Arabia: human-made disasters such as fire, loss of power, suppression or destruction of output, creation of fictitious and incorrect output, theft of data and information, unauthorised copying of output, unauthorised visibility of documents, unauthorised printing and distribution of information, directing prints and distributing information to people who are not entitled to receive it, and handling sensitive documents to non-security cleared personnel for shredding. These security threats are mainly related to the IS output security, and there is little information regarding the application of these areas to the most recent conditions present in Saudi Arabia, adding significance to the research. It is believed that conducting the current study in a developing country, Saudi Arabia, could thus yield significant results and bridge the gap in this research area.

Accordingly, the aim of the research described in this thesis is to investigate the significant perceived security threats of information systems in Saudi organisations. The aim of the research is to assess the current dealings and perspectives related to information security, while the research objectives are to: i) present modern perspectives related to information security and complications, ii) assess demands for changes in Saudi Arabia, iii) assess the gaps between organisational actions and best practices, and iv) present recommendations for research and developments.

The significance of this study is evident in the aims and objectives as well as research inquiries and direction. Identifying the specific threats to data security in Saudi financial institutions, as well as considering how existing threats are unique to the banking industry, contributes to the existing knowledge base to close any remaining gaps in literature; the study further aims to identify areas where continued research would be most beneficial, while this is also significant. The personal ethics of employees, in terms of relating to abiding by policies and honesty, will further provide a unique perspective for the conditions and environment present in the analysis. The current modes of presentation, significance of organisational traits, and role of IS within the institution will all further provide significant information which either supports existing studies in modern conditions or reveals unique information allowing readers to consider the effects of variables or conditions present in the study.

3.3 Phases of Research

The following section describes all areas relevant to the primary research and data of this study. The initial pilot study is described, the theory and development behind the questionnaires and interviews. Sampling techniques, sample sizes, distribution methods, and other areas are also described. The analysis of Saudi financial institutions has been designed for qualitative and quantitative results to facilitate detailed conclusions and recommendations, while the study also has been designed to ensure statistical significance in all areas.

3.3.1 Phase 1: Selection of Research Direction and Rationale for the Research Design

The first phase in any research methodology is to select a research direction, rationalizing it through existing literature and according to professional best practices. It is the duty of the diligent researcher and analyst to be continually aware of new theoretical developments, conceptual applications, technology, and other new and improved areas as they arrive. Meanwhile, the rapid change of information technology in conjunction with the broader application of user-friendly applications, the increasing demand for enhanced organisation, and the capacity for financial and accounting tasks to be conducted have simultaneous addressed growing needs while creating greater potential risks. Technological improvements can therefore affect information security in multiple ways, through facilitating greater detail and an increased capacity to process information, and through the increased quantity of information and accounting potentially vulnerable to internal and external threats. Technological enhancements are capable of improving security to a level matching the demands in IS, however, technology commonly develops more quickly in control practices while not being matched with employee awareness, education, skill development, or more general training (Abu-Musa, 2001; Abu-Musa, 2003). Developing compliance to address technological enhancements and associated protocol is also another common issue. As modern accounting and financial publications commonly report issues in IS including data errors, inadequate processing, control violation, and malicious crimes, even the most developed nations must place a great effort into staying at the forefront of information security (Alfawaz, Nelson, and Mohannak, 2010).

The pressing issues in IS are especially relevant to Saudi Arabia, and while the nation is able to keep a decent technological pace, efforts remain generalised and negligent of potential threats; demands and consequences typically must be observable prior to actions being physically carried out and resources actively distributed (Althaneer and Nelson, 2009). This increases the vulnerability of IS in financial institutions, as the mere possibility of threats in accordance with the most recent publications may be neglected entirely, and the organisations may not take action until the threat is considered either “common knowledge” or is observable in the news. Additionally, the described gap in the literature reveals conceptual areas which are poorly understood and considered within the nation; clearly, the increased efforts which have been recommended over the past decade are warranted, while this research is directed at following the described developments, becoming aware of threats as they exist within the nation, and considering what can be done to address active and potential threats from both internal and external sources (Abu-Musa, 2001; Abu-Musa, 2003; Althaneer and Nelson, 2009; Alfawaz, Nelson, and Mohannak, 2010).

Financial institutions have an especial concern to protect information, as customer and institutional information can be misused in a number of ways. Theft, fraud, identity theft, sabotage, and general invasion of privacy may result; Saudi financial institutions have an especially high priority to protect information, compared to other institutions, and thus the direction of this research will include Saudi financial institutions and their instrumentation and policies for information security (Althaneer and Nelson, 2009). The ability of these institutions to address present and potential threats and demands, find and amend security breaches as they occur, and manage policies and employees while reducing vulnerability will all be considered. The efforts of both managers and employees will be considered alongside the structure of information technology, organisational policies and culture, systems of procedures, and other areas. Information system security may be particularly challenging amid the availability of resources and potentially contradictory requirements (typically concerning the necessity to deal with open systems however mandating high protection in all areas), and thus this area is also of concern to the research.

Managers and employees must realise that the adequate treatment of IS risks and breaches requires a wide spectrum of knowledge, ranging from technology and organisational structure and processes to legislation and policies; this naturally demands that managers and employees be educated, trained, and aware of new issues and the need for additional training. Assessing an organisation can allow its various approaches to be considered and applied to theory, and with this, the organisation's techniques can be examined for weaknesses and strengths. While financial institutions are being examined,the knowledge of evolving financial and accounting trends are further relevant to the development of IS protocol. The approaches of Saudi institutions, in these areas, will be assessed for effectiveness and weaknesses alongside the other areas of assessment. The various theoretical approaches common in IS attempt to address the major issues in different ways: while some are nearly entirely technical (with relatively low emphasis on active security), some are more focused on human factors and managerial systems, and others place the greatest emphasis on policies, legislation, and compliance (Harmon, 2001; Powers, 2001). The research and analysis will consider Saudi financial institutions and their ability to effectively apply their chosen approach (while balancing it with other areas). IS integration within organisation and operational structures will also be considered, while the aim of this area of the research direction is to attempt to describe Saudi employees and organisational profiles, with regards to areas requiring improvement and potential development.

Data protection requires that organisations have some idea of threats while also having a fundamental system for addressing risks and threats in IS. Saudi financial institutions will be assessed in terms of their active, past, and potential systems as their development and capacity are considered alongside the development and capacity of threats and risks. Threats are generally assessed through multiple dimensions, while systems addressing them therefore are required to have multiple dimensions. One approach to this is to dedicate one dimension to communication using IS, while dedicating other dimensions to policies and legislation, organisation, technology, and management (Althaneer and Nelson, 2009; Alfawaz, Nelson, and Mohannak, 2010). While designing and implementing these approaches have already occurred in Saudi institutions, the present concerns are primarily in terms of their effectiveness, flexibility, and ability for employees to be compliant as these systems are maintained by managers. The detailed approaches and methodologies of the Saudi financial institution will be outlined, described in relation to multiple areas, and fully assessed. The direction of this research, beginning with the conveyance of literature and discussion of research methodologies in this chapter, will continue through the background of Saudi institutions and instrumentation, consider processes and outputs, describe business activities and compliance, outline management and leadership activities, and be supplemented with secondary research as described prior to the final analysis, conclusions, and recommendations. Other areas included in this general research direction will be encompassed by systems development, maintenance, threats analysis, security infrastructure, public key infrastructure, costs and outsources, technology, policy and planning, auditing, internal issues, and more. The emphasis of the research direction, in addition to the primary aim towards IS, will be on best practices; in this regard, EU and US regulations will be relevant, often described, and form the basis of analysis relevant to recommendations and improvement.

In addition to the direction through organisation and theory, just as the conditions of the financial institution in regards to IS will be described, the research will consider the variables and reactions unique to the Saudi Arabian environment as it is observed. The Saudi Arabian economy is particularly strong for the geographical area, meaning that IS is not particularly limited by the availability of technology and knowledgeable human resources in comparison to poorer nations. Saudi Arabia has a particularly high level of economic success, and as it comprises 25 percent of the Arab region's GDP, financial institutions are generally quite successful. As mentioned, this simultaneously places a greater strain on information security as organisational activities and relationships increase (Althaneer and Nelson, 2009). Although previous IT plans and aspects of the nation's five year plans have taken action to improve both resources and access to skill development, little attention has been paid to the IS for some of the nation's most powerful resources. The need for assessment and improvement reported by literature remains despite governmental knowledge and effort, while the research will explore the nature of these remaining areas and consider potential governmental actions.

In summary, the research direction explores all known factors and applications, while considering the present and potential developments, and recommend means to take advantage of opportunities while overcoming limitations. The two primary approaches to assessing the entirety of these areas include both primary and secondary research, and as the primary research is comprised of both questionnaires and interviews, the secondary research includes information regarding IS and best practices from other areas while also being tailored to the results of the primary research. The direction of the research, through the primary and secondary research efforts, continues through the primary threats affecting information security in Saudi Arabian financial institutions, the uniqueness of the threats to the sector, the policies and procedures currently in place, the compliance of employees in following security policies and procedures, and the components influencing willingness for compliance. Additionally, the influence of personal ethics on compliance, the influence of institutions on employee willingness and compliance, the potential limiting effects of policies and procedures, the effects of organisational traits on successful execution of information security, and the possible enhancements that can be made to increase the effectiveness of IS functions.

As mentioned, the research is not technical in nature, and is qualitative in nature. Considering the conceptual goals of the research aims, objectives, and questions, qualitative research is deemed most fitting according to best practices (Kothari, 2008). Quantitative research does not have the same inherent risk of bias, but it also would not yield the same theoretical relationships and conceptual results that are targeted through the research; the inherent risk of bias is a concern, but it is examined with caution throughout the duration of the study and considered in the analysis. Meanwhile, the selection process of the 10 research questions relates to the research rationale in that the qualitative approach is most fitting for each of the 10 questions; the 10 questions are qualitative questions that explore theory and concepts relevant to the kinds of organizational development needed to address security vulnerabilities. A case study could have been considered for this study, but the people examined from different organizations effectively constitute a case. The sampling methods (see section 3.5.4 for details) were also selected considering the qualitative nature of the study and objectives. Meanwhile, 10 organizations were selected because this number seems to be the highest that could be reached considering the limitations of an academic study conducted by a sole researcher without funding (see section 3.10 for details on limitations). See section 3.5.5 for details regarding the target audience for the instrumentation.

3.3.2 Phase 2: Creation of Research Questions and Hypotheses

The second phase in research efforts is the development of research aims, questions, objectives, and accompanying hypotheses (Collis and Hussey, 2009). As mentioned in the introduction and fully justified in the previous chapter, the aim of the research described in this thesis is to record new data about information system threats and security. More specifically, the aim of the research described in this thesis is to investigate the significant perceived security threats of information systems in Saudi organisations; the aim is to assess the current dealings and perspectives related to information security. This aim has spawned the following objectives (list them), the investigation of which will be accomplished through ten specific inquiries amid the broader category of IS effectiveness in Saudi financial institutions. As mentioned, these were selected to address the qualitative research design, as described in the previous section. The specific research inquiries are:

i) what are the primary threats affecting information security in financial institutions within Saudi Arabia?

ii) how are these threats unique to this sector?

iii) what policies and procedures are currently in place?

iv) how well do employees follow information security policies and procedures?

v) what factors affect the willingness of employees to comply with policies and procedures?

vi) how do personal ethics affect compliance with policies and procedure?

vii) how do various institutional factors impact employees' willingness to comply with policies and procedures?

viii) are there aspects of the current information security policies of procedures that make it difficult for employees to comply?

ix) how do overall organisational characteristics affect the successful execution of information security success?

x) what improvements can be made to increase effectiveness of information security operations?

As mentioned, the researcher intends to address these issues though questionnaires, interviews, secondary research (including best practices from more developed nations such as the U.S. and U.K.) and detailed analysis. While the recommendations and proposals for continued research naturally depend on the specific outcomes generated from the study, the researcher holds preliminary hypotheses at the earliest stages of developing the study. These are as follows:

i) The primary threats affecting information security in Saudi Arabian financial institutions are remaining up to date with technology, technological threats from outside amid weaker security (such as Blackberries, hacking, and more), and otherwise not abiding by best practices and maximising organisational procedures and structure. The financial institutions appear likely to have among the highest security of the nation; however it also seems that they will pale in comparison to the security measures of more developed nations. Meanwhile, unfortunately, the threats from within and outside of the nation remain comparably high, and this ratio naturally results in a higher and unsafe risk.

ii) The threats to the financial institution sector are unique because the information stored within these facilities is especially sensitive. As mentioned, financial information poses a greater risk to the institution and individuals, and there is a higher level of incentives and motivation for people to attempt to violate security. A number of crimes can result from violation including identity theft, fraud, theft, embezzlement, and more; while many organisations have funding information stored as information, there are typically not such an abundance of accounts and funds stored. Online banking poses a particularly unique threat as breaching security may result in distributing the funds without the need for additional action. Meanwhile, the gathering of bank card numbers can allow violators to commit fraud, theft, or outright identity theft, while there is less potential for this to occur in other industries.

iii) The policies and procedures currently in place require active and passive security through supervision and software. While this is effective in a basic level of security, it is inferior to policies and procedures in more developed nations while the organisations generally do not use the best resources available to them nor implement many aspects of best practices. Policies and procedures in place also address compliance; however the motivation, room for innovation, and managerial practices are also not in line with best practices. Legislation is somewhat lax compared to more developed nations, and this contributes to the reluctance to continually update technology and internal systems.

iv) Employees do not have any particular issue or problem following security policies and procedures, however there is little to no innovation or development in general employees or managerial employees. This is because of the lack of pressuring demand and lack of incentive in a system which is comfortable with barely adequate systems in the absence of major observable threats or a clear imbalance of technology. Although the policies and procedures in place require improvements to be made according to the findings of authorities, and authorities are mindful of the most pressing issues, employees play little to no role in improvement and development; furthermore, employees may be discouraged or even disallowed from playing any role in such positive development. This may result in the failure to report potentially useful information which has not resulted in a clear violation or continually observable risk. Overall, employees follow the procedures in place, however there is inadequacy observed in this area as policies generally restrict employees from taking a step further and contributing to development.

v) The factors affecting the willingness of employees to comply with policies and procedures are predominantly related to management and the organisation as a whole. Legislation may also be a factor, potentially giving employees little incentive to contribute to any improvement permitted. Meanwhile, however, the company policy for punishments is generally sufficient enough to keep employees from neglecting the required duties altogether; despite this, the policies are generally lax and only ensure that employees follow a protocol which considers the bare minimum of active and passive potential security risks and threats. Factors potentially affecting willingness may also include severity of punishment from within the institution, closeness of supervision, personal ethics, rewarded incentives for flawless or beneficial performance, and government requirements.

vi) Personal ethics may play a major role with policies and procedure. While the majority of compliance is mandated and punishable by legislation, actions which are not directly observable or recorded are most likely to be reliant on personal ethics; here, high ethical values would show an increased tendency to abide by regulations even when not doing so would go unnoticed. Similarly, low ethical values make the employee more prone to taking the quickest or easiest route amid policies and procedures if this could be done without the knowledge of any authority (or element of the system which could similarly document the occurrence for future viewing by authorities). Personal ethics are assumed to be a lesser, albeit clearly present, factor in compliance. This area may be one of the most difficult to measure are non-ethical employees may be prone to hide such behaviour while providing dishonest answers.

vii) Institutional factors have a major impact on employee willingness to comply with policies and procedures. While personal ethics and work ethic, as well as government regulations, may play significant roles in this area, the role of the institution is the greatest. The institution determines which areas are considered, the punishment for neglect, the reward for effort and compliance, and the nature of the operation. The institution ultimately determines the organisational structure and culture, the positions and distribution of employees and information technology, the specific job duties of employees, the nature of compliance itself, the policies for employees and clients, the relationship of the institution with the nation, and many other areas which define the nature of the institution and job alike. Naturally, these affect the nature of the position, and therefore play some role in nature of employee willingness for compliance. Although personal ethics affect this area as described, the institution is responsible for the constructs of the conditions, and thus has a greater influence on both the processes for compliance and the nature of compliance (and therefore willingness). Because of this, the institution is therefore capable of altering specific aspects in attempt to increase the willingness for compliance as needed. While it is unknown whether compliance is a particular issue (or to what extent), the nature of institutional factors and possible recommendations for positive change are unknown; it is assumed that this area is low albeit present, and both supervision levels and incentives for promotion would serve to improve compliance, as described in detail below.

viii) There are many aspects in current policies and procedures which may hamper an employee’s compliance; however these are generally not significant. A lack of training and access to resources is likely the greatest issue, while the organisation of the employees and operation facilitates this to some degree. Thus, to reduce these possibilities, the organisation should take greater action to monitor employee capacity and employee performance, and ensure that employees have both the means and complete ability to be compliant; the presence of complexities and the temptation of available shortcuts contribute to non-compliance to some level in these areas.

ix) Similar to the procedures and policies put in place by the organisation and effects on compliance, overall organisational characteristics play a major role in affecting the ability of employees to successfully execute information security while experiencing success. Aside from personal traits and governmental legislation, the traits of the organisation affect the remainder of processes in information security. The organisation of processes, the incentives and motivation of employees, managerial styles, goals, and allocation of processes and resources all play a major role in achieving and sustaining information security success. Information security success is achieved by properly applying technology and efficient organisation of skilled individuals and resources. Specifically, Saudi financial institution IS success is affected by the organisation’s willingness to divert attention to IS issues, the prioritisation of IS, and the prerequisites for employment. The specific managerial requirements and techniques also have an observable effect.

x) There are numerous potential improvements which could be made to information security operations. These can be made by Saudi financial institution employees, managers, and the government. Technology is the most immediately addressable area, as software and hardware could be replaced with cutting edge products and programs to minimise active risks. Meanwhile, employees could receive additional training on a routine basis regarding addressing attacks and new issues relevant to reducing threats. The organisation's management is assumed to be the only parties within the institution occasionally informing themselves on issues relevant to improvement, while the majority of the institution prefers to wait until there is a substantial difference in technology (or a publicised risk of threat) to take action. The general needs for improvement are in these terms of organisation and action, in addition to the technology.

3.3.3 Phase 3: Selection of Sampling Techniques and Sampling

After the development of the research questions and hypothesis, the next phase is the selection of sampling techniques and the actual sampling (considered part of the same phase but separate from the actual instrumentation distribution and data recording). This qualitative work demands sampling techniques possible to be conducted in a way that optimizes the potential for the research objectives to be met, and can be conducted in an academic nature which can be completed within the limitations to the researcher. The primary methods used are 'convenience sampling' or accessing the most willing people meeting the research criteria, and the inclusion criteria itself. Beyond this, best practices are considered. To best ensure that the respondents participating in the study are proper representatives of the areas assessed in the study, formal sampling techniques play a role in selections and samplings. According to fundamental theory commonly applied to such research efforts in the academic and professional worlds, there are two fundamental varieties of samples, the probability sample and the non-probability sample. In this regards, the probability sample is variant from the non-probability sample while the probability sample is a representative of the specific population to be assessed (while non-probability is thus not related) (DeVaus, 1985). Through this, and the aforementioned requirement of having at least two years of relevant experience, the target participants will be discovered, approached, and assessed. Moreover, the sampling method to be utilised with this questionnaire is more ideal for the probability approach to sampling (as opposed to non-probability). According to theory, the primary advantages of this approach to questionnaire surveys are the approach facilitating precise and coherent data representations in terms of an active body relevant to a specified area (such as IS security amid financial institutions within a nation), and the approach facilitating a clear opportunity for the conditions to be assessed for potential biases (Gratton and Jones, 2004). The organisations are to be first contacted in some manner (via phone, email, or otherwise) to be informally interviewed regarding participation and IS security. If the organisation is found to have an ample number of relevant employees amid the condition of being an institution with a full and complex IS in place, the request for participation will be given. This will continue until the aforementioned target sample is reached, thereby providing the study with an ample quantity of statistics for a significant analysis and conclusions.

As described at least 10 organisations are assessed, being the largest number felt to be still viable for research (being attainable yet significant) and more may be included if participation willingness and time permit. Within each organisation, five employees are selected based on relevance and willingness; this quantity is assumed to be sufficiently representative of internal organisational trends. Naturally, research and analysis theory assumes that the approach to drawing a sample and the size of such samples are highly significant to the accuracy of an analysis (as well as its potential to be generalised); moreover, despite the desirability of a massive scale research effort encompassing more individuals and organisations, the study is also bound in quantity (see limitations section). Therefore, the sample size of the primary data is dependent on willingness and limitations. In addition to the minimum 50 key respondents assessed in the study, others may be selected if the time is permitting and more still may be interviewed. Should this occur, all aforementioned techniques and structure will hold while these individuals will only serve to support the aim of the study and the statistical significance of responses. The probability method chosen for the questionnaire as described above, in combination with the requirements for participants amid a specific subject area, reduces the likelihood of generalisability (and thus increases precision and meaning) in the study (Marshall and Rossman, 2006; DeVaus, 1985).

3.3.4 Phase 4a: Questionnaire Survey Development

Following the third phase of selecting sampling techniques, the fourth phase involved selecting and developing the questionnaire instrumentation to use in the data recording. As described, the questionnaire survey was selected as an effective data collection instrument for this research effort. While common, the questionnaire is not ideal for all types of primary research efforts, however is assumed sufficient for this analysis of IS security and the organisational improvement of financial institutions. This survey is formulated based on the literature of IS and the current conditions and issues in Saudi Arabia, while it is to be tailored to the specific nature of the inquiries outlined in other sections. The questionnaire survey is tested by the pilot study for feasibility and practicality as mentioned, amended based on the findings of the pilot study, and distributed on a full scale to numerous institutions and IS-associated employees across Saudi Arabia. The design of this instrument forms the foundation for the presentation of analysis and results, all averages and statistics compiled and displayed, all qualitative observations revealed and discussed, and all trends so that recommendations for improvement and continued research can be made.

Many researchers have outlined the significance and potential of questionnaire surveys in formal academic and professional field research efforts. The primary objective of the questionnaire is to extract a massive amount of specific information in an efficient manner, and furthermore across a sizeable quantity of respondents. The use of this instrument has also been referred to as a method or technique (i.e. questionnaire method) and strategy is involved in applying formulated and pre-tested questions. While the questionnaire can include a series of yes or no, multiple choice, ratings (i.e. "on a scale of 1-10, how effective would you rate your company's approach to IS security), and short answer questions, the use of this instrument and method is one of the most commonly applied approaches to data collection (Saunders *et al.*, 2007).

This type of surveying is highly efficient in terms of combining data and in reaching a range of people. When considering the nature of financial institutions and IS security, the questionnaire is also capable of addressing fine details and extracting both simple and complex data. The questionnaire can also be designed to track the traits of those being observed so that these factors can be taken into account during the analysis. For example, if a questionnaire has been designed to rate the effectiveness of IS security and compliance amid specific organisational traits, a series of ratings questions can be combined with short answer and yes or no questions; meanwhile, in order for the spectrum of relevant variables to be most effectively considered and properly applied to theory, the questionnaire can begin with requesting that the respondent list their job position, company name, computer operating system, number of managers, or other information deemed relevant to a given area. While interviews can be designed in a similar way, with all desired information conceived written down in preparing for inquiries, this method lacks the efficiency of questionnaires (Saunders *et al*., 2007). Thus, all relevant facts and needs initially conceived may be addressed through this instrumentation as the researcher continues through the process of data collection in attempt to meet the study’s aims and objectives.

In this study, the target audience will have been informed of the nature of the study prior to participating, however the questionnaire will further list the nature of the study, reveal the confidentiality and other relevant areas of the research methodology, and provide clear directions for the survey’s various types of inquiries. This will serve to reduce the level of confusion, while the respondents will also be able to contact the researcher for any questions they may have in completing the survey. Lastly, the researcher will ensure that all respondents will have the proper amount of time to complete the questionnaire with the highest accuracy and to the best of their ability, established through communications regarding timelines and plans for the data collection and research.

Many theories, definitions, and classifications of research methodologies have considered the role of the questionnaire amid primary research while deducing that the optimally effective implementation ensues from a key balance of rigor versus time and restrictions, the appropriateness of assumptions in methodological as opposed to substantive issues, treating the development as an art as well as a science, and emphasising accuracy while eliminating the potential for confusion and error wherever possible (DeVaus, 1985; Presser *et al.*, 2004; Gratton and Jones, 2004; Saunders *et al*., 2007). Moreover, additional conceptual developments have claimed that the diligence in both development and application amid the topic and target audience may be even less influential than the aforementioned areas, depending on the nature of the primary research (and assuming general accuracy); meanwhile, the questionnaire can be formulated according to three basic categories, while it is the researchers responsibility to select the categories having the highest potential for facilitating optimal data collection for their topic and research design. From here, the researcher can apply the theory of this design as a template to begin the development of their instrumentation, while using a combination of theory, logic, and application of circumstances to strategically design a highly effective research tool capable of both effective communication and collecting significant data. Naturally, a hybrid of these categories can be selected as most desirable, while the research then has the ability to manipulate multiple schools of thought together in a custom methodology which best meets the needs of research inquiries for the topic at hand.

The three fundamental varieties of questionnaires, according to Saunders *et al.* (2007), are the open-question, closed-question, and multiple choice varieties of questionnaires. Each of these areas has a unique set of advantages and disadvantages, and naturally these traits may have varying effectiveness according to the topic and design of the research inquiries. The open question surveys are typically most effective in detailed and highly organised research methodologies; with these, the researcher assumes the respondents to supply especially detailed and complex information, while the distribution and administration is therefore particularly slow with this variety. Although the researcher can afford to invest some time in ensuring the answers are detailed in this study, the responses desired are known to be only moderate in detail while open questions may only be applied in a few areas of information system security in financial institutions. Open questions may allow managers to describe problems, solutions, and occurrences as they experience them in the nation, however they are not best for the compilation of responses to directly address the specific research inquiries listed. Meanwhile, closed questions allow the respondent to quickly select specific results, allowing the researcher to implement the relevant topics and issues and covering multiple areas based on known conditions or hypotheses. The selection of predetermined answers can be used to compile statistics, address a hypothesis, or face the respondent with predetermined alternatives to subjects which they are already familiar with (Collis and Hussey, 2003). Moreover, closed questions may be more desirable in the consideration of information system security in specific contexts as the spectrum of possibly influential factors can each be similarly addressed; also, such questions are assumed to be most desirable in the event that the researcher has clear and highly defined theories and hypotheses (and more so in the event that there are multiple clear and highly defined theories and hypotheses as they are present in this study) (Collis and Hussey, 2003). According to Saunders *et al*. (2007), closed questions have become particularly common in the furthering development of theory and the research into areas which have been extensively considered in literature. Lastly, the multiple choice questionnaire design allows for categorical questions to be selected, and are particularly used when the researcher desires collecting data regarding specific contexts, occurrences, behaviour, and traits.

The researcher has weighed the advantages and disadvantages of the various approaches to questionnaires, and has opted for a slight hybrid which predominantly consists of closed questions. Multiple choice questions are included in the survey, to quickly cover areas which can be summed up with such short responses, while the majority of questions are either closed or requesting the respondent to rate an element according to some scale. Open ended questions are included so that the respondent may address some areas of pure opinion or to otherwise inquire into areas where the potential answers are either unknown or not easily described in a range of components. Thus, after full and detailed consideration regarding the order of achieving the highest level of precision amid both the scope and limitations of the research to be carried out, the questionnaire attempts to make most of multiple elements of theory (although making especial use of the advantages of closed questioning). Only one set of questions will be prepared, and this same series of inquiries will be administered to all members of all organisations. While the pilot study may define the final form of this instrumentation, the basis of its development is IS and research theory; and this will be deemed sufficient for all organisations assessed (and all employees within).

The questionnaire is to include 30 items in all, so as to be comprehensive of all areas of IS theory while appropriately addressing all elements of research inquiries, with the first set of questions addressing the first five objectives, and the rest of the objectives addressing different questions for each (as described in the discussion chapter, see Chapter 5 for further details regarding relations to questions and outcomes for the objectives). As mentioned, many responses will be pre-created while requesting that employees rate levels of effectiveness, compliance, or other areas. The presence of elements may be answered in multiple choice or yes or no questions. Meanwhile, inquiries into other described areas may be best addressed by the employee’s description of the area, and responses to be selected may include choices such as “always,” “seldom,” and “never,” or “excellent,” “good,” “average,” or “poor.” As this research is to include interviews in addition to questionnaires, only a small amount of the survey will include open ended questions (regarding the improvement of the IS and roles of security,) while the remainder of open ended issues will be addressed with the interviews.

3.3.5 Phase 4b: Interviews

The interviews were developed following the questionnaires, considering a separate “sub phase” of the same basic phase of instrumentation development. The interviews conducted to complete the primary research are strategically organised to consider theoretical elements of IS security and research. Researchers commonly assert that this technique is used to collect information from specific people through inquiries. These have been found to be particularly effective when applied to feelings of one’s job, beliefs, or feelings, while these can be geared towards the research inquiries and aims as they become a powerful research instrument (Collis and Hussey, 2003; Saunders *et al*., 2007). Interviews in general are valuable in extracting information specific to any area, and as they can be applied to address or even formulate research objectives and questions, theoretical developments have categorised and analysed methodologies for creating and administering interviews. According to Gratton and Jones (2004), the interview may be more highly regarded across specific institutions and research efforts because they better facilitate confidentiality; companies may be more willing to participate in a short interview with the personal effort applied than to fill out a questionnaire simply sent to them.

Similar to the categorisation of questionnaires based on fundamental traits and theory applicable to research, interviews have been categorised by experts to be used as research templates when selected by the researcher. With this, there are three main types of interviews: the structured interview, the non-structured interview, and the semi-structured interview (Gratton and Jones, 2004; Saunders *et al*., 2007). The structured interview has been developed by the researcher prior to the administration, and during the interview this structured interview is followed to the fine detail; the structured interview is neither amended nor supplemented during the interview process. Although structured interviews have the advantage of direction, they have the disadvantage of inflexibility. Non-structured interviews, meanwhile, are entirely flexible while having little direction as the researcher arrives without a formal interview; non-structured interviews allow the researcher to pry into various areas as needed. While both the non-structured interview and structured interview have traits which are commonly undesirable in research settings, many research efforts (including this particular effort) choose to employ the semi-structured interview. This hybrid of the aforementioned types involves a strategically designed interview while permitting the researcher to change direction between individuals interviewed as desired. While this may provoke additional variation in results, it may also provide unique output from elite employees while allowing researchers to pursue unexpected topics of interest if they should arise.

The researcher will be interviewing one or two employees from each organisation regarding IS security, organisational traits, and compliance; while the interviews will be carried out using the strategically formulated template created by the researcher, the researcher will attempt to gain additional information by requesting that the interviewee elaborate on specific information given (or by supplementing with follow-up questions).

3.3.6 Phase 5: Pilot Study

Testing the instrumentation was the next phase in the methodology. Prior to the administration of the questionnaire to the entirety of the audience, a pilot study will be conducted to test the feasibility and practicality of the draft questionnaire. To accomplish this test, the survey questionnaire will be distributed to a small sample size of approximately 10 to 15 individuals across two or three organisations (the attempt will involve five members of each organisation, and address two or three organisations). Once these results have been collected, the researcher will examine the responses for any possible need to make final amendments prior to the full-scale distribution. It is assumed that testing the survey on a small portion of the target audience will reveal if there are any issues which need to be addressed, such as questions which are difficult to answer due to clarity (or otherwise), the inappropriateness of a question, questions which are misunderstood and mistaken, or otherwise. If the pilot study reveals any issues which demand attention, the questionnaire will be adjusted accordingly and redistributed as a full scale initiative. If the pilot study does not reveal such issues, the results will be stored for the final compilation while the remainder of the surveys will be administered to the remainder of the target audience selected. As mentioned, the overall intention of this study is to test the questionnaire; meanwhile, two additional assumptions will be tested, that financial institutions do not routinely update their IS security measures and that information technology (IT) products are substantially outdated.

3.3.7 Phase 6: Primary Data Recording and Instrumentation Distribution

Following the testing of the instrumentation, the next phase is to actually distribute the instrumentation and record the data. While the full-scale distribution of the questionnaire surveys initiates the framework for the final compilation and analysis, the beginning of the pool of information for statistics and qualitative observations will begin following the results (and amendments where needed) of the pilot study. With this, while the search for relevant information is underway, numerous elements must be considered to ensure proper collection and compilation prior to the analysis. According to Gratton and Jones (2004), research is characterised as a systematic investigation tailored to obtain and organise data relevant to some inquiry and theoretical direction. In this case, the systematic design includes the questionnaire survey, the interviews (together as the primary data sources), and the supplementary secondary data sources. A total of 15 financial institutions are to be assessed to ensure that any observed trends are typical across the nation; meanwhile, five employees (potentially more if deemed useful as an additional supplement) from each institution are surveyed and interviewed. These employees include either managers or operators of some aspect of the IS security, and while specific positions are not required for eligibility for participation, at least two years of direct experience with IS security in any position within the organisation will be required. Meanwhile, the researcher must consider the potential drawbacks of interviewing and surveying even knowledgeable and experienced employees, in accordance with the theoretical descriptions and applications of primary research as outlined by Gratton and Jones (2004); the authors emphasise that possible drawbacks to such an approach to an analysis, conclusion, and recommendations include limitations relevant to the data collection processes (which may require communication or even travel efforts on the behalf of the researcher), time restrictions (of particular concern in the time limited academic context), cost and resource requirements, and ensuring participants are true members of the target audience selected (and that this selection has been made correctly).

While there are many similarities in primary research and data collection through the described mediums, the role of the subject and theories of this study impacts the nature of the research carried out. The pre-dominant line of questioning in the research is in regards to the effectiveness of IS security, environmental conditions and impact, and compliance, and thus the research efforts are most mindful of influence, conditions, and potential. The financial institution was chosen to be included in the target audience as the financial institution has among the greatest needs for information systems security; moreover, the information systems in these institutions are particularly large, and there are a great quantity of institutions which increases the potential for the researcher to access a statistically significant quantity of participants. While the government has a comparable need for information systems security, its information system is not as easily analysed in terms of security; moreover, researching would be more difficult as the abundance of locations and accessibility is less than with financial institutions. Meanwhile, as mentioned, the primary members of the target audience will include any member of a financial institution with at least two years of experience with IS security.

The primary data is gathered from at least 50 knowledgeable employees of financial institutions within Saudi Arabia, describing the trends of at least 10 financial institutions and IS security. With this, the study attempts to supplement the findings with additional secondary data in an attempt to discover the causes of such trends. Interviews also look into this area, while the interviews will be strategically designed to be open to the findings of the questionnaire (but still structured to address specific relevant issues, see interviews section for specific details). Thus, the consideration of the financial institutions, through the primary research, will encompass a substantial proportion of the financial industry across Saudi Arabia, reveal the explanations of experienced and knowledgeable members, provide the basis for interview development and application, and will be further addressed with the direction of the secondary research.

While there are many ways of distributing questionnaires, and some have a set of advantages and disadvantages to the researcher which are more desirable in certain ways than the method selected, it is important to describe these methods and their traits as they assist research.

The two most fundamental distribution methods are face to face and group distributions. Meanwhile, a number of mediums could be used in conjunction with these, as personal surveys could be conducted over the telephone, surveys could be mailed using email or postal mail, personal appearances could be used to pass the surveys out to a large group of people, surveys can be faxed, etc. Naturally, the face to face method is the most demanding in terms of time (or travel expenses); however minimises confusion and practically ensures that the researcher leaves with useful information from willing participants. Meanwhile, group distribution is more efficient; however has the potential for confusion and miscommunication (Collis and Hussey, 2003). While the researcher attempts to strategically target people, and not reach a maximised audience, initially face-to-face distribution seemed more desirable; however, given the nature of the demands of the study, the ability to be especially clear within the survey by providing directions as needed, the ability to schedule time and explain the nature of the study personally over the telephone, and other factors, the researcher has decided to distribute the questionnaires in small groups and electronically. With this, the researcher will first contact the institution and attempt to arrange participation, then the nature of the study and participation instructions will be administered, a time will be scheduled, and finally the surveys will be administered. The researcher is to review the results and examine for possible errors, re-contacting parties if miscommunication seems evident. Based on the number of institutions desired compared to those available, the questionnaire goal seemed entirely attainable at the time of the decision for this structure; naturally, this ensures sufficient effort can be placed within the analysis, interviews, secondary research, and other supplemental yet crucial areas of the study.

3.3.8 Phase 7: Data Analysis

Aside from some of the secondary data analysis issues considered in the secondary data section, the final encompassing phase of the methodology is data analysis. Once the entirety of the data has been collected, it is first properly organised and compiled according to the specific research inquiries. Following this, quantitative information is averaged and used in graphical representations to reveal percentages and numerical comparisons between institutions or other areas. Cross-sectional and descriptive statistics are displayed to accompany discussion. Similarly, ratings and observed traits are totalled and assessed, while interviews and secondary research may serve to supplement and facilitate a complete analysis of data. All information collected, unless deemed unfit for analysis due to bias, incorrectness, or otherwise, is used in the analysis of data. The qualitative data will be described in terms of the inquiries, interviews, and secondary research, and any correlations observed will be subject to further analysis prior to presentation and discussion; qualitative data will be discussed in terms of relevant subject matter, with the emphasis given to the topics and concepts most frequently expressed by respondents. The Cronbach alpha statistic will be used for internal consistency and reliability of surveys. Once all totals, average, percentages, comparative tables, traits, statistics, and relationships have been observed, the remainder of the data is described and applied to either the most relevant data, a conclusion or recommendation, or an explanation of why the data is not particularly fitting.

3.4 Secondary Research and Data

The researcher supplements the findings from the primary research and data with additional literature and statistics in a secondary research effort. These serve to supplement the analysis, as well as provide additional reference for the researcher to refer to in describing theory in discussion, conclusion, and recommendation sections. As mentioned, some secondary research is conducted as a direct extension of literature to ensure the most recent and relevant literature is available for integrating with the primary research results, while other areas of the secondary research effort are reliant on the results from the primary data. With this, the nature of the primary research results and data guide the secondary research as it seeks to supplement these findings and implications.

The resources demanded in the secondary research effort are publicly accessible while much less demanding of the researcher's time; therefore, the researcher can undoubtedly carry out this research to every desired detail, unlike the limitations of expenses, accessibility, and time restricting the nature of the primary research. The resources to be used include company profiles and annual reports, government statistics, financial and business statistics, academic literature, scholarly journals, and other reputable and relevant sources.

3.5 Validity and Reliability

Naturally, the researcher must abide by academic policy while asserting that all information is correct, and to achieve this feat, reliable sources must be sought. A quality scholarly research effort best contributes to the current knowledge base when it reveals an abundance of new or supporting data, uses reliable sources, and maintains accuracy; this requires that the research and analysis not only seek valid and reliable topics and resources, but are free from accidental error in mathematical calculations or qualitative relationships. The fundamental theoretical applications of validity and reliability in a research effort such as this, according to Merriam (1988) require checks and balances, supervision, and consideration of potential researcher bias.

The researcher asserts that the information provided in this study is true to the best of their knowledge, and seeks to abide by the principles of validity and reliability; furthermore, the researcher asserts mindfulness of potential bias, while mathematical calculations and qualitative relationships have been closely considered for existing error. With this, the data analysis and discussion will encompass supervision, checks and balances, and adequate consideration of bias.

3.6 Research Ethics

Similar to the consideration of validity and bias, additional ethics apply to the development of this research and analysis. The researcher is well aware of the academic policies regarding research and analysis, as well as the conventional literature calling for ethical issues to be considered when conducting any formal research, such as those commonly referred to as outlined by Collis and Hussey (2003). In order to satisfy the demands of this effort, while abiding by the regulation obligated unto the researcher in this process, the researcher confirms that:

i) all participants will have taken part voluntarily, and not as the result of neither threat nor bribe

ii) the researcher takes care not to disrupt essential business functions while soliciting or conducting the research

iii) the researcher did not support any general opinion while approaching the study with full objectivity

iv) no facts provided by participants have been eliminated for the sake of maintaining theme or hypotheses

v) sources quoted, paraphrased, or otherwise used to aid the researcher beyond common knowledge will be appropriated cited and referenced as demanded by law and academics

vi) confidentiality will be respected under all circumstances

3.7 Limitations of Study

The primary limitations of this study will be the accessibility, funds, and time associated with such a project. Ideally, all financial institutions could be included while all employees with sufficient experience could contribute information. Naturally, this is not possible, and the researcher had attempted to optimise available resources in a practical manner. Meanwhile, the study is further bound by the ability of the questionnaire to extract data, and the ability for the employee to respond with complete accuracy, while both areas are assumed to contribute to the slight degradation of the research results and analysis. Moreover, while the researcher has taken effort to ensure no bias exists while remaining objective, additional biases and limitations may nonetheless exist unbeknownst to the development of this study. However, as described in section 3.7-3.8, the researcher maintains that validity and reliability have been sought throughout all points of this study.

3.8 Summary

This chapter has discussed the details of the research and analysis methodology. The primary and secondary sources have been described in terms of their many components. The two primary approaches to assessing the entirety of these areas will include both primary and secondary research, and as the primary research will be comprised of both questionnaires and interviews, the secondary research will include information regarding IS and best practices from other areas while also being tailored to the results of the primary research. With this, the secondary research will be somewhat reliant on the results of the data analysis, as the researcher will seek to best support and discuss the findings alongside recent statistics and literature by tailoring such research to the implications and nature of the findings from the primary research. The first action to be undertaken in any research effort is the pilot study. Next, interviews and a (potentially modified) questionnaire will be administered to employees and managers playing some role in IS within Saudi financial institutions. Both primary and secondary data sources and research will play substantial roles in formulating conclusions, recommendations, and topics for continued research.

This chapter has also described the rationale behind the specific strategic organisation employed. The areas of methodology considered (in terms of the pilot study, primary data sources, and secondary data sources) include sampling techniques, the sample size of the pilot study and of the primary data, the design and implementation of questionnaires (including organisational theory and distribution techniques), the design and implementation of interviews, and the resources to be used and considered for the supplementary secondary data sources. The significance of this study is evident in the aims and objectives as well as research inquiries and direction. Moreover, by identifying the specific threats to data security in Saudi financial institutions, as well as considering how existing threats are unique to the banking industry, it contributes to the existing knowledge base to close any remaining gaps in literature. The study further aims to identify areas where continued research would be most beneficial, while this is also significant. Lastly, the research inquiries reveal additional significance in the study.

Chapter 4: Description of Context/Case

4.1 Saudi Arabian Context

4.1.1 Introduction

This chapter outlines and analyses the context of information systems security as it exists in relation to the case. As the location of the research is Saudi Arabia, the context of the case is concerned with information system security concepts which are relevant to the nation in present times.

4.1.2 Key Saudi Arabian Conditions

Saudi Arabia is a developing country, and while it is not a global leader in overall development, it has strong economic components, considerable resources and exports, and potential for improving information security. According to recent analyses of the strong components of the Saudi economy, the country is the largest in the Middle East, with 25% of the GDP in the Arab world, while prior ICT plans had attempted to improve eduation, finances, and the influx of legal and technical skills needed to develop more opportunity in the private sector (Althaneer and

Nelson, 2009). Clearly, the nation has the potential for development and improvement, but many obstacles have impeded progress. The government has realised the demand for improved information security, both for organisations and the overall economy, but sufficient action remains to be taken.

National cultural factors in Saudi Arabia have been found to be obstacles to improving information security in themselves. According to research, Saudi Arabian conditions are known to have a tendency to be barriers to adopting cultural practices in organisations, such as new policies, modes of operation, attitudes, and spreading awareness (Althaneer and Nelson, 2009).

4.1.3 Present Demand for Improved Strategies in Saudi Information Systems Security

The demand for improved IT and IS in Saudi Arabia has existed alongside its use of technology, and, despite making considerable efforts (any many being partially successful) to meet the demands, the demand and clear rationale for the demand remains. Many research analyses, governmental analyses, and independent organisations have confirmed this (Saudi Gazette, 2007; Althaneer and Nelson, 2009). Considering one of the most large-scale surveys documenting the demand in the past five years, the Saudi Gazette (2007) reported on a global survey conducting a comparative analysis of 1,200 organisations across 48 countries, with a statistically substantial portion of Saudi Arabian organisations. Based on the findings of the study and the report of the Saudi Gazette, Saudi companies must keep improving their security to address the rising challenges related to information risks; meanwhile, participants in the study were found to be non-compliant with best practices, as less than half stated that they use formal information security approaches or a formal technique in general risk management.

Strategies to improve information systems (IS) security may involve many individual or combined factors ranging from improved software and applications, improved hardware, improved usage of existing technology, awareness of threats and strategic design, or even improved organisational cultures and training which facilitate enhanced security. According to the Zurich insurance company (2008), information security plays a major role in enterprise since it relies on information flow, and meanwhile "*confidence in the integrity and accuracy of the information is just as important as preventing unauthorised access and uninterrupted access to data. Many information security breaches and losses come from internal employees, industrial espionage by competitors, hackers, organised crime, and even foreign governments. Information security does not just mean controlling computer access, but also physical access to secured areas such as data centres*" (p. 1). This is especially applicable to Saudi Arabia, as the nation must improve IS to safeguard its businesses and entire economy; according to Althaneer and Nelson (2009), information security and IS management are essential parts of the information communications technology infrastructure required to support the development of the Saudi Arabia economy. The current conditions in Saudi Arabia thus demand improved technology as well as protocol, and in addition to a demand from financial institutions and businesses, the Saudi economy itself demands improvements (Abu-Musa, 2003).

In addition to this basic demand, the event that no action is taken could result in detrimental effects leading national organisations to lower levels (Saudi Gazette, 2007; Althaneer and Nelson, 2009; Abu-Musa, 2010; Muhaya, 2010). With this, a lack of a competent and thorough approach to research and improvements could cause significant damage to Saudi organisations and the national economy; realising this, the Saudi government has encouraged the establishment of secure environments in both public and private sectors. Muhuya (2010) reports that the security in 'cyberspace' is a natinal and international issue concerned with different types of business; moreover, it is associated with economics and politics, meaning policy development has been of rising interest" (p. 1). Governmental concern has been growing in the past five years, including initiatives as early as 2005, with Prince Muqrin bin Abdulaziz Al-Saud's presentation of a plan to integrate technological development and processes, and collaborating with the United States to improve procedures (Muhaya, 2010). Despite this concern and the efforts made, the demand remains in financial institutions, organisations within the private and public sector alike, and the government (to improve the economy) (Althaneer and Nelson, 2009; Muhaya, 2010).

4.1.4 Developments Contributing to or Affecting Present Context in Saudi Arabia

The Data Protection Act of 1998 from the UK was one of the most major and influential catalysts of change for both IS and security in the information technology age, including Saudi Arabia (The National Archives, 2010). The Data Protection Act of 1998 is therefore an example of how changes may impact this area in response to legislation in the future. The Data Protection Act includes eight principles for information handling that has become the foundation for modern best practices in IS and IS security. These principles are concerned with fair and lawful processing, processing for limited purposes, adequate (and relevant) without being excessive, accuracy, not keeping for longer than necessary, processing in line with rights, international transfers, and other areas (The National Archives, 2010). More specifically, these principles state that personal data should be fairly and lawfully processed, shall not be processed in any manner incompatible with lawful purposes, shall be adequate and relevant, shall be accurate and up to date, shall not be kept longer than demanded by all defined purposes, shall be processed in accordance with the rights of data subjects, that data shall be subject to appropriate technical and organisational measures and that personal data shall not be transferred outside the nation unless that country assures appropriate protection (in according with rights and freedom of information topics relevant to the data) (The National Archives, 2010).

The CTIC (2005) states that the first portion of the new millenium, particularly the first four years, involved much growth for major elements of information communications technology in Saudi Arabia. These elements of growth are reported to include "*mobile subscribers with cumulative annual growth rate (CAGR) of 58.6% (more than twice the world CAGR of 23.4%), with subscribers approaching 12 million as of October 2005 (over 50% penetration). Internet users grew by over 430% in four years, amounting to CAGR of 44.4%, (vs. world growth rate of 27.4%); internet users are exceeding 2.5 million. Personal computers (PC) penetration has also grown 40% annually (vs. world PC growth rate of 9%) to around 16% penetration. Fixed mainland telephones are approaching 4 million lines (a tele-density of 17%). Internet international bandwidth capacity has increased by nearly 7 fold in 4 years to over 1800 Mbit per second*" (CTIC, 2005, p. 1). Althought these changes were great for the nation, they were not always accompanied by the proper improvements of security, and the overall infrastructure and its security were still deemed to be insufficient.

Fortunately, Saudi Arabia is at least used to ongoing changes in these areas, and is thus less likely to be resistant to continuing change towards adequate IT and IS; by 2004, Saudi Arabia had experienced substantial reforms in its Telecom sector, in IT, and in legislation. The following years also gave rise to many changes which have created the current IS context. Further contributing to the vulnerability amid these changes in the early millenium are the major rises in e-commerce and online banking (CIST, 2005). The rise in such technology in the absence of proportional rises in IS (compounded by the fact that the IS prior to these changes was already inadequate) created great vulnerabilities in many areas, and especially within financial instituions offering electronic services.

In 2005, a National Communications and IT Plan (NCITP) was developed. This included a five-year plan for Communications and IT in the country, and a long-term perspective for Communications and IT in the country (Althaneer and Nelson, 2009). More recently, the Saudi government has established ICT infrastructures to increase the productivity and performance of organisations and individuals in Saudi Arabia. Although this was intended to facilitate improvements, as a result, adopting some practices within Saudi organisations is a major challenge to be dealt with; now it can be more difficult for financial instituions to protect their economic assets from attacks and intruders amid these increased productivity requirements (Althaneer and Nelson, 2009). Additional improvements in specific security protocols, to at least match the established policies, are thus now also in demand.

In 2007, the United Nations described a complex plan which Saudi Arabia had considered for redesigning its ICT sector with the intentions of improving the economy through the resultant increased competition, increased local and foreign investment, and the additional protection of consumer and stakeholder rights (United Nations, 2007). In 2003, Saudi Arabia’s governmentally operated telecommunications organisation was partly privatised, affecting the nature of the largest communication entity, and compounded the results of the Communications and Information Technology Commission’s (CITC) establishment in 2001. While these areas were acquiring power to develop protocol for any aspect of information technology and information security in major Saudi Arabian communications, while further achieving a higher level of financial and administrative independence. According to the United Nations (2007), the government has attempted to liberalise the market to create a positive framework to invest in the ICT, and by 2004, there was competition in the mobile and telecom areas; competition also led to fixed serves and market liberalisation was created to issue licenses in 2007 (p. 5). As mentioned, such improvements have done little to change the overall situation in Saudi Arabia.

Also, as mentioned, e-commerce has grown greatly in the past decade, and this has increased internet usage and a general demand for other convenient online services and internet technology. Saudi Arabians have been able to use the internet since 1998 (when domestic servers were implemented), and the number of users rose from 350,000 in 2001 to 2.2 million (roughly 10 percent of the population) in 2008; this rate continues to grow along with the falling prices of technology and the growing population, and this alone creates a greater security risk overall (Alfuraih, 2008). Meanwhile, the overall population is limited by the price of service, the limited ISPs available to non-university organisations.

In 2010, the conditions for IT infrastructure and IS had not improved; while new developments and initiatives for improvements continue to be considerable in number and continually mindful of the problem, the overall solution eludes the country while all existing aspects are incomplete (Abu-Musa, 2010; Muhaya, 2010).

4.1.5 Incomplete Elements of Implementation in Saudi Arabia

Incomplete security solutions are as much of a problem as ineffective security solutions in Saudi Arabia, while security threats and attacks commonly find a loophole in systems comparably as often as they find a way though an existing security measure (Bellamy, Perri, and Raab, 2005; Stamp, 2006). Saudi Arabia has many examples of incomplete solutions, as the combination of existing technology and policies have addressed the issues but failed to offer a complete solution. The optimisation of IS security in Saudi Arabia should therefore involve balancing both protection as risk as to counter both the defence against attacks as well as vulnerability to general threats. In the case of the firewall defence instrument, a common element offered amid the present incomplete solutions, defence is generally the use of software in terms of hardware characteristics, and thus has a hard-coded functionality set (Wells, 2007). However, the aforementioned improvement of the overall ICT infrastructure is required for adequate IS.

In a recently analysis of the effectiveness of IS, Abu-Musa (2010) found a general lack of completeness and effectiveness, reporting that most Saudi companies do not have any plans for disaster recovery to management information security complications or even emergencies. Moreover, the information security roles and responsibilities are not explicitly defined or communicated with the employees or even amongst the managers. Their analysis determined that the relationship between IS and the companies' business strategies are ineffective, recommending improvements in all areas. Clearly, there is an unfortunate lack of effective implementation and success in current procedures despite all described actions from the government, in response to awareness, or through other changes. Abu-Musa (2010) also found that all risk management processes for IS are neither integrated or maintained at a level capable of meeting demands, that IS is rarely an aspect routinely considered in operation by key authorities of organisations, and that there are no sufficient management systems for IS in the majority of organisations across the nation. Abu-Musa (2010) concluded that, despite all efforts in the past years, there was a clear and present need to improve IS and IS management for the good of the entire nation. Incomplete solutions are common, and a conceptual approach to developing strategy in Saudi Arabia may give rise to a methodological and systematic optimisation of instrumentation, networks, infrastructure, processes, and overall operation.

Generally, incomplete solutions are a common problem, and nations behind the developed nations are vulnerable to IS threats much greater than developed nations which have discovered areas of incompleteness and risk. While a conceptual approach to developing strategy can give rise to a methodological albeit precise improvement of IS security instrumentation, networks, infrastructure, processes, and overall organisational operation.

4.1.6 Other Aspects of Existing Threats

The nature and potential of threats has proven to be a continual concern in Saudi Arabia over the past decade. Recent research and formal analyses of examples have examined the nature of existing threats to reach conclusions, and have revealed the nature of development in the country as it examined the attempts to improve overall results. In Saudi Arabia, the fundamental threats of hacking, information theft, and sabotage remain potent in the present as they were in the past decades, making information system security comparably important on a conceptual level despite the advances in technology (Mahaya, 2010). Meanwhile, numerous methods of attack continued to challenge existing Saudi Arabian information security specialists, and the threat evolves alongside the changing uses of developing technology.

Analysing Saudi Arabian IS security policies may involve individuals or groups that are allowed to access variety categories of information, and this often involves security levels or specific classifications for information. Threats and attacks exist across the spectrum of topics described above in addition to other potential areas, and incomplete security solutions are as much of a problem as ineffective security solutions. Security threats and attacks commonly find a loophole in systems comparably as often as they find a way though an existing security measure in any nation, and Saudi Arabia’s conditions amplify the severity of this trend (United Nations, 2007). Threats and attacks can potentially forcibly penetrate even the more advanced systems in developed nations because loopholes have been discovered in firewalls, DMZ, VPNs, and SSL in recent years; any nation behind on implementing technology are all the more vulnerable to the risks discovered in the most advanced technology, and clearly the initiative in place in Saudi Arabia are unable to adequately address these concerns (Abu-Musa, 2010).

4.1.7 ISO 27000 Compliance

The ISO 27000 series (also known as IS027k) of standards is a recent set of information system security standards which have been observed around the world, however most commonly within more developed nations such as the U.K. and U.S. According to the IsecT Ltd (2011) webpage, "the "ISO27k" (ISO/IEC 27000-series) standards provide good practice guidance on designing, implementing and auditing Information Security Management Systems to protect the confidentiality, integrity and availability of the information on which we all depend. Ten ISO27k standards are published so far." Although Saudi Arabia has shown interest in becoming ISO27k compliant, the available information shows that they are among nations with markedly lesser progress and concern. While the information regarding compliance is scarce, the majority of available statistics reveal standards purchasing trends, and often times these are depicted only by nation (and not in breakdown of organisation as sales and data processing organisations have refused to provide such breakdowns); journals and published research have avoided this topic, and sales records in the past five years generally show that less than 30 Saudi organisations have purchased the standards, compared to the 300-500 organisations (each) in the U.S. and U.K. (NSI Ltd, 2006; ISO Directory, 2007; Issociate, 2007; Compliances Forum, 2008). The lack of data on even this level in recent years shows both a gap in focus and concern from both the nation's organisations and researchers alike.

Although no studies have targeted the precise nature of the lack of participation regarding the ISO 27000 adoption, the low purchase rates are clear examples of the trends observed and explained by the aforementioned literature. Abu-Musa (2010) recently observed a lack of efforts in completing security plans, developing security policy statements, or even developing and integrating concrete strategies. He also found that these areas and a lack of disaster recovery plans were commonplace in the majority of Saudi organisations. Muhaya (2010) observed a similar incompleteness and lack of motivation for formalities and improvements, and Althaneer and Nelson (2009) observed apathy or resistance towards adopting new policies, modes of operation, or even spreading awareness. As ISO 27000 are fairly new standards, and Saudi organisations seem to have a trend of avoiding exerting time and resources unless it is required, the (comparatively) low participation in ISO 27000 is another example of this trend.

4.1.8 Final Remarks Regarding Saudi Context

As the above has shown, Saudi Arabia, like many other fast-developing countries, faces IS problems that are specific and, in some respects, of greater magnitude than developed nations of the world. While certain organisations may choose to ignore the risk and operate with little concern for improvement, Saudi financial institutions are in an extraordinarily vulnerable position. Despite efforts to improve IS and IT infrastructure in general, the Saudi government has been unable to strategise and implement a sufficiently complete solution. Generally, IS is presently at the crossroads of four diverging poles of interest, and management teams must make informed decisions as Saudi IT staff serve the system, Saudi auditors attempt to control the system, and Saudi users use the system according to legislation developed and implemented by the Saudi government. Meanwhile, Saudi security professionals must be mindful of the incompleteness of even modern tools, while research and implementation efforts should be conducted periodically as well as when needed to ensure that vulnerabilities due to incompleteness do not give rise to breaches. Numerous methods for improving IS have been proposed from and to information security specialists in recent years, and while the threat evolves alongside the changing uses of developing technology, continuous analysis and strategic implementation is in high demand across the entire Saudi economy.

4.2 Saudi Banking Industry and Significance of Sampled Organisations

Justifying the statement that 10 banks is a statistically significant portion of the banking sector, this section briefly introduces the banks. The 10 institutions used were the National Commercial Bank (the bank with the most Arab assets, owning 90.4% of the NCB's Capital, the premier Investment bank in the nation, also having SAR 345.3 billion (US$ 92.08 billion) in assets), the Arab National Bank (with 178 national branches, 183 total and ~3500 employees), the Al-Rajhi Banking & Investment Corp. (the largest Islamic bank in the nation, with 7,600 employees), the Riyadh Bank (a larger and therefore 'significant' bank with SR 3.030 million annually and total assets of SR 176 billion), the Saudi American Bank (now referred to as the Samba Financial Group, with 66 local branches and a few dozen international facilities), the Saudi British Bank (a larger joint stock company with over 5,000 employees), the Albilad Bank (a joint stock company with ~3200 employees and capital of 3,000,000,000 Saudi Riyals), the Saudi French Bank (the first private bank opened in nearly 40 years in 2004), the Saudi Hollandi Bank (the oldest operating Saudi bank, opened in 1926, currently with approximately 1400 employees, and the first to introduce many aspects of banking technology), and the Saudi Investment Bank (having full range services including Islamic banking, medium market cap size) (Gulfbase.com, 2012).

4.3 Conclusion

As mentioned, Saudi Arabia is a developing country, and while it is not a global leader in overall development, it has strong economic components, considerable resources and exports, and potential for improving information security. The local context is one in need of improvement, even in the larger banks; also as mentioned, Abu-Musa (2010) recently observed a lack of efforts in completing security plans, developing security policy statements, or even developing and integrating concrete strategies. He also found that these areas and a lack of disaster recovery plans were commonplace in the majority of Saudi organisations. Muhaya (2010) had observed a similar incompleteness and lack of motivation for formalities and improvements, while Althaneer and Nelson (2009) also observed apathy or resistance towards adopting new policies, modes of operation, or even spreading awareness. Numerous methods of attack have continued to challenge information security specialists in recent years, while the threat evolves alongside the changing uses of developing technology. Clearly, the potentials of threats and attacks have been found to be a continual concern in recent examples; they have the potential to match or exceed the potential safety provided by information systems security. This has led to experts and analysts questioning current security levels, and forms the basis of recent and on-going research. Analysing IS security policies may involve individuals or groups are allowed to access variety categories of information, and this often involves security levels or specific classifications for information. Threats and attacks exist across the spectrum of topics described above in addition to other potential areas, and incomplete security solutions are as much of a problem as ineffective security solutions.

Chapter 5: Results and Analysis

5.1 Introduction

This chapter presents the results of the primary research, revealing the responses of the survey questionnaire and interviews. While a minimum of 50 survey respondents across 10 organisations were considered in the development of the research methods, a total of 100 respondents were willing and able to participate in the study within its time constraints; the initial 50 were able to participate quickly within the time constraints (using email), and once another 50 were able to participate, the researcher felt that this was a sufficiently statistically significant number (considering literature) and ideal 'stopping point' for surveying. Meanwhile, the minimum of 10 interview respondents mentioned in the research methods would be exceeded by six within the available time.

5.2 Pilot Study and Distribution

As mentioned in previous chapters, a small pilot study was planned prior to full scale distribution. This study used the entirety of the questionnaire, distributed to only a small percentage of the target audience. A total of five respondents, representing 10 per cent of the minimum sample size, completed the survey questionnaire. After reviewing the results, their completion of the questionnaire was deemed suitable as the questionnaire items were deemed viable for full scale distribution. The results of the pilot study were therefore included as a portion of the net results, and became part of the totals used for the results and analysis below.

5.2.1 Demographic and Misc. Information

The demographic information section was a brief segment of the questionnaire which was placed between the completion instructions and the first questionnaire item. This section requested that respondents list their age, gender, organisation, position, and time employed with the organisation. The average age of respondents was 34 years (SD=7.2), with the lowest age at 18 while the highest age was 62. The majority of the respondents were male, as the total was comprised of 65.4 per cent men and 34.6 per cent women; although this is not a completely representative sample of gender or age in the financial sector, it is nonetheless indicative of the observable trend of men dominating the workforce in Islamic nations. The percentages of employees serving in the aforementioned list of organisations was also calculated from provided totals, with approximately 18 per cent from Al-Jazira Bank, 14 per cent from Arab National Bank, 11 per cent from Al-Rajhi Banking & Investment Corp., 14 per cent from Riyadh Bank, 6 per cent from Saudi American Bank, 11 per cent from Saudi British Bank, 6 per cent from Albilad Bank, 6 per cent from Saudi French Bank, 8 per cent from Saudi Hollandi Bank, and 6 per cent from Saudi Investment Bank.

The leading position among the respondents was a variation of a computer technician (such as "technical supervisor," "systems operator," and similar titles), while approximately 59 per cent of respondents reported being employed in this position. All employees confirmed having a substantial role in information security prior to participation. Following this, a lower-level management position was most common, with 24 per cent of employees having some sort of team leader position (while titles included "department supervisor," "assistant manager," "technical supervisor," and others). The remaining portion of employees (17 per cent) were members of middle or upper management. The average time spent at the organisation listed was 7.6 years (SD=4.3), with the minimum time being 6 months, and the greatest amount of time being 22 years. Figures 5.1-5.3 below (graphically) display the age, gender, and position statistics.

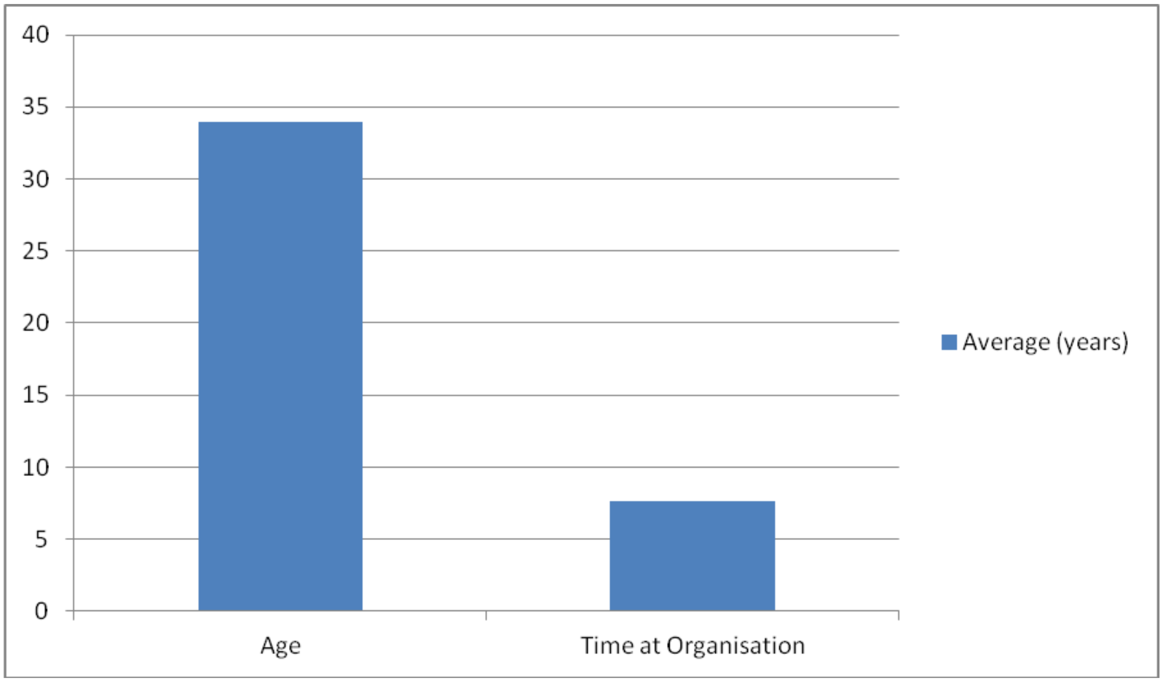


Figure 5.1: Average age and time at organisation

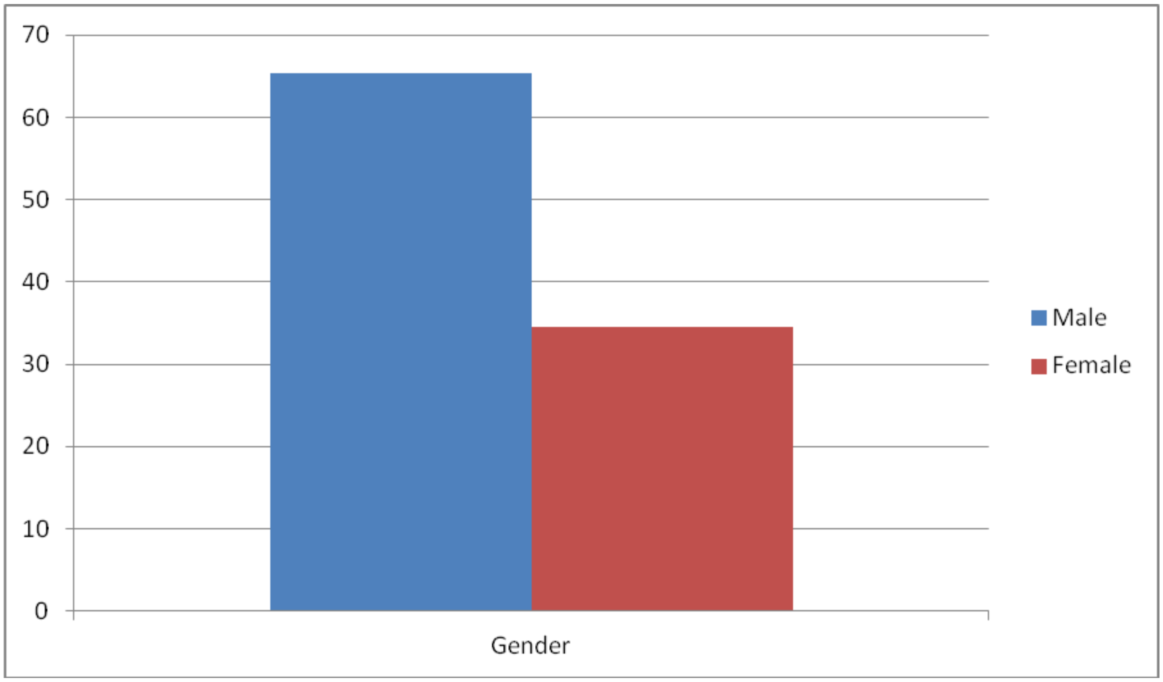


Figure 5.2: Gender Percentage

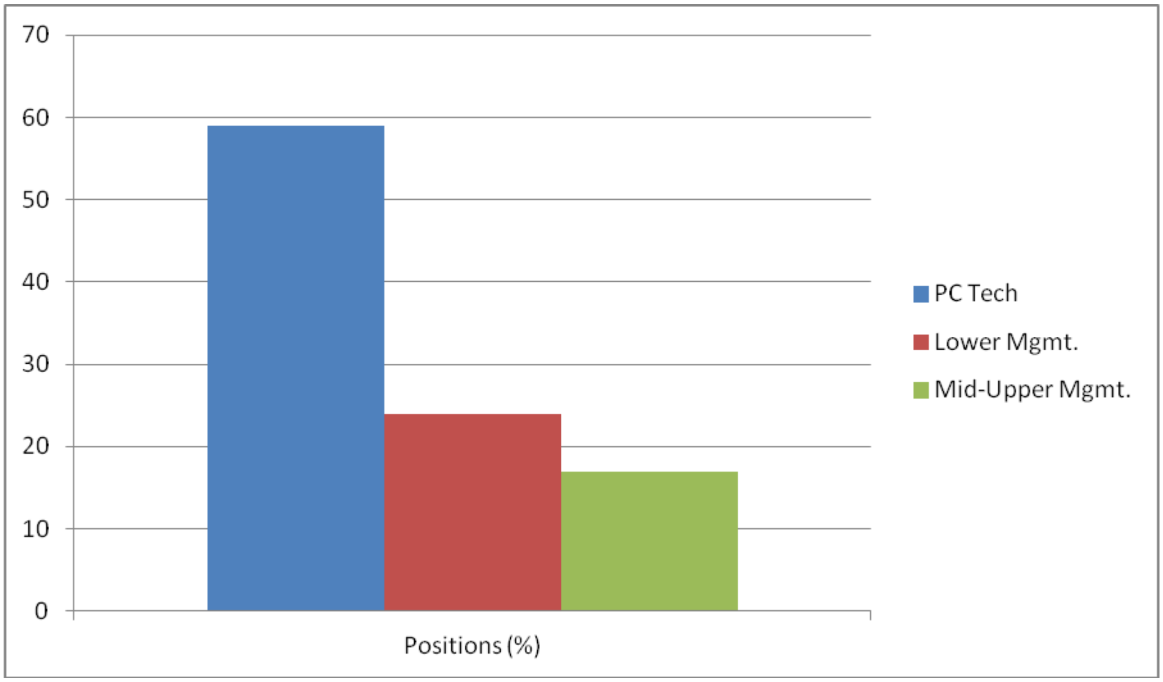


Figure 5.3: Positions

This portion of the questionnaire shows that the majority of employees work directly with IS operation, while a substantial portion of the employees monitor and manage these operations. The employees also have, on average, an amount of experience with the company which is more than substantial for the purposes of this study.

The pilot study, seeming to the benefit of the study, did not inform of anything except the acceptability of the instrumentation and introduce the feedback. Nothing else substantial was learned from the few completed instruments, but the researcher expected this. The following section presents the hypotheses, followed by questionnaire results provided by this blend of employees.

5.3 Hypotheses

As stated in the research methods, 30 questionnaire items were designed to address 10 subareas within the overall inquiry. Restating these subareas prior to discussing the hypotheses, the inquiries are: i) what are the primary threats affecting information security in financial institutions within Saudi Arabia? ii) how are these threats unique to this sector? iii) what policies and procedures are currently in place? iv) how well do employees follow information security policies and procedures? v) what factors affect the willingness of employees to comply with policies and procedures? vi) how do personal ethics affect compliance with policies and procedures? vii) how do various institutional factors impact employees’ willingness to comply with policies and procedures? viii) are there aspects of the current information security policies of procedures that make it difficult for employees to comply? ix) how do overall organisational characteristics affect the successful execution of information security success? and x) what improvements can be made to increase effectiveness of information security operations?

5.4 Questionnaire Results

This section presents the results of the questionnaire, considering the 100 total respondents. Totals, averages, and percentage comparisons are provided where relevant. Standard deviations are provided in parenthesis, denoted by 'SD' and a subsequent value. T-tests, providing values for t, are also provided for responses involving ratings (i.e. responses considerate of a scale of 10), and are denoted alongside standard deviations as 't.' T-tests are calculated using the one-sample method for middle values (i.e. 5 on a scale of 10 to represent no bias in response). P-values were calculated using the degrees of freedom (sample size-1=99) and t-values, while values less than .05 were assumed significant; the results reveal most areas have comparable significance.

The 10 institutions used for these questionnaires (as well as the interviews) were the National Commercial Bank, the Arab National Bank, the Al-Rajhi Banking & Investment Corp., the Riyadh Bank, the Saudi American Bank, the Saudi British Bank, the Albilad Bank, the Saudi French Bank, the Saudi Hollandi Bank, and the Saudi Investment Bank. The discussion in this section is divided across multiple subsections, including the presentation of demographic information (preceding the results), multiple subsections covering portions of the questionnaire, and an additional section (completed by the researcher) regarding additional information regarding the nature of the organisation.

5.4.1 Questions 1-6: Threats and IS Development

The first questionnaire item requested that employees rate the level of current threats perceived to information systems, using a scale of 1-10 (with 10 representing the highest level of threat). The average response to this item was a rating of 6.9 (SD=1.2, t=15.83, p=0), denoting a clearly substantial threat. This also shows that while a substantial portion of the respondents viewed the threat levels as moderate, a comparable level of employees felt that the threat level was quite high (or even near the maximum level). In any case, this clearly suggests that information system security is an issue across the organisations, and across Saudi Arabian financial institutions, and is therefore an issue worth pursuing. This is further supported by the second item, asking respondents whether this level was typical of information security threats at the organisations; 83 per cent of the respondents stated that the level was typical. Following this, the third item asked respondents to rate the average level of threat severity, and the average level received here was 6.7 (SD=1.8, t=9.4, p=0). This shows that the respondents which stated that the levels of threat were unusual experienced a combination of threat levels above and below average. Overall, the questionnaire results highlight that employees feel the security levels have been substantially compromised, under a range of conditions.

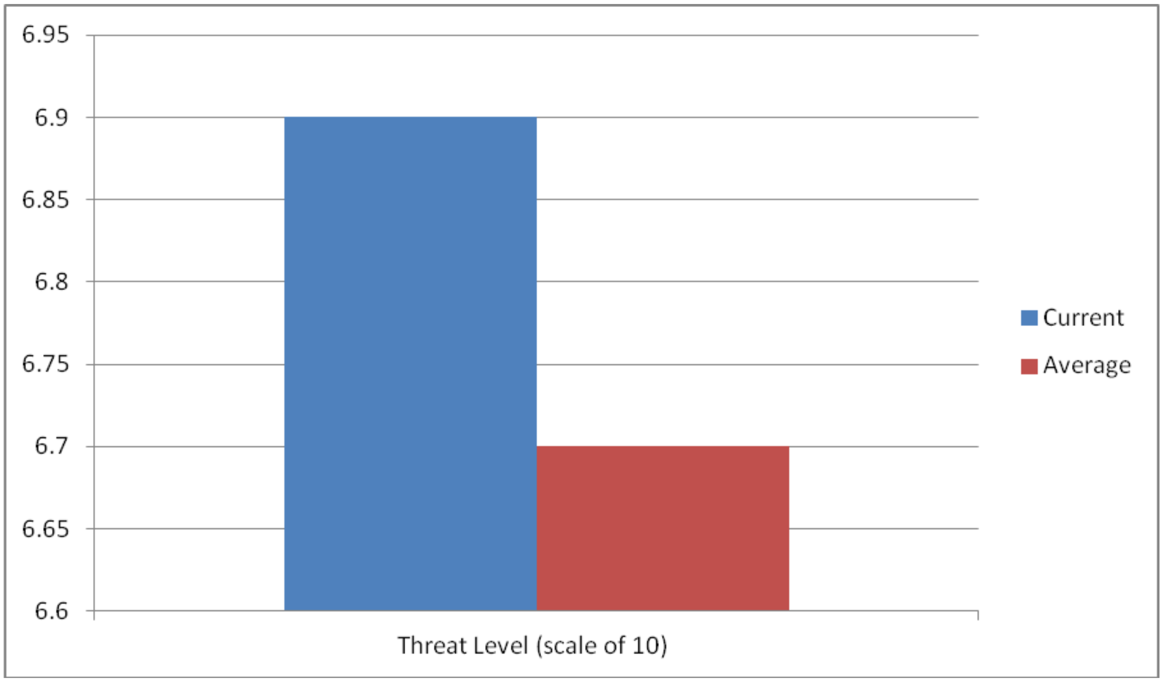


Figure 5.4: Threat level

The fourth, fifth, and sixth questionnaire items addressed information security as addressed by management, the prevalence of system upgrades, and the prevalence of policy and procedure updates (respectively). Responding to the inquiry, "how often is information system security addressed by management in the facility," while choosing between the selectable responses "never," "seldom," "when needed," "fairly often (routinely)," or "often (routinely)," the majority of respondents stated "when needed." More specifically, 1 per cent of respondents chose "never," 28 per cent chose "seldom," 44 per cent chose "when needed," 22 per cent chose "fairly often (routinely)," and the remaining 5 per cent chose "often (routinely). Figure 5.5 below displays the frequency IS was reported to be addressed by management.

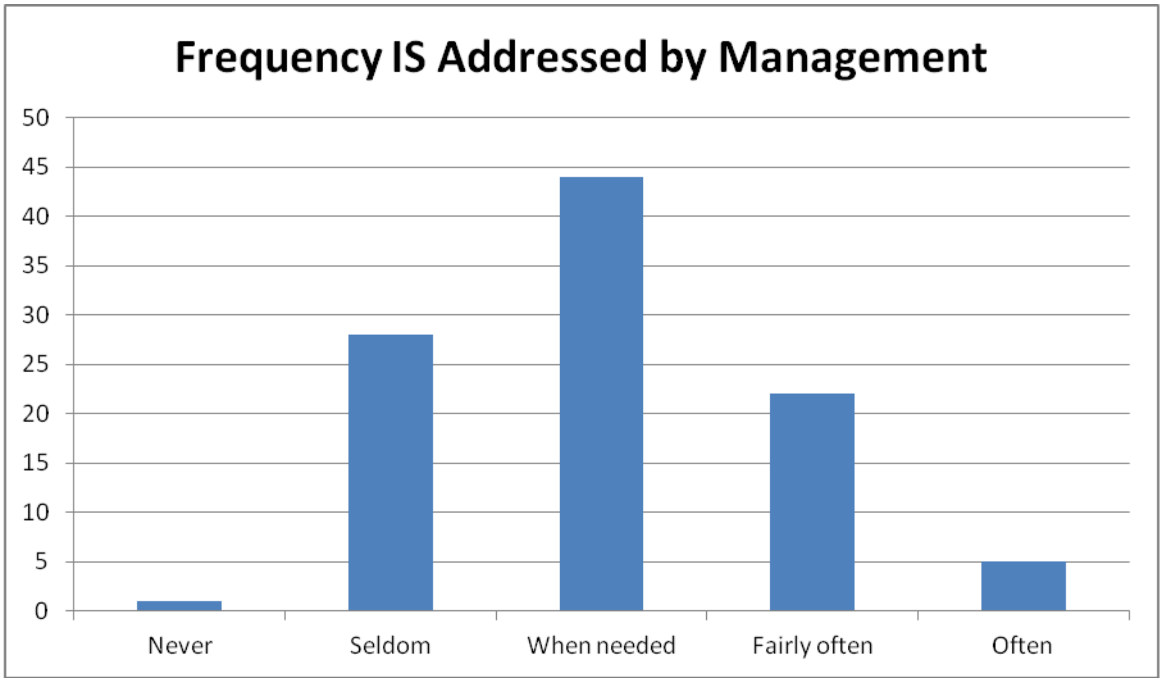


Figure 5.5: Frequency of IS addressed by management

Responding the question "*are routine upgrades made to hardware and software*," only 27 per cent of respondents answered "yes." While the possible time intervals defining 'routine' were not mentioned in this inquiry, over 70 per cent (73 per cent) of respondents claimed that there was no program in place for routine maintenance and upgrades to hardware and software. The sixth question then asked respondents to state whether policies and procedures were routinely updated, and 64 per cent of respondents stated that their company did not have a system for routine upgrades in this area either. While this figure is less than the figure for hardware and software routine upgrades, the percentage is relatively large, implying that there is a lack of organisation for addressing development.

5.4.2 Questions 7-13: Policies and Procedures

The seventh through twelfth questionnaire items each asked respondents to address some aspect of policies and procedures. The seventh item asked, "*how effective do you rate the policies and procedures, on a scale of 1-10?*" To this question, respondents rated the elements somewhat higher than is implied by the other responses, with an average rating of 6.3 (SD=2.2, t=5.91, p=0).

Next, for the eighth item, respondents were to state whether the prevalence of information system security examination and testing is best defined by 'routinely,' 'occasionally,' or 'never.' The majority of respondents selected 'occasionally' (68 per cent), with the substantially lesser remainder selecting routinely (19 per cent) and never (13 per cent) (see Figure 5.7). This question, similar to the item in the previous section which did not have a clear definition, could have been more valuable if the nature of occasionally was provided from respondents having selected it. Meanwhile, it is clear that the majority of respondents do not see routine maintenance of physical or organisational elements. The occasional nature of examination and testing may also play a role in the lack of action, or action considered 'as needed' being rare, as a lack of examination and testing may leave company authorities unaware while the systems remain vulnerable.

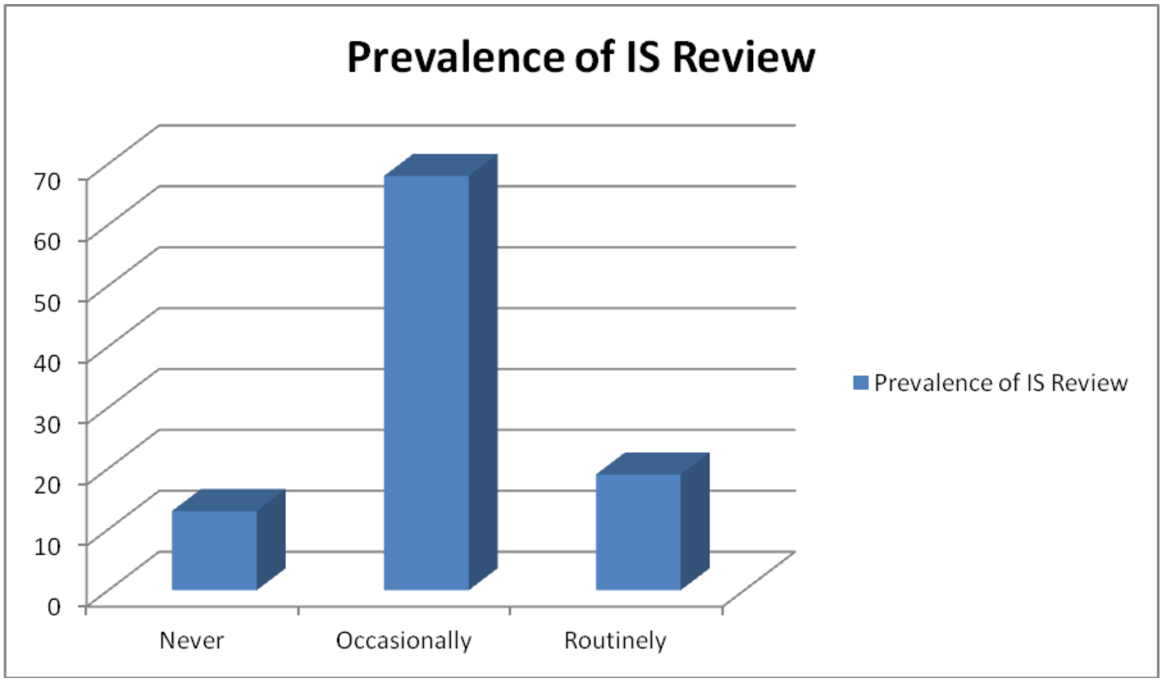


Figure 5.6: Prevalence of IS Review and Examination

The ninth item requested that respondents provide details regarding the nature of training. Specifically, the respondents were asked to select from the possible answers "routinely," "occasionally," or "never" in regards to the prevalence of employee training or work-related education. The overwhelming majority (81 per cent) selected "occasionally," while only a fraction (15 per cent) selected "routinely," with the remaining 4 per cent selecting "never." The impact of this finding demands further research and while it implies that employees are not properly trained while these statistics contribute to vulnerability, details regarding the demand for training are unknown. The following and tenth item asked respondents to rate their managers' compliance with information security policies and procedures. In response, the bulk of employees (44 per cent) rated their managers as "average" in this area, the next largest amount (24 per cent) rated the compliance as "poor," with a comparable amount (23 per cent) rating it as "good" alongside the meagre 9 per cent rating managerial compliance as "excellent." Aside from a larger portion of employees rating managerial compliance as 'poor' than 'good,' the amount of employees rating it as ‘average’ is nearly five times the amount rating ‘excellent.’ This implies there is a need for improvement in managerial compliance of information security policies. Considering this to be a scale of 1-4, the mean response was at 2.17 (SD=.9, t=1.88, p=.316), and thus slightly above the ‘average’ rating. The eleventh item asked respondents to rate employee compliance in this area using the same range of adjectives, and the results show a comparable but lesser level of employee compliance; fortunately, however, these results show that managers are examples for employees in spite of less than ideal percentages. The ‘excellent’ choice was selected by 7 per cent of respondents, the ‘good’ choice selected by 18 per cent, ‘average’ selected by 56 per cent, while the remaining 19 per cent selected the ‘poor’ option. Considering this question to also be based on a scale of 1-4, the mean response was 2.13, (SD=.8, t=1.625, p=.054) comparable to the previous response and slightly higher than a 2.0 average (carrying out a two-sample t-test with the previous two questionnaire items, t=.03). See Figure 5.8 for detailed comparisons of employee and managerial compliance).

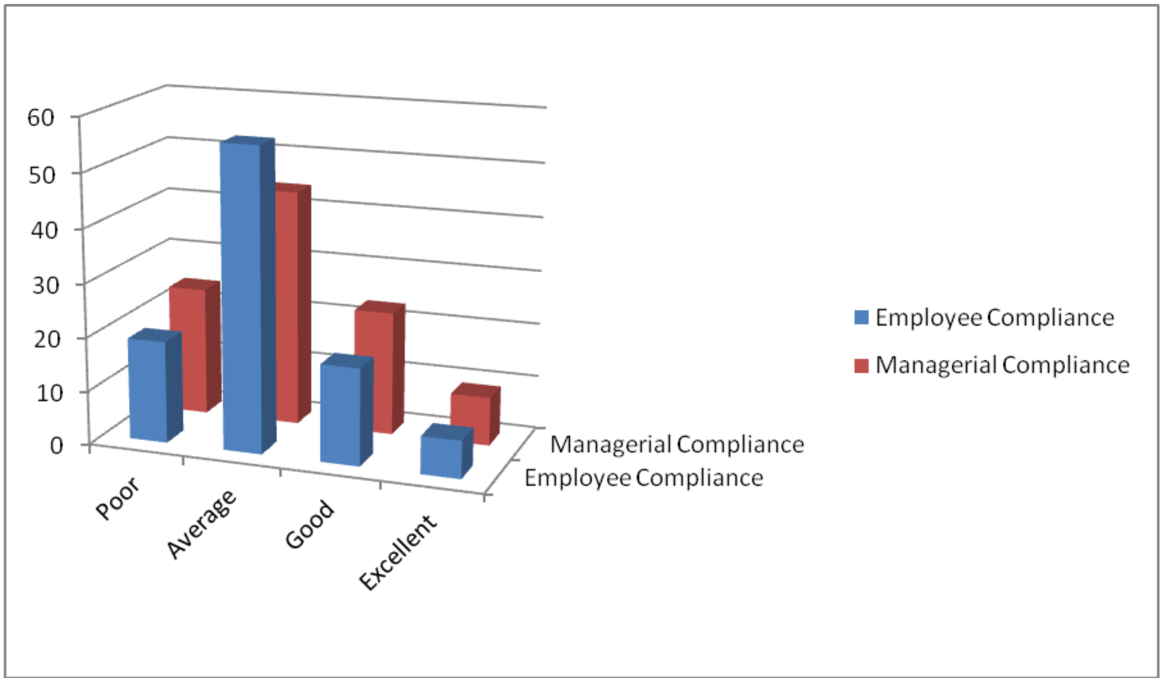


Figure 5.7: Results to items 10 and 11- compliance ratings (managers vs. employees)

The twelfth item on the survey questionnaire was open-ended, and asked respondents “what is the primary reason that managers may not follow policy?” Respondents provided a range of responses, while many of them were effectively different versions of the same responses. The majority of respondents (nearly 50 per cent of the total offered a response of this type) stated that the primary reason was a lack of organisation and seriousness in the organisation, entailing that managers effectively make their own rules. This also implies that it is acceptable to bend or break rules for reasons understood within the organisational culture, and that policies are not sufficiently updated to address issues as they arise, leading to an acceptance that policies are simply formalities and not governing elements within the organisation. This was not, however, confirmed by any follow-up questions within the survey questionnaire, while the previously mentioned implications have a stronger possibility of being the primary motivating factors, although the interviews were able to extract some supplemental information regarding this observation. Other prominent responses to the twelfth questionnaire item included a lack of sufficient knowledge, a lack of incentive, and attempts to increase efficiency. Similar to the previous two questionnaire items, the thirteenth item attempted to discern the nature of employee actions, allowing for a comparison between employees and managers in the same area. When asked about the primary reason employees are not compliant with policy, a greater amount (compared to responses considering managers) stated that ignorance of policy was the cause (these are also reflected in the interviews, see the following section and Appendix B for details). Clearly, this shows a demand for increased awareness or training. Other responses included attempts to be efficient, attempts to operate more effectively, and general carelessness; with this, meanwhile, there was a substantially lower percentage of employees stating that employees were careless compared to managers. This suggests the power of authority facilitates employee compliance, while managers may feel their position of power makes them ‘above the law’ and freer to ignore policies as they see fit.

5.4.3 Questions 14-17: Security Threats

The fourteenth questionnaire item asked respondents if they are aware of any threats which are unique to their institution (with the potential to select either ‘yes’ or ‘no’ as a response). Only 12 per cent of the respondents selected ‘yes,’ in agreement with the studies reviewed in the literature section implying that threats common in Saudi Arabia generally apply to organisations in a comparable manner (Abu-Musa, 2009; Muhaya, 2010). Figure 5.9 demonstrates the unbalanced proportion of responses to this question.

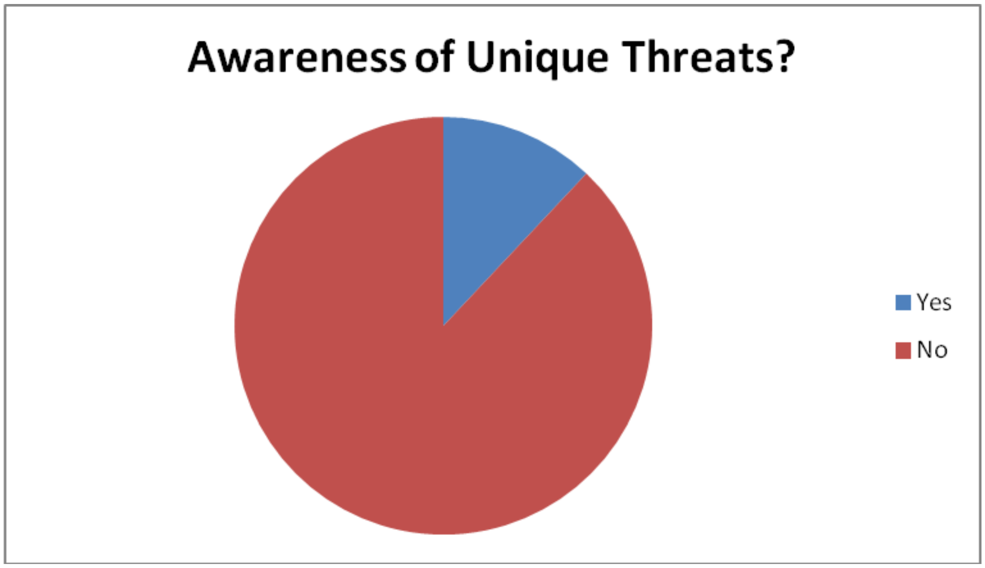


Figure 5.8: Awareness of threats unique to organisation

It was assumed that even employees aware of the details of security threats may not have the experience or perspective to compare threats with other organisations in such a manner that they could confidently state that they are unique, but this item was nonetheless included in the questionnaire as an attempt to gain potential insights into the matter. (It was also assumed that the combination of the responses and the data extracted from the interviews had a higher potential to generate meaningful information.) The subsequent question, item fifteen, asked respondents to state the nature of this threat (this item was an open-ended question). Of the mere 12 per cent of respondents for which this item was applicable, these respondents stated that the unique threats were due to their computer hardware, software, and network infrastructure. A larger number of individuals claimed they were aware of threats unique to their sector (via the sixteenth item), implying that the low number of responses claiming unique threats to the institution was a partially a result of perspective (and not due to such a low level of unique threats). The 31 per cent of respondents claiming they observed threats unique to their sector described the nature of threats through the following question (item seventeen); this revealed that the majority of these threats were also in the form of hardware, software, and network infrastructure vulnerabilities. Figure 5.10 shows the awareness of unique threats.

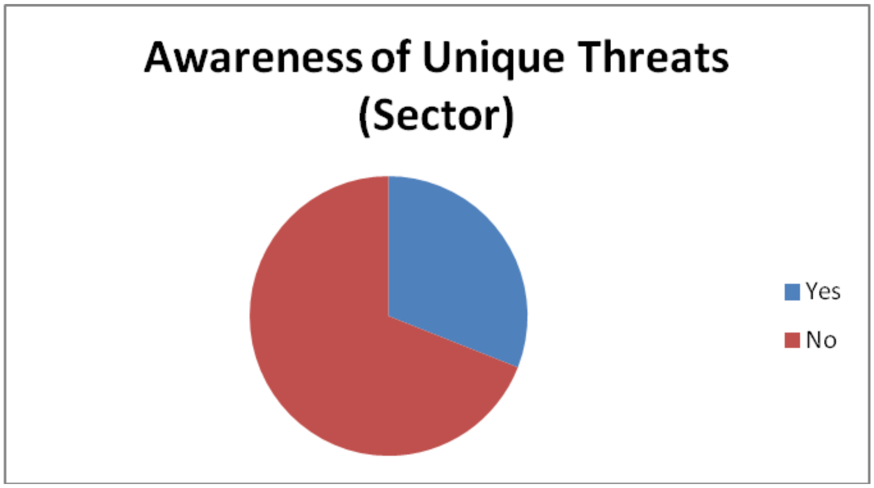


Figure 5.9: Awareness of threats unique to sector

Although the information from this group of questions implies that security threats are either more easily recognised between sectors, or that security vulnerabilities are more similar between organisations than sectors, there are too many possibilities for misinterpretation for these items to contribute to solid conclusions in the discussions included in the following chapter. Mention must be made that, despite the potential for unviable information to be generated from these questions having been considered following the pilot study, the researcher nonetheless allowed them to stay while assuming that the combination of these items with the semi-structured interviews would generate data worthy of consideration.

5.4.4 Questions 18-23: Ethics, Focus, and Improvements

The following six items of the survey questionnaire requested that respondents share their perspective and opinions regarding ethics, focus, and improvements within their organisation's information system security. Item eighteen asked respondents "do you feel personal ethics play a role in managers' compliance," while respondents had the opportunity to select either "yes" or "no." The overwhelming majority of respondents claimed that ethics do play a role in managerial compliance, with 72 per cent of the employees stating that ethics is a considerable cause of non-compliance. Despite the strategic design and emphasis of the questionnaire, as well as its pilot study, this question may have benefitted from a restructuring while using the rating scale for possible responses; employees were unable to state the degree by which ethics impacted managers, while the previous tenth item allowed employees to rate levels of compliance on four different levels ranging from "poor" to "excellent." As stated above, 68 per cent of employees claimed that managerial compliance was "average" or "poor," with only 23 per cent rating their compliance as "good" alongside the mere 9 per cent rating it as "excellent." Naturally, the extent by which these respondents felt that ethics impacted managerial compliance would have ranged a considerable amount if known. Meanwhile, only 34 per cent of respondents chose to list some reason explaining why they felt that ethics played a role in managerial compliance, with listed reasons including managers’ feelings that the ends justify the means, managers simply having a general disregard for policy, and managers’ feelings that policies are only (partially successful) attempts at generating desired responses.

The following item (number nineteen) also allowed ethics to be considered amid a comparison to the previous item regarding employee compliance. When asked whether personal ethics play a role in employee compliance, 80 per cent of respondents stated that personal ethics plays a role in employee compliance. Citing the previous responses to the eleventh item, 75 per cent of respondents stated that employee compliance was average or poor, with the remaining 25 per cent selected good (18 per cent) or excellent (7 per cent). The definition of “average” had not been discussed, but even if “average” could be equated to acceptable within the company, nearly one fifth of employees and nearly one quarter of managers were rated to be outside of this range of acceptability; meanwhile, assuming that only “good” or “excellent” levels of compliance are expected from either managers or employees, only one quarter of employees and approximately one third of managers were rated as being within this acceptable range. Reasons as to why ethics are assumed to play a role in employee compliance included low work ethic and motivation, carelessness and a lack of obedience, and the feeling that they better address needs through their own action.

The twentieth item (see Figure 5.11) requested that respondents state whether or not information system security requires more attention within their institution (with potential answers simply being “yes” or “no.”) Respondents clearly revealed that further attention is required, as the overwhelming majority and 83 per cent chose ‘yes’ on their surveys.

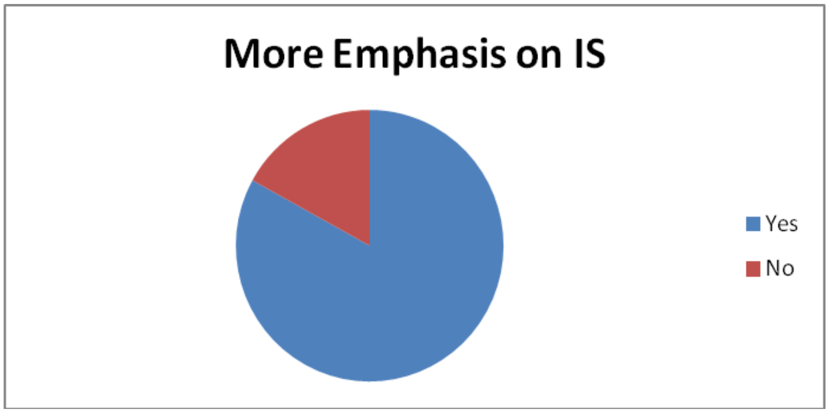


Figure 5.10: Support for additional attention given to IS at the organisational level

Only 22 per cent of respondents provided a follow-up response, listing a reason they feel more attention is needed; these responses were mostly variations of assertions that the potential for improvement had not been achieved while an improper amount of resources and dedication had been given to the area. The following item, question twenty-one, asked respondents if they felt that further attention should be given to information system security within their particular sector (as opposed to the institution). Here, a comparable (although lesser) amount of employees stated that further attention should be given to their specific sector, as 72 per cent of respondents selected ‘yes.’ More respondents chose to list reasons for this response (compared to respondents choosing to list reasons security across the institution required more attention), as 36 per cent listed some reason; many of the reasons listed here were also related to unreached potential and inadequate resource allocation, while some respondents also stated that known new threats to their particular sector had yet to be addressed.

Survey items twenty-two and twenty-three requested that respondents name improvements they feel should be made in the areas of managerial functions and compliance policy. The twenty-second item asked respondents to “name the improvements you feel should be made to managerial functions regarding information security.” The majority of responses were very general, and the study may have benefitted from a short note requesting that respondents be more specific; most participants simply stated that managers should put forth more effort, be more considerate and innovative, and (somehow) improve the information systems. Other respondents stated that managers should be required to undergo additional training to be sure they are aware of new threats (and ways to address them) as they become realised. Still others recommended that managers spend more time requesting their employees to share information, although the nature of this information was not specified (nor the level of access managers may already have to such information). Following item twenty-two, item twenty-three requested that respondents name the improvements that they “feel should be made to compliance policy regarding information security.” Here, the clear majority of respondents stated that compliance policies should undergo major updates while further being scheduled for routine updates in the future; it was further suggested that an underlying cause of low compliance is a low level of trust that compliance policies are as aware and considerate of details as employees. Meanwhile, others stated that compliance policies should be more ‘open’ in certain areas, allowing employees to use judgement in areas which are difficult to encompass and develop protocol for within the policies.

5.4.5 Questions 24-27: Training, Devotion of Efforts, and Adequacy of Technology

Questionnaire item twenty-four asked respondents their feelings regarding training; specifically, they were asked if they “feel employees should be required to undergo additional training regarding information system security,” with the ability to select either ‘yes’ or ‘no.’ The majority and 69 per cent of employees selected ‘yes,’ effectively recommending such a change to take place in their institution. This result is unsurprising given the participants' responses to previous questions (see Figure 5.12).

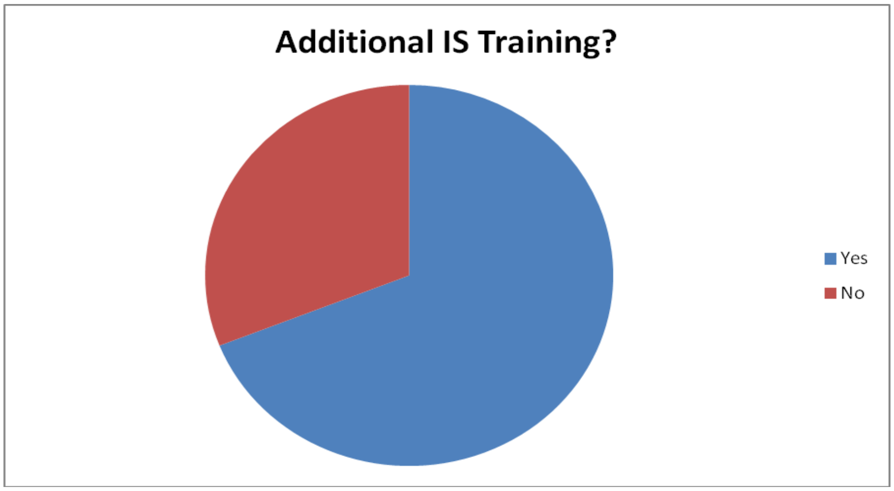


Figure 5.11: Should IS employees undergo additional training?

The following and twenty-fifth item asked respondents about their feelings regarding company representative devotion to information system security and threat awareness. In response, 82 per cent of respondents felt more devotion and effort should be placed in these areas, in agreement with the responses regarding managerial and employee attention to general security. Threat awareness was also a common theme mentioned in the responses regarding training and development, and thus appears to be an element needed in many areas for organisations to improve while reaching their potential.

Survey items twenty-six and twenty-seven requested that respondents provide their opinions regarding the adequacy of the security technology installed within their employing institution. Firstly, via item twenty-six, respondents were asked if they feel that the technology installed in the institution should be defined as 'adequate,' with the potential to simply confirm or refute by marking 'yes' or 'no.' Secondly, item twenty-seven then requested that respondents rate the level of adequacy more specifically, using a number to represent adequacy across the previously used scale of 1-10. The slight majority of respondents expressed feelings that the technology in their institution was not adequate, as 61 per cent chose ‘no’ as their response to item twenty-six. Figure 5.13 shows the unbalance of opinions regarding the perceived adequacy of technology.

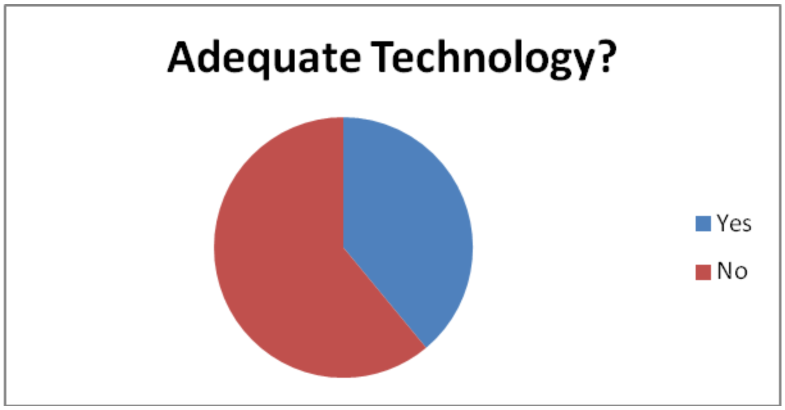


Figure 5.12: Is the IS technology adequate?

Next, it was revealed that the average rating for the adequacy of technology was 5.2 (SD=1.7, t=1.18, p=.120), suggesting that the technology is only accomplishing the bare minimum requirements for information system security (for most institutions and sectors). Considering that the majority of respondents stated that the technology was inadequate, the majority of institutions and sectors have a need to improve the technology itself; with this, it may be impossible for some information security measures to sufficiently address security threats and issues, as technology is the foundation of these developments.

Many institutions and sectors thereby require improvements on multiple levels: the technology itself, application, organisation, employee training and compliance, and actions to maintain sufficient awareness of growing or changing threats.

5.4.6 Questions 28-30: The Importance of Information Systems, Information System Security, and Information System Security Policy

The final three items of the survey questionnaire had identical designs, as respondents were simply asked to rate the importance (in relation to their institution) of a following list of three topics; these topics were information systems (item twenty-eight), information system security (item twenty-nine), and information system security policy (item thirty). The same scale of 1-10 was used for these final items. Addressing information systems, the respondents rated the importance of this area at 7.9 (on average; SD=1.6, t=18.13, p=0). This shows that the respondents feel that information systems are a central and vital element of the institutions, while showing that they are not considered a singularly all-important component. Meanwhile, information system security was given an average rating of 6.2 (SD=1.8, t=6.67, p=0). This number was expected to be lower than the statistic generated for information systems in general, despite the theoretical importance, but proved to be even lower than expected. This low rating is likely an underlying cause of the lack of adequacy, development, training, attention, and all other areas considered; naturally, if an area is not considered to be critical or even significantly important, it will likely be given a proportional prioritisation within an organisation. Because of this fact, increased prioritisation and the needed courses of actions suggested by the previous responses may not be possible without significantly altered perceptions in this area. Awareness regarding the importance of effective and improved security may thereby be a key issue, while the questionnaire could have benefitted from items elaborating on this topic.

The average rating for information system security policy was 5.3 (SD=1.4, t=2.14, p=.017). Despite the high number of responses supporting the additional actions and reform measures addressing policy and compliance in the previously discussed items, information system security policy was given an especially low importance rating when respondents considered the whole of their institution. Similar to the analysis of the previous item and response, this low level also implies that such opinions are underlying causes of a need to reform generated from low prioritisation, and thereby may require increased prioritisation amid the overall effort for improvement. Figure 5.15 shows the comparative perceived importance of these three areas.

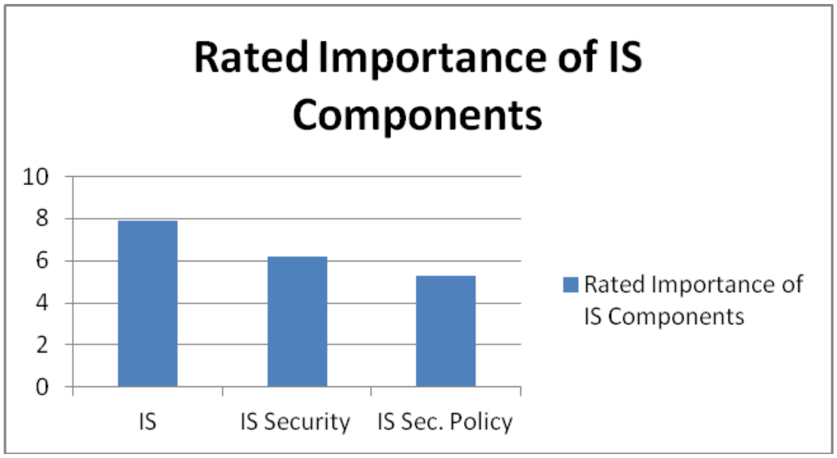


Figure 5.13: Significance ratings in IS (using scale of 10)

5.4.7 Supplemental Data: Organisations, Employee Quantities, and Size of IT/IS Departments (completed by researcher)

A brief section following the 30 items was completed by the researcher, in attempt to study and understand possible connections between responses and traits within the organisation. As the overall study was an analysis of occurrences across major institutions within the nation, the results were presented as totals (rather than by organisation), in accordance with best practices for random sampling with a specified category. Meanwhile, however, the researcher wished to record the organisation name, employee quantities, and department sizes to see if any further useful information could be generated while supplementing the main findings. (The turnover rates of each organisation were to also be researched and displayed by the researcher, but this was later deemed insufficiently relevant for analysis and discussion.)

As mentioned, the 10 institutions used for this study included the National Commercial Bank, the Arab National Bank, the Al-Rajhi Banking & Investment Corp., the Riyadh Bank, the Saudi American Bank, the Saudi British Bank, the Albilad Bank, the Saudi French Bank, the Saudi Hollandi Bank, and the Saudi Investment Bank. While the study aimed to collect a random sample across Saudi Arabia, it was not assumed that each institution was proportionally representative of some aspect of information security, and it was therefore deemed unnecessary for the number of respondents to be precisely equal across each organisation. By the time the researcher deemed data collection could cease with a statistically significant quantity gathered, and an appropriate amount of available time had been used, 12 individuals from the Riyad Bank, 11 from Al-Rajhi, 12 from National Commercial Bank, 11 from Arab National Bank, 10 from Saudi American Bank, 11 from Saudi British Bank, 8 from Albilad Bank, 9 from Saudi French Bank, 8 from Saudi Hollandi Bank, and 8 from Saudi Investment Bank provided responses for the questionnaire. This information could be used, perhaps using additional participants and further expansion, to conduct a comparative analysis of security capacity and demands across the organisations. Meanwhile, as mentioned, this information was considered only to supplement the main findings regarding occurrences across the nation; moreover, considering this information provided the researcher with the potential to point out organisations which were (comparatively) grossly unrepresentative of what were found to otherwise be usual trends. No institution was deemed to be grossly unrepresentative in such a manner, as participants across the organisations offered similar responses, supporting the existence of similar trends across the nation reported in literature. The only major difference occurring which stood out was a difference in technologies within the larger organisations (National Commercial Bank, Arab National Bank, Al-Rajhi Bank, and Riyad Bank), as members of these organisations showed a level an average level of satisfaction with technology generally on an order of two points higher than members of other organisations. This is likely due to increased purchases within these institutions, resulting from the higher revenue, greater power, and an overall greater capacity for technological improvements.

The number of employees in the observed organisations range from hundreds to thousands, although all institutions have a substantial clientele base within the nation. There did not appear to be any trends stemming from the number of employees, aside from the tendency for more employees within the larger organisations (and thus the increased satisfaction with technologies described in the previous paragraph). The size of the information technology and information security departments also ranged considerably, but here too the only relationship with notable potential is the relationship between size, potential, and technology. Considering these observations together, it appears that the more powerful Saudi institutions have a slight albeit observable advantage over other organisations. However in agreement with the literature, organisations generally face similar challenges in information systems security (Muhaya, 2010).

5.4.8 Basic Implications of Results in Relation to Literature

Although the discussion chapter is to serve as the primary relation between research results and literature, the basic implications of the results in this way provides a valuable supplement to the presented results and initial analysis. Althaneer and Nelson (2009) and Muhaya (2010) provided evidence that technological demands remained across the private and public sectors, despite plans for improvements (and actual improvements). Essentially, an overall solution was found to elude the country, while existing aspects of IS were deemed incomplete (Abu-Musa, 2010; Muhaya, 2010). The questionnaire results support this finding, although employees appeared to be more optimistic of their situation, and tended to have more confidence in IS than authors cited in the literature provided.

Incomplete security solutions have been found to be (comparably) as much of a problem as ineffective security solutions in Saudi Arabia. Meanwhile, security threats and attacks have found loopholes in systems comparably as often as they find a way through active security measures in place within certain systems (Bellamy, Perri, and Raab, 2005; Stamp, 2006). While this literature has asserted that the country has many examples of incomplete security measures within information systems, solutions, the questionnaire results show that the prominent bank organisations are mostly only faced with the problem of only having a “bare minimum” required to defend against threats. Although the questionnaire results did not investigate the completeness (and thereby potential incompleteness) of security systems and policies (i.e. disaster recovery), the interviews allowed more room for these less commonly considered areas to be explored. Considering the most fundamental results generated from the questionnaire, despite the resources and satisfaction within the successful institutions, the optimisation of IS security was nonetheless in need of improvements in the areas emphasised in literature.

5.5 Interview Results and Analyses

A total of 16 individuals were interviewed for this study; the researcher found the appropriate time to interview six individuals in addition to the minimum 10 proposed. Also as proposed, a semi-structured interview was developed and administered to the participants, allowing the researcher to address strategically determined ideals while reserving the freedom to pursue topics however deemed beneficial. While the same 10 questions were used as a template for all interviews, follow-up questions accompanied some of these questions, which differed across the interviews and were dependent on the nature of the subject’s response. The template questions used are listed below (see Appendices for completed transcripts, and see the following paragraphs for details regarding the responses).

Question 1: “*What do you feel is the biggest concern for information system security in Saudi Arabia*?”

Question 2: “*What do you feel is the biggest concern for information system security in your organisation, and do you see variations in concerns between departments?*”

Question 3: “*How do you think concerns can be addressed within the nation, and do you feel your organisation could address the concerns differently*?”

Question 4: “*Do you feel that employees and managers need to improve their levels of compliance, and if so, do you see greater compliance in either employees or managers?*”

Question 5: “*Does it appear that major reforms are needed within any policies concerned with information security threats?”*

Question 6: “*Are ethics an issue in managers and employees, and if so, what can be done?*”

Question 7: “*Should there be a greater strive to improve technology within the organisation, and assuming this is always desired, what seems to be the best course of action?*”

Question 8: “*If resources and time were no object, what changes would be most viable and effective?*”

Question 9: “*How do you feel that security-related training should be approached in the future?*”

Question 10: “*Are there any other changes you feel are required to minimise threats to information systems?”*

As anonymity was promised to all participants, as well as having a role in the ethical guidelines of this study (confidentiality and the potential risk that truly honest responses regarding practices is not well received), the names of interviewees are not listed. The following interview responses are organised in accordance to the observations and occurrences across the range of institutions. Responses are written using the interview responses, but are not verbatim, due to the differences in context between question responses and presentation. Verbatim (to the best of the researcher’s ability) responses are provided in the Appendices. Deviations (sub-questions) from the semi-structured interview are included in the following collection of observations, and are listed explicitly in the Appendices. The responses to the questions are analytical in nature, while an additional analytical section follows the observations from each institution; this is further related to the context of some of the literature, further supplementing the analysis and providing a precursor for the discussion chapter. Employees were informed that their responses would be presented in this manner, and anonymously, under the confidentiality agreement.

The following sections are categorised according to the areas where the bank management provided the most comparable or contrastable responses to the interview questions: security concerns, compliance and policy issues (including impact and potential reforms), and overall progressive development.

5.5.1 Security Concerns

At Riyad Bank, one of the most noticeable concerns experienced in this institution are viruses and internet security. Their biggest concern overall is hacking, because breaching the system can cause a great amount of damage. The potential for private technology to exceed internal technology is the most relevant concern. The biggest nation-wide concern is the growth and use, or misuse, of technology. Mobile technology is a particular concern, and is known to be a threat to bank security in Saudi Arabia. The bank feels very secure compared to the rest of the nation, but the organisation has experienced the most problems with firewall breaches and acquiring viruses. There are problems on networks more often than projected, and this is evident across all departments. The biggest concern for information system security is always protecting the network, and at this point in time, the most vulnerable technology is the firewall and security software. Employees hope that both improvements in available software take place at a rate faster than those would wish to break into the network can develop hacking methods, and that we continue to have access to defence technology within a fair amount of time once it becomes available. There is not much that can be done to address concerns in the nation, organisations can only attempt to access security technology through their own investments.

Al-Rajhi Bank managers expressed similar concerns. Their biggest IS concern is the possibility for threats from commercially available technology. It is assumed that people have equal or even greater access to technology that is capable of breaching security, and if it were capable of doing so undetected, there would already be a serious problem. Another concern is the rates of development; development continues while threats develop at a rate more comparable to developed nations, but internal technology is slightly behind. The biggest concern within the organisation is the availability and use of software. Ensuring that the best software is found, updated to address new threats, and otherwise used properly seems to be the greatest concern within the organisation. Maintaining and improving the software is also important, while threats can develop outside the organisation, unknown to the information security specialists. This is a concern to all departments. The nation itself is considered to be more concerned with the economy, finance, and development. There is concern for banks, but in terms of development rather than information security.

The Saudi French Bank, similar to the two previous banks, had strong concerns in technology. Their biggest IS concern in this organisation is keeping up with the technology and practices, which continue to change at fast rates. Firewalls and SSL have the most security-related issues here. These issues generally affect the company equally. There does not seem like there is anything that could be done on a national level, but people here could generally try to improve standards and practices for security. This applies to the technology as much as strategic development. Many employees need better plans for how to react to certain threats, because no planning in these areas leaves them especially vulnerable.

The Arab National Bank emphasised language more than any other bank. Their biggest security concern is the developed technology outside of the country, which the company has a hard time ‘keeping up with,’ and then using with the employees and customers. This is mostly in terms of software, as it is easier to ensure that the company has some of the best hardware available. Software and the English technology is undoubtedly a concern in the organisation, and the acts of convincing those with greater power that improvements are needed is difficult. This is less of a problem for security or online banking, but is a concern nonetheless. There is little that can be done on a national level, aside from national improvements. The Saudi British Bank also considered language amid technology. Major concerns include the availability of software and materials that can be approached with the language barriers. Another concern is the lack of concern itself, it seems, because some people don’t seem to realise the potential of existing threats. Yet another concern is developing security for an information system that assists such a wide range of customers with a wide range of services. The IS system is complex in itself, and building security that is considered both effective and versatile is challenging to the company. IS concerns cannot really be addressed within the nation, at least not directly. The best thing that can happen on a nation-wide level is economic improvement, but even this would affect the organisations differently. The organisation’s actions being different from the rate of the development of the nation is the only real way to gain a competitive advantage, and this organisation has the benefit of being one of the more successful companies of its kind. Beyond that there is no planned way of acting differently to get ahead with concerns.

According to the Saudi American Bank, Saudi Arabia has to worry about technology developing at different rates, and there are a lot of travellers in the country, and technology capable of breaching security can be brought in rather easily. Currently, most actions that are capable of violating information security can be detected, but improving technology (especially some of the mobile technology) seems to have potential for hacking without the same kind of detection, so it is a concern. There are no real differences in security concerns between departments. The biggest concern at the present is meeting customer concerns with technology which can be secured. The concerns for the organisation are the same mentioned for Saudi Arabia. The threat of improving private technology threatens this organisation as well as others. The organisation can attempt to invest in improvements, or even pursue research and development; although there is more incentive for the nation to do this, it is generally not deemed practical by the company.

Meanwhile, the National Commercial Bank seemed to acknowledge concerns similar to Sauid American Bank while being more apathetic. Their biggest IS concern is a combination of technological development outside of institutions needing security, and a lack of awareness of general technology within the institutions. Another concern is the size of the data and funds stored, compared to the nature of upgrades and organisation. The bank attempts to address departments as needed, so there does not appear to be critical variations between departments. The network and some technological components are not always improved at the same rate of the bank's development, which can produce changes to threats. There is little that can be done on a national level, so the organisation could address concerns differently by applying change how it is needed and as changes become available. The Saudi Hollandi Bank had a similar level of focus and apathy; according to them, technology, practices, and planning are the biggest IS concerns. The organisation has had problems with dedicating the time and resources suggested from threat implications, and may be more vulnerable than is realised. The fact that many employees simply are not aware of the threat potential in certain areas is something that should be considered. There does not seem to be much that people can do in the national in terms of strategy, each organisation should simply invest in improvements as they become available. No superior strategy has been realised.

Albilad Bank best described the motivational impacts of ranging concerns with their responses. Acquiring and improving defensive software at a rate which is ahead of the potential for threats seems to be their main concern, both inside the company and protecting the services offered to clients. The same basic threat to the nation is observable in the organisation, but the organisation faces more of a struggle with upgrading technology as needed, because that requires private funding. The government could help itself improve security for information systems in the public sector, but that would not have much of an impact on concerns within financial institutions. This organisation could simply choose to improve security to the highest level, investing considerable money in the process, but that would not cater to the competitive advantage. The competitive advantage takes the greatest priority within most decisions regarding those kinds of investments.

The Saudi Investment Bank simply supported basic assertions. They are concerned that competition and demand are major issues, because security must always accompany changes. Growing technology without the security to match is basically ‘asking for trouble.’ Firewall problems, or ‘loopholes,’ are another concern, as are high levels of encryption. Those two areas are common topics in recent concerns. Experts could cooperate in attempt to improve information security as a field, but it does not seem like there will be enough of an incentive for that any time soon, either within the nation or within the organisation.

5.5.2 Compliance, Policies, and Potential Reform

The Riyad Bank had a great deal to report regarding ethics, compliance, policy, and reform, but (like many banks) was not convinced that there was a genuine need for major reforms in these areas. According to their perspective, employee and managerial compliance are the biggest correctable problems that can be seen, but unfortunately concern is also low, so little has been done. The best way to make improvements is assumed to be through awareness and change management processes. Managers have seemed to be more compliant overall in recent years, but instances of non-compliance have more commonly been greater deviations from what is expected. The nature of management positions involves greater power, so non-compliance is more likely to be more serious in nature. Non-management or ‘normal’ employees are more commonly non-compliant, but these instances are also more likely less serious. Undoubtedly, compliance has been and continues to be an issue of concern and focus. Managers and employees alike should make sure they are following procedures, but when a manager chooses to be non-compliant in areas related to information systems and security, the results have a greater tendency to be more serious. Managers generally feel that they are ‘above’ policies and obligation, while employees seem to think they have a greater chance of avoiding detection if they choose to take shortcuts. Reforms are needed in many areas, but the level of reform needed is normal and changes are always needed; no ‘major’ reforms appear to be needed. Change and change management must be emphasised so the organisation can change as needed, and as the company has been successful in security and operation. Ethics is always an issue, and in that sense, there is little that can be done in the organisation. Greater incentives and greater consequences can help to insure compliance and ethics remain in all parts of information, security, and operation, but it seems as if it will always still be an issue. Ethics are of course responsible for many non-compliant actions, as well as general actions at work, but it does not seem like much more can be done. Information systems and security should have the greatest strive to upgrade technology virtually wherever possible in the organisation. There does not seem to be any real strategy to this, aside from gaining the profits required while ensuring that profits dedicated to technological improvement do not negatively affect other areas. Without the strive, the threats from those outside that do strive for technology would be incredibly great, thereby putting the organisation at great risk.

Perspectives of compliance and potential reform are similarly apathetic at Al-Rahji Bank, while these areas would prove to generate the most common ground out of the categories in the interviews. According to this institution, compliance is somewhat of an issue, but not a major one. Compliance doesn’t usually lead to improved threat. Managers seem to feel ‘above the law,’ but employees feel that there is less risk for the policies that apply to them. Both managers and employees should be advised regarding improved compliance, although the importance of this has not changed much over the past years. The company might benefit from policies requiring changes. Ethics are always an issue, and the only feasible changes which can be conducted involve stricter policies and consequences. New changes are assumed to bring new opportunities for ethics to become an issue elsewhere. Ethics are something that managers should be more mindful of, observing and ensuring proper employee conduct. Being selective when choosing authorities, and being mindful of their actions (and allowances) as they grow with the company, appears to be a potential solution. Similarly, the Saudi American Bank feels compliance is not considered perfect, but it is not a major issue either; compliance could always be better in a conceptual sense, but it is generally not perceived to be ‘a problem.’ Managers are usually more compliant (compared to employees). Meanwhile, there could be stricter requirements to improve technology, but there are also times where this policy may seem to ‘get in the way’ and need discretion anyhow. Ethics are an issue, but they are not considered to be the cause of any major failures or problems. Ethical issues in managers are more serious on a higher level, while ethical issues in employees are more serious on the lower levels; both result in problems, and though ethics has seemed to play a role in some problems, other aspects of the company are prioritised in development. Most of them are actually not related to security, and are part of normal business development, but security is considered as the company continues to improve technology and electronic services. For example, according to one interview, “The biggest nation-wide concern is the growth and use, or misuse, of technology. Mobile technology is a particular concern, and is known to be a threat to bank security in Saudi Arabia.”

The Arab National Bank had the common apathy regarding compliance and ethics, but saw more potential in some areas of reform. At this location, compliance is always a concern, but is always considered, so no major improvements seem to be needed. A neglect of compliance or reviews would be bad, though. Employees seem to be more compliant, because they are more likely to lose their jobs and remain unemployed for such actions. Both managers and employees should improve in this area, but managers should strive for flawless compliance. Threats become part of awareness issues and discussion when they become apparent, and actions are taken if it is determined that this is needed. Policies regarding training and software or network upgrades could be more demanding, but especially as discretion would be required, the changes would not really be ‘major.’ Ethics could improve information security defences as well as any other areas, but compliance and ethics generally do not directly affect the defence itself.

According to the National Commercial Bank, managers have set examples for employees here in most relevant areas, including compliance with policies. In information security-related positions compliance is generally not a problem, neither within manager-based positions or normal employee positions. Major reforms could better protect against threats, but policies alone do not need ‘major’ changes at this time. Policies requiring updates and development, including technological development, could better ensure that the organisation’s security develops on a level more comparable with the development of the technology itself, but it then would likely not be able to make decisions or have discretion. Discretion seems to be the best approach at this point, despite the possible issues with motivation and freedom stemming from it. Ethics are always an issue. They do not seem to be responsible for any increased threat or critical issues here, however. The only realistic approach that can bet taken to address ethical problems is to examine each instance of ethical violation on a case by case basis. In information security, this seems to be less of a problem than within other areas of the bank.

The Saudi British Bank continued with the trends of similar opinions regarding ethics and compliance. Compliance is not much of a concern within the company in past years, but employees have had more violations. There are more employees than managers of course, but they also seem to be more prone to violating security and other protocol. Compliance does not seem to be an unusual concern anyway, and it seems to be comparable across the company as well as in comparison to other companies. It has been hard to create policies that are both detailed and not in need of discretion as variables change. Security and the nature of the system could be reformed for the clear benefit, such as through network restructuring, advanced software use, and other ways, but there does not seem to be a good way to improve security through major policy reform. Policies regarding training, researching and upgrading technology, and improving the nature of organisation (such as through increased dedication and staff) could reduce threats, but unfortunately there does not seem to be a definite path to ‘major’ improvements with any practical investment. Ethics, like compliance, are not a major concern with the company. The company has no major plans for change in this area. Ethical issues seem to be an underlying cause with some concerns, such as compliance and basic employee conduct, but it is one of the least prioritised areas within the company’s plans for development. The company could stand to invest a little more funding and effort into improving technology, especially in terms of researching the market for possible improvements, but the current processes seem to be good enough to create a considerable competitive advantage.

Albilad Bank management had some of the strongest opinions regarding compliance and effective reform. For example, according to one interview, “The government could help itself improve security for information systems in the public sector, but that would not have much of an impact on concerns within financial institutions. This organisation could simply choose to improve security to the highest level, investing considerable money in the process, but that would not cater to the competitive advantage. The competitive advantage takes the greatest priority within most decisions regarding those kinds of investments.” There, employee non-compliance is handled by managers on a regular basis, but less action is taken for managers in similar situations. Some improvement is needed in both areas, but it is hard to measure the extent or develop a strategy to achieve perfect compliance. The systems and security could benefit from major reform, but the policies themselves cannot have the discretion required for technological improvements as technology changes. The only developments in policy which would have the greatest influence would be improvements for crisis plans or disaster recovery, which is given little consideration in existing policy. Ethics do not seem to be much of an issue outside of compliance. There should be a major strive to improve technology wherever possible, but it already exists. The emphasis on competitive advantage through services will always remain, and technological improvements outside of this area do not seem to be practical. If resources were no object, the continuing optimisation of technology would be effective. Expanding the quantity of staff would also be effective.

At the Saudi Hollandi Bank, compliance always needs improvement because it is almost always less than perfect, especially over a given time. There should be greater incentives for developing security and greater consequences for breaching policy. Changes to policy are recommended in terms of backup and recovery planning, but aside from that no ‘major’ reforms seem to be needed. Ethics are something that we value, but we mostly emphasise compliance with policy and procedure. Ethics could be improved with greater incentives, or consequences, but the emphasis will remain in other areas. At the Saudi French Bank, compliance will always be a minor issue with any policy, so it will always be a concern but will not likely have any increased emphasis. There are no ‘major’ reforms that are needed for policy, but slight improvements could be made in most departments. For example, there is little protocol for emergency plans, if something were to go wrong with the network or services, much time would likely be lost since there are none of these plans. Ethics are an issue, and policies and new strategies often try to improve ethics in many ways. It is not considered a serious issue, even though ethics could be a lot higher; it takes major problems in ethics for ethics to gain great attention. Similarly, at the Saudi Hollandi Bank, employees and managers both need to improve levels of compliance do, technically, since it is less than perfect. Compliance is rarely a serious concern. Some reforms for improvement and protocol for emergency procedures could help, but no major reforms appear necessary in routine operations. Ethics, like compliance, are rarely a serious issue. Employees have different ideas about what it means to be ethical, and the company is only demanding in certain areas.

5.5.3 Progressive Development

Most banks emphasised technology in their responses, but there was more uniqueness in the approaches or realistic justifications of many areas of progressive development. Training was also commonly emphasised. According to the Arab National Bank, There is already a strong desire to improve technology wherever possible. Network connections and the main software used could be improved, and more employees could be used to improve the network for security effectiveness. General information system effectiveness could be improved by hiring a team of more qualified (in technology) expert professionals to choose technology best-fit for the organisation and remodelling it accordingly. Firewalls, anti-virus software, and better encryptions would be the most effective security upgrades, but decent versions of this technology exist already. According to Riyad Bank, improving hardware and software to top-of-the-line products, then giving the network the best design and security measurable known, would be ideal changes. Replacing all of the current technology, and then ensuring it is properly supervised, maintained, and upgraded by employees would also be ideal. Meanwhile, training sessions should be more involved and given more often, with more consideration given to available technological improvements, outside of the nation as well as within it. Improved organisation and leadership may help to minimise threats, but no paths to such major improvements have been successfully implemented in the past nor appear to be realistically possible now. Aside from this, employees do not feel there to be any real critical threats at the present time.

The desire for technology is usually present at the Saudi American Bank, but changes in research and strategy for acquisition could be improved. The company could benefit from charging some employees with researching security elements more vigorously, and this is something that is discussed from time to time. There is usually an extremely competitive strive to improve technology in terms of services to customers, and changes to security technology change in response to this as well as to changes to internal technology. The strive to improve service-related to technology will always be the greatest, because it is competitive. If resources and time were no object, the changes that would be most effective would be rebuilding the internal network for internal processes and services with the best technology available. There is some technology that could be changed to help security a little bit, but most changes that would be effective in that situation are related to information systems (alone) and general business. Training should be more technical in nature, having more emphasis on the best tools and best practices. Literature could also have more of a part in training development.

Al-Rajhi Bank asserted that security should continue to seek the best technology available, so long as the money is invested in truly beneficial improvements. Elsewhere in the organisation, this was more debatable. The best perceived course of action is to simply increase profits while researching the technology on the market. The nation in general has access to effective technology, but it is slightly different than the technology available in developed nations; there is no known practical path to improving technology so that is identical. If resources and time were no object, the bank’s network infrastructure would be remodelled using the best technology available. An expansion of facilities and the placement of new facilities in new locations could increase profits well enough to have an investment for the future, and this could then be used to address the areas we have discussed. Training should be more in-depth, and carried out more often, so that employees are aware of what is available, in terms of both threats and defences. It should be more technical in nature, so that employees are more aware of the tools and features available to them.

At the Arab National Commercial Bank, the existing level of striving for technology is assumed appropriate and that it should simply continue. The current course of action seems effective, despite the issues in technology described in existing articles and publications, the company has not experienced major breaches or threats that would jeopardise the company’s integrity in any major way. Security breaches a concern but not on a level near crises. The most viable change perceived would be to ensure employees have a higher level of education and training in the future. Additional paid employees providing additional labour and ideas would certainly benefit the organisation if money and wages were no object, but this is not ‘viable’ under normal circumstances (although it is assumed to be effective). Training should be more considerate of technical aspects and technological potential, it seems to be too general. Training for managers is assumed to be an area that should improve, while employees have more resources and could ask managers for assistance at any time. The requirements for hiring employees could be improved, though, and help to minimise these issues. Training should be conducted formally more often, most training is not in-depth or detailed on the level that it should be. Both resources and time have been challenging (as training in this way removes employees from work), so this would need to be considered in the future. Restricting tools which are generally used for breaching security may be more helpful.

At the Saudi British Bank, the best course of action appears to be to approach technology mindful of potential, without making unnecessary upgrades (upgrading before a new line of products comes onto the market). Here, educating employees, improving the network structure, and improving software would be effective actions. The security system could be best improved using new firewalls, and plans should be created for things like disaster recovery. Training should be revised completely, many parts of it have just been put together without the effort required, often times with important information not realised until later. It should place more emphasis on the concerned realised by experts, rather than considering mostly corporate concerns. Lastly, firewall protection should have more effort devoted to it, to make sure there are no loopholes and that it is updated as needed. A general investment of human and material resources in security would be an ideal first start, allowing the other areas discussed to be more possible. Albilad Bank had less to state in these areas, claiming that training needs to be improved all around, specifically in terms of technical applications and upgrades, but it could use improvement in just about every area. Some employee should be charged with the task of improved continual research in terms of threats, developing defences, and developed best practices.

The opinions of the other banks reveal a similar emphasis on training, technology, and business development. At the Saudi French Bank, managers felt that the organisation should acquire the best technology, and in this sense there is a ‘strive,’ but the lack of progress is due to resources, strategy, policy, etc. Recommended actions include improvements in firewalls and protection software, while the networks are sufficient and the service technology has evolved at a decent rate. Restructuring technology and organisation seem to have the most potential, aside from expanding. It should be more thorough, especially in terms of development beyond systems and procedures in place. Meanwhile, at the Saudi Hollandi Bank, the need to alter the existing strive for improved technology is debated. A new network with new services, thereby improving competitive advantage and potential for future development, is deemed the most desirable improvement (in the event sufficient resources are readily available). Training should be carefully planned, and not just ‘dealt with,’ as the present mentality seems to be. A greater emphasis on security as a field might lead to new improvements, but outside of that, it seems to already be a developing topic of emphasis. Lastly, at the Saudi Investment Bank, the strive for greater technology already exists, and the company implies it cannot afford to divert efforts any farther. Expansion could help quite a bit, and so could remodelling all information technology and networks; they would both be practical for their own reasons. Here, training should become more of an educational process and less of a quick attempt to change bare-minimum processes as they are realised. It is assumed that there will always be threats, and only the most innovative people can conceive defences to threats that have yet to exist. This chapter has examined shared themes, specific interview responses, and implications; the following section begins to relate this back to literature, while the following chapter provides further thematic analysis, relation to literature, and recommendations. Chapter 7 provides further analysis and relation to stakeholders, while Chapter 8 then provides still further thematic analysis and relation to literature.

5.5.11 Summary of Interviews, Immediate Implications, and Initial Relations to Literature

The interviews revealed perspective and trends partially in agreement with literature and the questionnaires. The interviews did not reflect opinions as strong as those in the questionnaires regarding the need for improvement, although a considerable amount of employees did mention issues listed in the literature, such as firewall and SSL complications. Responses regarding ethics and compliance were also substantially less critical than ratings provided in questionnaires. Many of the interview respondents seemed to feel that the companies were developing at a decent rate, and information security was not a real concern. In spite of the findings described in the literature (i.e. Saudi Gazette, 2007 Abu-Musa, 2009 and Muhaya, 2010), company representatives may feel that competitive advantage should remain an area of focus, and significant investments in information security need only occur if the potential threats are even more serious than described by expert analysts.

As shown in the previous discussion relating questionnaire results to literature, despite the developmental potential of these successful institutions (coupled with employee confidence), results nonetheless revealed needs for improvement in alignment with literature. The interview results differed from questionnaire results in that there was more confidence expressed in the interviews. Although the driving factors behind this are somewhat unknown (potentially being due to the varying nature of the positions, the impersonal nature of questionnaire participation facilitating criticism, or personal obligations for interview participants to express optimism), interview results nonetheless showed a need for improvement in other areas. Abu-Musa (2010), among others noted in the questionnaire section, reported demands for improvement amid incomplete or ineffective security measures in a range of systems. Abu-Musa (2010) further reported that the majority of Saudi organisations have no disaster recovery or emergency plans. This was noted in multiple interviews, and no satisfaction of these elements was mentioned. Findings here also imply that organisations have been approaching IS in such a way so as to achieve the “bare minimum” defence to known threats, with little emphasis on pre-emptive optimisation or development. Wells (2007) noted frequent complications in Saudi firewalls, also confirmed in the interviews.

5.6 Chapter Summary and Closing Remarks

The findings generally support the theoretical framework, and they show evidence of a demand for change and manifestations of the vulnerabilities from the Saudi research. Meanwhile, there was no evidence of the newer strategies, best practices, or technologies implemented in the organizations. The results confirmed the findings in literature, although the interview responses were less critical while implying there is a lesser need for improving security. Even the more prominent organisations may feel their emphasis on improving their competitive traits should take the highest priority, while security measures and planned development is far from ambitious. The following chapter moves beyond the presentation and analyses of these results, relating the findings to previous mentioned and additional secondary literature, across a more in depth discussion.

Chapter 6: Recommendations

6.1 Introduction

The results and analysis reveals a clear need for change, the presence of restricting factors, and unacceptable levels of apathy and ignorance; these are thus the key issues in recommendations for improvement and analysis. The review of literature demonstrated numerous potential influences that are affecting portions (if not the whole) of the country, and there may be resistance to change within companies as well. Considering this, the organisations, managers, and perhaps the government, are in need of recommendations for progressive development most conducive to security and operational objectives. However, any recommendations simply considerate of these goals are not likely to be effective, as the challenges and restrictions may halt these attempts entirely. Effective recommendations must consider resistance to change, the range of factors mentioned in the results, and the general theoretical needs, objectives, and challenges outlined in literature. This chapter provides recommendations, suggestions, and a framework for improved information security policy and governance.

6.2 Fundamental Areas of Recommendation

As mentioned, the initial literature review presented provided a solid demand and array of areas of concern in the Saudi context, while the hypotheses reflected (and would be generally proven) the relation of these recommendations to the organisational levels. However, the context, particularly the nature of demands and restrictions regarding improvement at this level, was unknown prior to this study; as such, the fundamental recommendations could only serve as guidelines, with the results being required to develop the finer points of policy and framework, governance, etc.

The elements of the hypotheses proven correct form the foundation of the majority of the recommendations outlined throughout this chapter. The ten areas considered the primary threats to Saudi Arabian financial institutions, threats from external technologies, an array of demands for developing policies and procedures (although this reality proved to be less demanding than initially anticipated, compliance, personal ethics, institutional factors and employee willingness, training and access to resources, and organisational characteristics; with this, it is recommended that optimised IS policies and governance make improvements in each of these areas.

The primary threats to IS in Saudi Arabia in the general context are known to involve the threats from external technology developing at a rate comparable or greater than the development of security technologies, demanding that IS policies evolve to better compete against the resultant threats. As this has not happened, it seems that the problem could lie in either the demands of investing in this development, the prioritisation compared to developments in other areas, a lack of awareness, or a lack of technological potential; the research has shown that the true reason is a combination of each of these areas, and thus each area should be addressed in an optimised reformation effort. Meanwhile, organisations must address the known challenges in organisation and maintaining a structure which facilitates the implementation of best practices, using discretion to note which practices apply to the circumstances of the organisation and its variables.

Another vital area which demands attention is the lack of disaster recovery and emergency management. This should be a required element of all Saudi organisations, especially financial organisations, and no IS policy should be considered complete without this. Additionally, organisations could be penalised by the government for not having an effective solution to address finances and other factors which affect customers in the event of a crisis, while the government is recommended to improve its policies to include requirements and reprimands for incomplete IS policies relevant to consumer property. Giving further consideration to the government, although it has established a dynamic system of laws and punishments for breaching protected databases, a re-examination of policies and increased deterrence would naturally serve to reduce the risk of violation. Additional developments, such as required logging or tracking procedures, could also assist security, although additional studies are recommended in these areas prior to strategic development.

Policies and procedures related to employees demand a combination of active and passive security measures, while the observed limited effectiveness and apathy regarding many employee policies can be perceived as both a small concern for the negative impacts of these policies and a resistance to change in any attempts for improvements from this angle. It is clear that employees view the finer points of compliance with apathy, that work ethic is moderate at best, and motivation to do more than what is necessary is minimal. Meanwhile, the value of innovation in information security is also low to nearly the point of counter-productiveness, as the organisations observed were found to be lost in a mentality where the absence of crises has served as a false sense of security; knowingly out-dated security systems were generally accepted, with improvements bringing them to basic standards evolved in recent years were discussed almost as if they were a luxury rather than a basic requirement. This would be understandable if the organisations participating were small businesses, but both the prestige and success of financial institutions suggest that these organisations should not adopt such attitudes. The resources for development are available, they are just not prioritised, and the most important change to policies should involve a redistribution of invested funds (or a greater percentage of profit invested in resources) for continually upgrading information security systems. Additional foundational elements of policies related to management employees that should be addressed are in compliance. There should be some developments which integrate both incentives and reprimand for compliance and ethics, serving to remove the apathy in these areas. This should apply to both managers and employees as managers are assumed to be a major cause of this apathy; managers required to implement or maintain the policies for incentive and reprimand should be subject to similar terms. Managers should also conduct individual studies of organisational factors influencing personal ethics, so that they have a better understanding of employee perspective of information security, and how to motivate employees to facilitate optimal security. Members of upper management should continue setting the groundwork for continuing improvement by assessing the most influential institutional factors and their relationship with managers and employees.

The next most significant foundational element of IS improvement is training. Training has the potential to improve the nature of existing conditions, awareness, and skill, or it can efficiently and effectively assist developmental initiatives, overhauled systems and technology, or restructured policies. Despite this, it was found to be rarely used as such a tool in the organisations observed, although a full perspective of the underlying causes here was not provided. Similar to the state of resources and developmental initiatives, this could be due to apathy, a lack of awareness, a lack of prioritisation, or a lack of desire to invest (or any combination). Thus, training should be prioritised in multiple ways, including time and funds invested, development and customisation, and assurance that all areas of concern are effective covered in training administered. Lower and upper management should respectively track the employees in demand of training and areas of operation which could benefit from the integration of a new training program.

The role of organisational traits in information security, such as the nature of managerial styles, development of and reaching company goals, resource allocations, and organisation of databases or processes should also be the subject of some type of routine analysis. The results of this analysis may or may not lead to areas of concern warranting restructuring managerial techniques or the formation of organisational goals, but there should be mechanisms available for operation should these concerns manifest in this manner.

This introduction of foundational elements recommended for improvements is not intended to be exhaustive; while they effectively serve as the basis of the majority of topics and processes proposed and discussed below, additional and indirectly related areas are also outlined and recommended.

6.3 Addressing Saudi Arabia's Developing Need for Security

The actions the observed Saudi financial institutions need to take to properly address the security risks and related concerns in IS policies are exemplary of common problems across the nation listed by literature, although the power of the financial institutions implies that they have a greater potential to address security concerns plaguing the country in their areas. In any case, the institutions can be exemplary to other sectors and organisations through their developments, while the literature reveals the similar nature (and thereby potential relevance of financial institution solutions) of the challenges. Considering this, the financial institutions can be pioneers in addressing Saudi Arabia’s compiling need for improved information security, ideally playing a role in ensuring that the developments of threats cannot so rapidly exceed the ‘counter development’ of solutions and security. The recommendations of literature should serve as guidelines to organisational development. These are sparse, as shown in Chapter 2, but provide a consensus and details adequate for developmental guidelines. Alnatheer and Nelson’s (2009) assessment of security culture and practices should be used in examining the nature of organisational culture and how conducive it is to information security, how flexible it is to development and change, the role of monitoring, how it facilitates communication, and how compliance and ethics are promoted. These authors’ warning that apathy towards ambition or major developments in IS management could ultimately affect the national economy is highly relevant to the sector, as the role of financial institutions in the economy is especially great (in addition to the power of the institutions for development and the example they may set). The Saudi government could play a further role in promoting these developments, for the sake of safeguarding the economy, although a joint effort promoting information security awareness or development could go a long way towards removing the apathy towards seemingly unnecessary technological developments or policy restructuring.

Alnatheer and Nelson (2009) also provided guidelines for establishing or improving prevention and recovery plans, elements of which were found to be minimal or non-existent in the present and other studies. As mentioned, these should be essential elements of information security, with the critical elements potentially affecting customer property mandated by law. Regarding direction in development, aside from the specific objectives of safeguarding against known potential threats, the authors recommended the prioritisation of three concepts: i) confidentiality of sensitive information (concerned with preventing disclosure of information to unauthorised users), ii) integrity (concerned with ensuring data cannot be modified without authorisations), and iii) availability (concerned with ensuring information must be available to authorised users when they require them) (Althaneer and Nelson, 2009). The findings of Muhaya (2010) and Abu-Musa (2010) determined that this focus was generally absent, and although the present study did not place a great emphasis on the concepts, it was determined that there was a general apathy towards any emphasis which aimed to achieve more than what is needed to maintain what is perceived in everyday operations; in the absense of complaint or breached integrity, the improvement of confidentiality and integrity should be a primary direction of future developments, while innovation in availability should be examined and considered alongside the relevant potential vulnerabilities.

The findings of the Saudi Gazette (2007) and Zurich (2008) also serve as guidelines to recommended improvements in the targeted institutions. The Saudi Gazette’s (2007) findings should be an emphasis of awareness initiatives in the companies as well as across the nation, and Zurich’s (2008) prioritisation of information security should be modelled in strategic developments and implementation.

The development of technology on local and global scales has been a primary factor in the increasing gap between information security and potential for threats, as both have caught information security programs ‘off guard’ with many potential threats either unseen, not fully understood, or not considered sufficient to warrant the restructuring of systems. Meanwhile, the rapid technological developments occurring in other nations such as the United States and United Kingdom have increasingly been integrated within the nation, or the connectivity (and thereby accessibility) in national networks has increased with globalisation and general network expansion. Many institutions may still have not come to terms with this reality, and even those that have must come to terms with the significance to information security. Mobile phones should be a key area of focus in awareness and improving security systems, and the rising number of mobile phone users, internet users, and the increasing capacity of mobile technology to be integrated with online technology should be at the forefront of information system education and development for years to come.

For example, each bank observed could inform employees of statements such as the mobile subscribers with cumulative annual growth rate (CAGR) of 58.6% (more than twice the world CAGR of 23.4%), with subscribers approaching 12 million as of October 2005 (over 50% penetration) (CITC, 2005). Internet users grew by over 430% in four years, amounting to CAGR of 44.4%, (vs. world growth rate of 27.4%); internet users are exceeding 2.5 million. Personal computers (PC) penetration has also grown 40% annually (vs. world PC growth rate of 9%) to around 16% penetration. Fixed mainland telephones are approaching 4 million lines (a tele-density of 17%). Internet international bandwidth capacity has increased by nearly 7 fold in 4 years to over 1800 Mbit per second" (CITC, 2005, p. 1); additionally, all managers should be required to attend periodic meetings where this type of information is presented on a three month basis, with subsequent local meetings informing information security staff of the implications of these facts.

Previous developments in Saudi Arabia provide guidelines for both desirable and undesirable developments in the future. For example, the described 2004 reforms of Telecom were ideal in that the technology was improved through a substantial overhaul of systems, but it was determined that little to no security developments were implemented alongside these changes.

This is exemplary of how development should not take place for policy, but is exemplary for hardware. Meanwhile, the 2005 development of the National Communications and IT Plan (NCITP) is a guideline for structure which should be continually modelled and related to important areas of information security. Also, in 2007, the United Nations (UN) outlined a plan which Saudi Arabia had considered for redesigning its ICT sector.

This was created with the intentions of improving the economy through the resultant increased competition, increased local and foreign investment, and the additional protection of consumer and stakeholder rights (United Nations, 2007). In 2003, Saudi Arabia’s government-operated telecommunications had been partially privatised, affecting the nature of the largest communication entity; this had also compounded the results of the Communications and Information Technology Commission’s (CITC) establishment in 2001. These areas had acquired the power to develop protocol for any aspect of information technology and information security in major Saudi Arabian communications, contributing to increased levels of financial and administrative independence. According to the United Nations (2007), “*the Government has taken a number of steps to liberalise the market, and create a positive regulatory framework to encourage investment and promote growth of the ICT market.”* (p. 5). As mentioned, this and other chains of events were unable to change the overall information security situation in Saudi Arabia.

6.4 Policy Recommendations Regarding Employees and Questionnaire Topics

The rated effectiveness of the company policies and procedures implies that changes should be made based on the opinions alone, both in terms of developing employee perspective and in terms of making changes to the nature of the policies. The average rating of policies being only

6.3 on a scale of 10, combined with the fact that the employees generally felt that all areas were sufficiently functional, implies that even the ‘effective’ policies do little more than safeguard against the most basic threats. The information security policies should be formally structured, printed in detail, provided to each employee, and routinely reviewed. The employees and managers should be polled on a routine basis regarding the perceived effectiveness and potential for change, and then managers should petition for changes to policy or relevant factors (i.e. software) based on this feedback. The prevalence of information security examination is also too low on average, with the overwhelming majority being less than routinely. This should be a routine examination; even if the examination is only brief, it should be thorough and occur at a three month minimum. As mentioned, the occasional nature of examination and testing may also play a role in the lack of action, or action considered ‘as needed’ being rare, as a lack of examination and testing may leave company authorities unaware while the systems remain vulnerable.

The average ratings of training in effect gives rise to the recommendations for major changes in these areas, with this also being along the lines of the non-routine occasional occurrence mentioned for examining policy. Training does not necessarily need to be lengthy when all areas relevant have been taught or outlined in detail, but brief training sessions should be scheduled on at least an annual basis to update the employees on changes to technology, policy, or threats; additional training need not be periodic, but should be sufficient to parallel the implementations of new elements in any area of IS.

The average ratings regarding compliance and ethics across the questionnaire sample agreed with the managerial sample regarding apathy, but these results were unique in that a larger number of employees provided perspective from their level. Naturally, developments in IS must be considerate of both employee and managerial perspective. Meanwhile, a difference between managerial and employee compliance was noted, with a similar difference noted in ethics; this implies that greater efforts must be made in motivating employees versus managers, but also implied that managers are vulnerable to the authority of their position. With this, some managers appear to feel that they create rules and norms which are actually above their authority, while they are effectively ‘above the law’ in terms of many aspects of policy. This must be avoided at all costs, as it reflects on the employees as well as the immediate implications for information security integrity, awareness, and development. Lower level managers should be examined by upper management on a routine basis, reviewing their efforts in information security alongside their performance reviews. Managers determined to be ignoring the developed policies should be subject to punishment. The primary reason suggested for managers not following policy generated a range of responses, but a common response was lack of organisation and seriousness in the organisation. This confirmed the implications from other items that many managers are prone to making their own rules which are a conflict of interest to information security. The other suggestions (lack of knowledge, experience, or incentive) should be investigated in each branch, and addressed through increased strictness, reprimands, or an adjustment to policy as needed.

Ignorance to policy must be addressed through awareness initiatives, although it may be difficult to gauge the required knowledge of changing policies without actually ‘quizzing’ the employees regarding policy. However, as ignorance to policy was reported to be a major cause of non-compliance, it must be addressed through more thorough awareness initiatives, training, or another method deemed effective by the organisation. Other responses included attempts to be efficient, attempts to operate more effectively, and general carelessness, and these should be monitored by a more aware upper management and dealt with.

Managers must also be provided with resources, time, authority, and incentive to address IS issues which may not be foreseen by upper management in developmental initiatives. The frequency management was reported to address issues in IS varied widely; only a small percentage stated that this frequency was either “fairly often” or “often.” Although many managers may have been involved in situations where they were capable of addressing the circumstances for an effective solution, there are almost certainly many instances where they were powerless to act while assuming the issues would be eventually noticed and addressed. This mentality cannot be allowed to exist, and the reviews and discussions related to improvements may very well be too infrequent to properly address the threats. Managers should be liable to report any potential threat to security, and be provided with further means to handle threats should the present themselves. For example, should a new virus be reported in the news months prior to the scheduled meeting and assessment, the manager should request to update or upgrade the existing firewalls and anti-viral programs. The manager should then either have a means of performing these actions solely, or should have access to someone who can perform this action immediately.

The comparative differences between employee and managerial compliance show that more managers are ‘excellent,’ ‘poor,’ or ‘good,’ with more employees being in the ‘average’ range (see reproduced figure below). In addition to managers feeling above the policies, this relationship also suggests the apathy of employees, more prone to doing only what is required of them to maintain their position. This in combination with the opinions of the emphasis on information systems supports the demand to increase its prioritisation from both an internal perspective as well as the literature findings, demonstrating that even apathetic employees feel the emphasis should be increased. Information security systems and policies which lack the emergency management, assessments, and other areas mentioned should be restructured entirely, while all organisations should consider a similar method to appropriately encompass and integrate an information security policy which meets the array of generally unaddressed demands reported in literature and the present study.

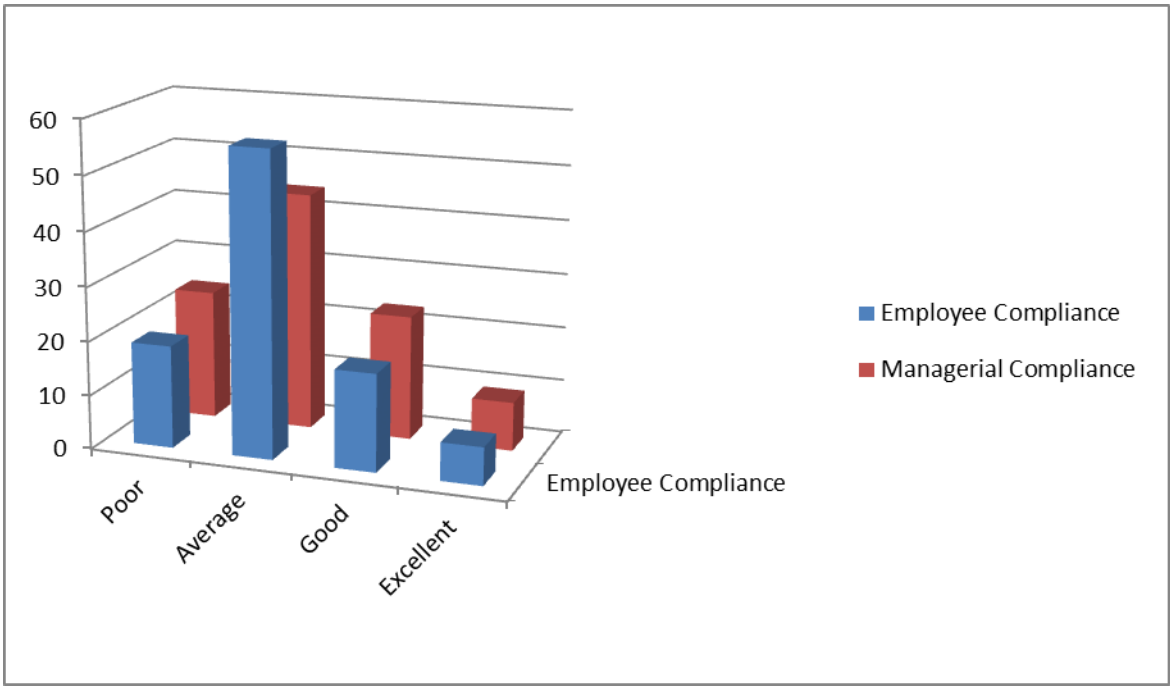


Figure 6.1: Compliance Ratings, Managers vs. Employees

The reproduced figure below shows the strong feelings of employees whom were prone to be apathetic to the range of information security issues. If this is the perspective of apathetic employees, it can rather safely be assumed that the reality of the literature findings apply wholly to even the advanced (compared to the average Saudi institution) and powerful financial institutions.

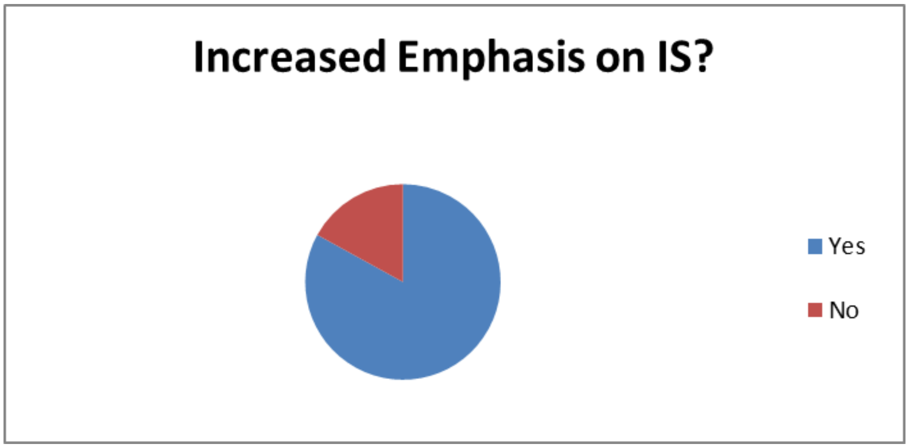


Figure 6.2: Recommending additional Emphasis in IS (at the Organisational Level)

The recommendations offered from employees provide some insight into the required recommendations for optimising IS, but have limited local perspective which generally do not consider the large issues which only lower or upper managers may be aware of. As such, these issues should at least be reviewed, and then filtered or refined as needed for development and implementation. These developmental areas include greater effort from managers (including innovation and consideration, as well as greater involvement in the company's information systems), additional training for managers, additional IS training for all employees, improved facilitation for employees sharing information, improvement of policy to ensure that the technological potential is optimised (as the majority of employees asserted that the technology alone is not sufficient for meeting IS demands), and an improvement of technology. These generally support the recommendations outlined, and should entirely justify the development of initiatives aimed at addressing the areas for improved IS; meanwhile, areas such as improved employee communication should be considered by including employees in a short portion of the meetings (or separate routine meetings) to discuss concerns, experiences, or suggestions for general improvement.

Summarizing significant recommendations in brief, these include:

- the recommendations from Althaneer and Nelson (2009) should be followed, including: i) increased confidentiality of sensitive information (concerned with preventing disclosure of information to unauthorised users), ii) integrity (concerned with ensuring data cannot be modified without authorisations), and iii) availability (concerned with ensuring information must be available to authorised users when they require them)
- mobile phones should be a key area of focus in awareness and improving security systems, and the rising number of mobile phone users, internet users
- each bank should inform employees of statements such as the mobile subscribers with cumulative annual growth rate
- the information security policies should be formally structured, printed in detail, provided to each employee, and routinely reviewed
- the employees and managers should be polled on a routine basis regarding the perceived effectiveness and potential for change
- brief training sessions should be scheduled on at least an annual basis to update the employees on changes to technology, policy, or threats

6.5 Policy Recommendations Regarding Managers and Interview Topics

Although the managers provided only a comparatively small sample, their perspective, experience, and resultant implications carried significant weight; one should regard their experience and perspective with seriousness, and their responses implied the situations are in fact as serious as published in the recent literature (i.e. Saudi Gazette, 2007 and Muhaya, 2010). Thus, recommendations for these areas are of comparable or greater importance. Naturally, areas which are considered in both instrumentation pieces are critical, and especially those which have been noted in literature as well. Some banks reported feeling very secure in comparison to the remainder of the nation, but have nonetheless reported problems with firewall breaches, viruses, and other issues which could be better addressed through evolution on a par with similar organisations in developed nations. According to the interviews, there are problems on networks more often than projected, and this is evident across all departments; meanwhile, the biggest concern for information system security is always protecting the network, and at this point in time, the most vulnerable technology is the firewall and security software. Employees hope that both improvements in available software take place at a rate faster than those would wish to break into the network can develop hacking methods, and that they continue to have access to defence technology within a fair amount of time once it becomes available. These areas can be addressed through the aforementioned recommendations as well as an emphasis on technology.

The manager perspectives imply a greater need for technological improvements, although the employee responses suggest that the technology alone is not sufficient to address the lower-level everyday issues. Ideally, both should be addressed, with investments in technology only taking place when there have been clear improvements over existing technology. Members of upper management should discuss existing improvements to technology in the proposed routine meetings, and decide whether the improvements to hardware or software would translate to a useful difference to information security processes or demands. The greater concern of the threats from commercially available technology can only be addressed through the improvements of technology and procedures on a comparable scale, but improved efforts to study and communicate these threats in an organised manner would decrease the potentials for the threats to catch the organisations 'off guard.' Similar to the lack of organised emergency management or disaster recovery, there does not appear to be an organised procedure to facilitate this communication (nor requirements to locate and assess threats); clearly, this should be implemented into policy.

Software maintenance was more commonly mentioned by managers than employees, although employees may have simply taken this area for granted. This should simply be an area of concern, observation, and discussion that is a formal part of policy. The relations of operations to firewalls and SSL were found to be the greatest concerns in the organisations observed, and this was noted in literature as well.

The remainder of the other implications from the interviews, such as a lack of concern for development, general concerns of threats, and apathy towards compliance and ethics, can be addressed through similar means as those described in the previous section.

- managers should conduct individual studies of organisational factors influencing personal ethics managers should better motivate employees to facilitate optimal security

- upper management should continue setting the groundwork for continuing improvement (by assessing the most influential institutional factors, and their relationship with managers and employees)
- the employees and managers should be polled on a routine basis regarding the perceived effectiveness and potential for change
- managers should petition for changes to policy or relevant factors (i.e. software) based on this feedback
- managers should be liable to report any potential threat to security, and be provided with further means to handle threats should the present themselves
- managers should request to update or upgrade the existing firewalls and anti-viral programs managers should either have a means of performing these actions solely, or should have access to someone who can perform this action immediately
- members of upper management should discuss existing improvements to technology in the proposed routine meetings
- managers should decide whether the improvements to hardware or software would translate to a useful difference to information security processes or demands

6.6 Summary and Implications to Stakeholders

Listing the main recommendations of this effort, these were determined to be:

- managers should conduct individual studies of organisational factors influencing personal ethics managers should better motivate employees to facilitate optimal security
- upper management should continue setting the groundwork for continuing improvement (by assessing the most influential institutional factors, and their relationship with managers and employees)

- the Saudi government could play a further role in promoting these developments
- safeguarding the economy
- the recommendations from Althaneer and Nelson (2009) should be followed, including: i) increased confidentiality of sensitive information (concerned with preventing disclosure of information to unauthorised users), ii) integrity (concerned with ensuring data cannot be modified without authorisations), and iii) availability (concerned with ensuring information must be available to authorised users when they require them)
- mobile phones should be a key area of focus in awareness and improving security systems, and the rising number of mobile phone users, internet users
- the increasing capacity of mobile technology to be integrated with online technology should be at the forefront of information system education and development for years to come
- each bank could inform employees of statements such as the mobile subscribers with cumulative annual growth rate
- the information security policies should be formally structured, printed in detail, provided to each employee, and routinely reviewed
- the employees and managers should be polled on a routine basis regarding the perceived effectiveness and potential for change
- managers should petition for changes to policy or relevant factors (i.e. software) based on this feedback
- brief training sessions should be scheduled on at least an annual basis to update the employees on changes to technology, policy, or threats

- managers should be liable to report any potential threat to security, and be provided with further means to handle threats should the present themselves
- managers should request to update or upgrade the existing firewalls and anti-viral programs managers should either have a means of performing these actions solely, or should have access to someone who can perform this action immediately
- members of upper management should discuss existing improvements to technology in the proposed routine meetings
- managers should decide whether the improvements to hardware or software would translate to a useful difference to information security processes or demands
- the remainder of the other implications from the interviews (i.e. a lack of concern for development, general concerns of threats, and apathy towards compliance and ethics) should be addressed through similar means as those described in the previous section

Essentially, organisations facing multiple problems and issues addressed through the present study and literature are advised to completely restructure their IS procedures; this would serve to encompass the entirety of concerns, best practices, and flexibility for routine assessments and developments. The changes demanded are so great that there are major implications for stakeholders, in relation to both technological improvements and restructuring policies. A table of these concerns was presented in the analysis section, is reproduced in the figure below, and is the subject of the continuing analysis in the following chapter.

Issue	***Importance to Stakeholders***
Technology upgrade demand	Stakeholders should note that: additional resources and means to acquire or improve technology in demand, current emphasis on development in other areas may require change in priority
Apathy regarding compliance	Compliance need not be addressed, while emphasis may even be removed from this area in future developments
Apathy regarding ethics	Ethical guidelines should remain intact, however, any developmental initiatives or resources diverted to improving ethics may be better diverted to a more practical area.
Mixed opinions regarding policies	Policies should be examined individually and more cautiously in any considerations for reform, while the time dedicated to this process should depend on the varying responses regarding this topic.
Security concerns	These should increase the prioritisation of technology, research, and overall reform initiatives.
Ability for nation to address problems	Stakeholders should remain mindful of the incapacity of the nation to address root problems in the near future, becoming motivated and facilitating motivation for change.
Inability to take action matching strive for technology	Similar to the other areas, stakeholders should increase the motivation and prioritisation for actual change, although it also shows the motivation for acquiring technology alone is generally considered sufficient.

Figure 6.3: Summary of Key Recommendation Topics and Implications for Stakeholders

Upper and lower management must assume additional responsibilities to ensure that the prioritisation recommended in literature and demand confirmed in the previous analyses are sufficiently integrated into practice; this demands technological improvements and assessments, routine meetings considering potential threats and improvements to systems, altering policies to address employee operations and demands, and removing the apathy towards both threats and compliance. These policies should be tailored to the specifications of the individual organisations, printed and distributed, strictly enforced, and updated (with the cycle repeated) as deemed necessary in periodic analyses. Managers must have a means of making changes prior to these analyses, whether it be through suggestion and assisted research or immediate development pending policy restructuring. Training must also be given additional prioritisation, and the suffering awareness can be facilitated through this and the inclusion of employees in routine meetings. See Chapter 8 for further relations with literature.

Chapter 7: Evaluation of Stakeholder Recommendations

7.1 Introduction

Stakeholders from the ten institutions targeted for analysis were targeted for feedback regarding the recommendations proposed in Chapter 6. As reading the entirety of the chapter alongside express written feedback and recommendations for future development did not seem feasible (or ideal to recruit participation), the researcher developed an additional set of questionnaire instrumentation to apply to stakeholders. Three stakeholders from each institution were contacted, forming a sample of 30 participants overall,.

While the findings of the primary research are important to stakeholders, the feedback from stakeholders regarding the direction of recommendations is important for the development of the company; stakeholder opinion and influence are major factors in development, and with many issues important to stakeholders addressed in proposed recommendations, an assessment of their feedback regarding the key points of these recommendations is valuable to the study. Generally considering or addressing issues in annual general meetings, Board of Directors' meetings, or Executive Committee meetings, stakeholders are commonly known to express their concerns in areas including the soundness of organisational governance, asset protection, and return on investment, while all of these issues are relevant to the findings of the primary research. Stakeholders may respond to these issues and recent actions by judging whether reform efforts have been sufficiently thorough, rating the effectiveness of growth or profit, and offering recommendations or posing questions in other areas. Through this area of the research, the issues in the primary research can be addressed in a sample of stakeholders directly, allowing the researcher to apply and discuss the combined evaluations of managers and stakeholders. This has implications for the demand for action and the nature of change, thereby allowing the researcher to 'close the loop' as mentioned while leading to the concluding discussion of this research initiative.

7.2 Stakeholder Recommendations

7.2.1 Sampling

The managers participating in the interviews were contacted regarding recommendations for accessible stakeholders. Brief lists were provided from one manager from each facility, and these stakeholders were contacted regarding their willingness to participate. As the target sample size was 30 stakeholders, equally representing the companies analysed, subsequent stakeholders were not contacted once three participants had agreed to contribute to the sample. With this, convenience sampling was the predominant method used aside from inclusion criteria.

7.2.2 Instrumentation

As stated, a survey questionnaire was developed and applied for this area of the research. A total of 12 items were strategically developed to address key areas of the recommendations, as well as the primary areas of importance, outlined in Chapter 6. While the interviews revealed differences in opinions between managers and banks, and the banks are assumed to be operating with different technological capacities and unique policies, the instrumentation used was the same for each stakeholder; no custom consideration was made, and the instrumentation examines the general areas of concern, common areas of neglect and demands for improvement, common attitudes, and the recommendations which had been developed considering these areas. Some of the questions were designed to assess the prioritisation of each noted area of importance, others to rate the effectiveness of the specific qualitative recommendations, and others to rate the perceived demands for change in information security. It was assumed that the stakeholders were aware of the issues outlined in the study, as well as the general demand for improvements in the nation; however, the stakeholders were recommended to read provided material (covering the background and issues of concern) if they were not familiar with the rationale for information security changes in Saudi Arabia. See following section for relations to recommendations, and see Chapter 8 for relationships with objectives (as well as analysis in relation to literature).

The instrumentation questions were developed as follows:

1. *"Upper and lower management are recommended to assume additional responsibilities, to ensure that IS prioritisation recommended in literature is sufficiently integrated."* Please rate how strongly you agree with this statement (1 representing no agreement and 10 representing strong agreement). ___________

2. Regarding the statement presented in Question 1, please indicate the ratio you feel these IS responsibilities should be divided (e.g. 50% upper management and 50% lower management). ____________

3. Technological improvements and assessments are recommended as a top priority for progressive change. Do you agree (Y/N)? If yes, please rate the prioritisation you feel should apply to this area (please use a scale of 1-10)______ If no, please state why you do not feel this should be a priority in change________

4. Routine meetings considering potential improvements to systems are also recommended as a high priority for progressive change. Do you agree (Y/N)? If yes, please rate the prioritisation you feel should apply to this area (please use a scale of 1-10)______ If no, please state why you do not feel this should be a priority in change________

5. Removing apathy towards threats and compliance is another of the most highly recommended changes towards improved IS. Do you agree that this should also be one of the leading priorities (Y/N)? If yes, please rate the prioritisation you feel should apply to this area (please use a scale of 1-10)______ If no, please state why you do not feel this should be a priority in change________

6. The final leading priority recommended for improved IS is altering policies to address employee operations and demands. Do you agree that this should also be one of the leading

priorities (Y/N)? If yes, please rate the prioritisation you feel should apply to this area (please use a scale of 1-10)______ If no, please state why you do not feel this should be a priority in change________

7. Considering the outlined recommendations for improving IS in accordance to common demands, tailoring policies to the specification of the organisation, printing and distributing them, strictly enforcing them, and updating them as necessary (in accordance with periodic analyses) are recommended. Please comment

____

____

8. To achieve the above, managers must have a means of inciting change, whether through recommendation and pending additional research, or immediate development pending policy restructuring. Each has potential advantages; do you recommend the i) recommendations pending research and approval, ii) immediate developments and policy restructuring, iii) a vote to take either action, or iv) another approach? If you selected iv), please describe

____

____

9. Do you agree formal training (at least one full day) is required to properly address IS issues (Y/N)? Why or why not?____

10. Do you agree that compliance and ethics are only minor concerns, while the majority of employees generally do not create any issue responsible for current levels of IS (Y/N)? Comments?____

11. Do you agree that restructuring initiatives must be developed, implemented, and maintained, or do you feel that generally improving awareness within companies will lead to change? Please explain ____

12. Please provide any other comments you feel are useful in this effort to improve the provided recommendations; any information is appreciated.

____

____

____

7.2.3 Results

The pilot study of the questionnaire revealed that the original draft of the instrumentation was sufficient for the final distribution, and thus the data provided by those respondents was included in the study. Once the targeted quantity of 30 had been achieved, the sample was deemed complete, with the results compiled.

Responding to the first question, asking for a rating from 1-10 regarding the assumption of new managerial responsibilities, the average response was a 7.6. This shows that the average stakeholder feels that the managers need to assume a substantial amount of new responsibilities, while this is the ideal direction towards progressive change. This also shows that the general context of the recommended changes was well received, with the majority stakeholders willing to participate in this assessment feeling that changes are needed to address issues in IS. The second question revealed that stakeholders feel that upper management is more responsible for these changes that lower management, with the average ratio provided by respondents being a 70-30 split of added responsibilities; this is generally in agreement with the recommendations, although no ratio had been presented in the recommendations, the outlined direction and changes require more actions from those with sufficient power (and less actions from those controlling and monitoring lower functions). Meanwhile, stakeholders are more capable of discussing the recommendations and proposed changes with those they feel should be evoking them, but they generally must recommend courses of action for change for those whom have less contact with the stakeholders. The average ratio of recommended responsibilities is shown in Figure 7.1 below.

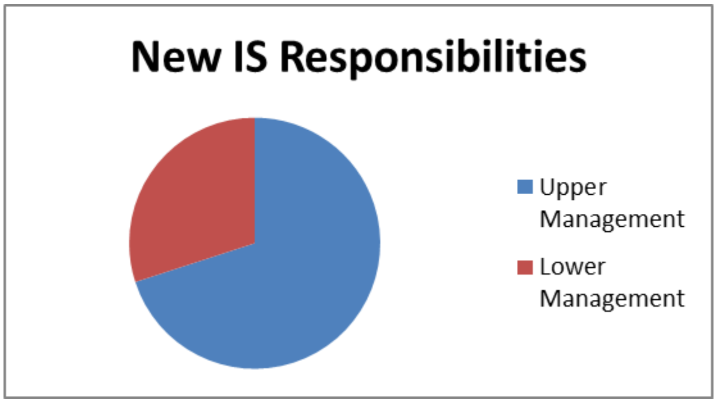


Figure 7.1: Recommended division of new IS responsibilities controlled by management

The third question asked respondents to state whether they agree with technology improvements and assessments being a top priority. Here, 50 percent of respondents stated they agree with the statement, and 50 percent stated they did not agree; with this, the reason for the substantial disagreement was the wording of the statement, as stakeholders generally felt that the use of technology (including assessments) should be the primary focus, with the technology itself being more adequate in the current situation (especially hardware). The respondents rated the prioritisation of this area at an average of 6.2. Additional comments regarding the prioritisation of this area included the need for a few software improvements compared to the greater need for improved organisation, monitoring, and policy; moreover, roughly one-quarter of the stakeholders commented that organisation should be pursued first, with technological demands outlined and addressed following these efforts, making the probability for demanding technological improvements high but ultimately unknown without institution-specific analysis of detailed specifications related to demands.

Regarding the fourth question inquiring about the demand for routine meetings discussing IS capacity and demand, the majority of the respondents agreed that this type of improved communication is needed to better address areas of IS. Thus, 67 percent agreed with the recommendation, while the remaining third of the respondents stated that the current levels of discussion in their institutions are sufficient in terms of time and frequency (but generally require improvements in the efficiency and effectiveness of these discussions). The average rating for prioritisation was 6.2, with additional comments regarding prioritisation including increased analyses being conducted outside of meetings, brought to attention at the meetings, and the amount of time dedicated to IS being recommended on a case by case basis. Here, approximately one third of the respondents did not feel that routine attention to IS in meetings was necessary aside from the brief mentioning of findings or concern. Figure 7.2 reveals the general willingness of stakeholders to support routine IS discussion in meetings; the fact that the majority of stakeholders feel such an investment in time would be worthwhile further shows the general support for additional diverted effort, as well as the recognition for substantial development in IS.

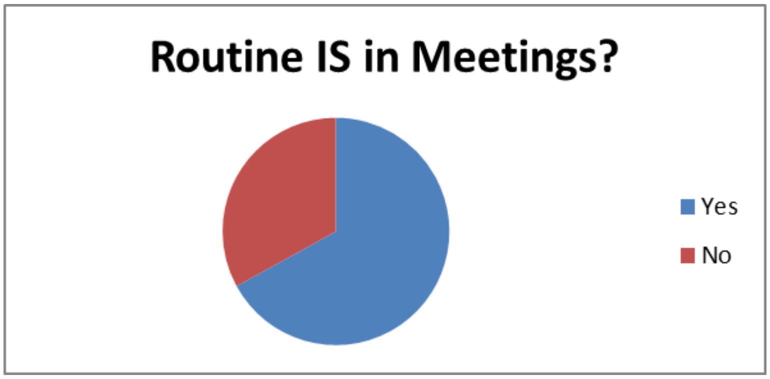


Figure 7.2: Percent of sample recommending routine discussions of IS prioritised in meetings

The fifth question asked respondents to address the observed apathy regarding compliance and potential threats; the research recommendations suggested a prioritisation (and thus increased attention and effort applied) towards the existing apathy. When asked whether they agree that this should be one of the leading priorities in a campaign for improved information security, 73 percent of the respondents reported that they agreed, with the remaining 27 percent reporting that they feel these areas should not be prioritised in such a campaign. Rating the prioritisation they feel should apply to the area, the average stakeholder rated the prioritisation to be at 7.6. This shows one of the more significant prioritisations in the campaign, with a large number of comments stating that apathy towards threats is a much greater problem than apathy towards compliance (as was also implied from the interview questions). A small portion of respondents (approximately on quarter) commented that compliance should be addressed but in a minimal (non-prioritised) manner.

Addressing the sixth question, examining the demand to alter IS policies to better regulate employee operations and demands, 80 percent of the respondents agreed this area should be prioritised. With this, the average rating of prioritisation was a 7.8, being the most highly rated recommended priority. The minority 20 percent provided comments including that policies must be added or enforced to address the most pressing issues, with the potential for existing policies needing to be altered was minimal for their circumstances. Naturally, the exact variables relevant to this are expected to vary significantly between organisations, as policies are an area most prone to differences compared to the other areas considered. In spite of this, the generalised recommendations aimed at the common and shared themes between organisations, produced this highly supported and prioritised recommendation.

The seventh question asked respondents to provide comments regarding the recommendations for tailoring the existing policies to better meet the demands to improve IS (while still considerate of the organisational variables and needs), printing and distributing policies throughout the organisation for maximum awareness, and updating them in accordance to routine examinations. The overwhelming majority of respondents simply agreed with this, stating that they felt this would be the best course of action for any bank attempting to implement such initiatives to take. Others felt that these areas would naturally follow from the other mentioning of altering policy; there were mixed comments regarding the nature of routine examinations and updates, with some agreeing there should be periodic assessments, with others feeling this may be a waste of resources in the absence of a probable cause. Through the pilot study implied that additional and meaningful information could be generated through the inclusion of this question (and its due consideration of the summary of recommendations provided), the responses did not reveal anything that was not implied from previous responses.

The eighth question requested that the stakeholders comment on the managerial needs of inciting change, through recommendation and pending research (versus immediate developments and policy restructuring). Acknowledging the potential advantages, the study requested that respondents state whether they recommend either action over the other, a vote to take either action, or some other approach; in response, 20 percent sided with changes favouring (further) research and restructuring, 30 percent favoured immediate developments and policy restructuring, 40 percent reported that the vote would be the best action, and the remaining 10 percent thought another approach would be best. The 10 percent reported that they thought the best approach would be to, rather, a combination approach based on a vote; here, members of management (presumably with stakeholder influence) would vote on how to designate desired developments in either of the two areas. This shows that the recommendations are generally supported by the stakeholders, but half of them feel they would discuss them further before attempting to take action to actually change anything. The other half generally supports the recommendations, and feels that the best way to go about seeing real change is dependent more on circumstance and permissible methods of action. This was expected to some degree, as the recommendations were admittedly based on the shared themes and demands noted in the primary research. The final questions in the survey attempted to gain more insight regarding stakeholder evaluation and more specific aspects of plans for progressive development within the individual institutions.

The ninth question asked the respondents if they agreed that formal training, involving at least one full day of structured information exchange or preparation, is required to properly address existing IS issues. Unfortunately, this question does not consider the quantity of individuals potentially involved in the training, leaving the respondents to select a response whether they feel two individuals should be trained or half of the company trained; this was not noted in the pilot study while the researcher assumed the responses would still be sufficiently useful. Fortunately, the follow-up ‘why or why not’ element of the question allowed the researcher to extract at least some meaningful information from the stakeholders. Addressing the closed element of the question, 80 per cent of the respondents agreed that at least some formal training was required to meet desired IS objectives, generally in support of the need for change and the methods required to bring the changes. Addressing the ‘why or why not’ component, respondents gave responses ranging from lower level management needing training, upper level management needing training regarding IS management and leadership, lower level security workers needing training regarding their own pursuit of IS issues and communication with management, training for managing research and development, and training for change management. The remaining 20 percent of respondents felt that this could be addressed without formal training, and could slowly be addressed informally through management initiatives, meetings, and integrations of such actions into job description. While this appears to be more challenging, less organised, and having the potential for lower levels of effectiveness (or even efficiency) in outcome, the potential for overall efficiency is nonetheless evident; further discussion on these topics at theoretical levels is provided in the following section.

The tenth question asked respondents to state whether they agree that compliance and ethics are only minor concerns, while most employees' non-compliance does not contribute to current issues in IS; 90 percent of respondents reported agreeing with this question. Although the commentary generally agreed with the recommendations, comments included recommendations for examining compliance and impact in greater depth, emphasising compliance with a lesser consideration of ethics, and asking employees if they have noticed ethics affecting daily aspects of IS.

The eleventh question then asked respondents if they agree that restructuring initiatives should be developed, implemented, and maintained, or if they feel that improving awareness alone can facilitate the required changes. Here, the majority of the stakeholders agreed that awareness alone could not bring about the types of changes demanded, with only 20 per cent asserting this method should be sought. These stakeholders provided an extension of the logic provided in regards to the meetings and structure, stating such effort would not be demanded while a general encouragement and informal call to action in daily routines would lead to the changes demanded; these stakeholders felt their institutions are capable of inciting significant change without strategic planning, development, and change management.

Although the institutions with the higher levels of organisation and general success in operation may have the capacity to achieve such feats in a way which appears to be more efficient than seemingly more consuming restructuring campaigns, it is common knowledge among management and organisational literature that significant changes benefit more from change management; these campaigns need not be consuming, but they should be organised, planned, and monitored to some degree to ensure success (Muhaya, 2010). This is discussed in further detail in the following section, while this preliminary analysis accompanying the results suggests that strives for efficiency responsible for shortcomings in IS are evident in a considerable portion of stakeholders as well. Meanwhile, the stakeholders which agreed that restructuring initiatives must be developed, implemented, and maintained did not specify if they felt the extent of formality and structured recommended in change management best practices would be required for successful change; however, the variations between stakeholder opinions, management opinions, and the recommendations in best practices is an area worthy of consideration in developing IS (as well as other areas).

Lastly, the twelfth question asked respondents to provide any other comments they felt would be useful in the overall initiative to improve the subareas of the provided recommendations; fortunately, the majority of the respondents did provide some commentary, with only 30 per cent declining to contribute to this particular item. The most common comment (mentioned to some extent by 40 percent of the sample) agreed with the findings of the preliminary research that management was commonly prioritising efficiency over effectiveness in IS, with some stakeholders pressing for the prioritisation of effectiveness and continuous updates. Approximately 20 per cent of stakeholders commented on the lack of concern for emergency management and disaster recovery policies, were aware of the existing literature reporting this to be a common issue across Saudi Arabia, and recommended a formal approach to at least this area; with this, approximately 30 percent stated they felt certain IS demands could be addressed informally, and only a partial amount of the recognised areas demanded a formal campaign or initiative to effectively guide change towards the objectives.

7.3 Evaluation

7.3.1 Introduction

There are many recommendations that need to be followed, and the arguments for this are clear, considering both the range of literature reviewed and the research assessed. The argument for the recommendations is further supported by this evaluation, while it also considers stakeholder recommendations.

7.3.2 Stakeholder relations

With the majority of demands for change acknowledged in the majority of stakeholders, the implications for management and the institutions are thereby amplified. Although a considerable portion of the respondents did not feel that formal initiatives are required for effective change, a larger portion reported feeling there is a genuine demand for formal change in at least a portion of the areas. With this, only a fraction of the institutions may agree to plan and implement a campaign for improving information services, but the majority of stakeholders and managers agree with the needed direction for change in the areas discussed. This implies a comparable perspective in managers and stakeholders, and implies the stakeholders generally agree with the recommendations of literature guiding this research, in spite of the current state of the system and present lack of informal or formal change initiatives. Whether the agreed demands for change are formal or informal, the results from the stakeholders and managers imply that attempts to pursue best practices and IS upgrades are held with a higher regard, and the study may have prompted additional research, informal efforts and increased awareness, or even some structured attempt to address the issues pointed out. The demand for stakeholder support for significant changes appears to have a high potential to be met with this level of support, based on the current sample and responses, but changes requiring a wide range of stakeholder support may still be challenged by the much larger samples affecting all institutions. This report could serve to encourage managers wary of stakeholder response to pursue action.

7.3.3 Management

The 7.6 rating for increased managerial responsibilities has proportional implications for the demands on managers to play a critical role in improving information systems. As described in the previous chapters, a common issue restricting developing IS to its current potential is a mentality that existing threats have been addressed to maintain the existing levels of operation and incidents. Managers may also feel too preoccupied with their duties or stresses for improvements in other areas, leading to the lower level of prioritisation in IS; meanwhile, some stakeholders feel that this is an area in need of top priority, while others agree that it need not be prioritised beyond the basic developments required for basic service, likely leading to division regarding the prioritisation of optimising development. With the rise of technological capabilities, it is commonly known that systems which appeared to be more secure only a few years in the past may be vulnerable to many threats in a small amount of time, and Saudi Arabia has been found guilty of an inability (or apathy) to continually 'catch up' with technological developments; also as stated in previous chapters, even if the entire nation maintains a comparable level of gradual technological development, increasing globalisation and entrance of new technology further increases the potential for treats (Saudi Gazette, 2007; Muhaya, 2010). Banks should be at the forefront of IS optimisation, and it appears that the combination of literature and findings, manager opinion, and stakeholder opinion may be required to prompt the organisations to 'take the lead' in optimising IS within the nation. In addition to helping their own organisation while reducing the threat for security breaches, the models these institutions follow for optimisation can serve as a model for other Saudi organisations to follow.

7.3.4 Combined evaluations

The 70-30 rating for the split in managerial decisions suggests that the stakeholders have a direct means of discussing how they feel changes should be developed, implemented, or monitored, as they generally have easier access to members of upper management. Meanwhile, the split regarding technology improvements and assessments shows that a great deal of discussion will likely take place before stakeholders and managers agree on significant changes. The analysis and general recommendations leaned towards software improvements more than hardware, with the comments provided by the stakeholders suggesting that this is the most likely change to take place.

Stakeholders generally agree with the need for improved organisation, monitoring, and policy, with explicit expression for prioritising organisation. The recommendations acknowledged its importance, but reflecting on the original results with this in mind, it is evident that the majority of complications could be addressed through a combination of improved awareness and organisation. Meanwhile, however, this also implies that the organisation should involve structure in all areas, with the informal improvements preferred by a substantial portion of the sample being less than ideal in favour of formal or more organised ones. The capacity to organise progressive development without formal changes to policy or highly structured initiatives may be limited (in terms of implementation, monitoring, or unforeseen demands for adjustments), but it may be possible to address the demands of the portion of stakeholders preferring the most discrete and direct improvements, avoiding the potentially distracting and draining campaign approach; further research or attention in this area could benefit understanding or efforts. The two thirds of stakeholders agreeing that routine meetings discussing IS (or at least including IS discussions in all routine meetings) are unlikely to be overwhelmed by popular opinion or resistance to change, assuming the effort for change is made, but it is unlikely that new meetings will be established; IS should not be given a low priority simply because no threats have actually breached the system, with new threats, security technology, and existing states of the system in place at least mentioned in the existing routine meetings. Such discussions should occur on at least a quarterly basis, with the stakeholder results implying they further agree with designated employees researching these threats and protection potentials to provide this information.

The apathy towards compliance and potential threats is likely to only be addressed in terms of potential threats; managers and stakeholders alike feel that apathy towards compliance due is only rarely due to any serious issue directly related to IS functionality; rather, compliance is recommended to be addressed through awareness and questioning employees, while the apathy for potential threats is to be addressed through the combination of changes recommended (restructuring policy, training, awareness, etc.) With this, one of the most highly recommended changes was the restructuring of IS policies to better regulate operations while addressing demands, with the 80 per cent of stakeholders agreeing this should be prioritised suggesting that at least some changes are likely to be incited in the near future. The remaining 20 percent suggesting that existing policies must be better enforced are likely to contribute to changes in this area as well, with the specific variables involved naturally differing between organisations and circumstance.

Preferences for change management are likely to be debated, but the general support for improvements in IS are nonetheless prioritised. The fact that there were comparable responses regarding formal training compared to other formal initiatives further reflects division regarding the optimal approach to change in this area.

Further details regarding more specific changes at the institutional level are naturally possible with the development of separate recommendations for the specific shortfalls and preferences of each institution (and the specific evaluations of each set of recommendations), while the analysis of the institutions revealed shared themes common across each institution; moreover, these findings were comparable to the IS findings in literature observing Saudi Arabia IS in general. The fact that the majority of the stakeholders agreed with the recommendations for IS improvement was likely facilitated by the presence of the related studies, the findings of the literature, and knowledge of the conditions observed in the primary research. The differences in opinion could be due to varying levels of communication with the managers, varying levels of awareness, and different prioritisations of components in business models (i.e. preferring a continuous approach on prioritising maximum profit versus a cautious approach). Considering the causes for differences could be meaningful in further research, but the majority opinions of managers and stakeholders regarding the topics approached in the research strongly supports the notion that banks are equally ‘guilty’ of the lack of IS optimisation, and are thereby in need of improvements. This type of stakeholder support could improve or even incite attempts to address the issues implied by literature and confirmed in this study.

7.4 Summary

The primary research revealed many areas that could benefit from improvement initiatives in IS, with areas importance to stakeholders including demands for i) technological improvements, ii) apathy towards compliance, iii) apathy towards ethics, iv) mixed opinions regarding policies, v) security concerns, vi) the ability for the nation to address issues, and vii) the inability to take action matching the strive for technology. Stakeholder evaluation suggests that all of these areas are indeed important across the entirety of the stakeholder body for the institutions in question, with the exception of components iii) and vii), which were respectively given less priority and addressed through other means. In any case, this analysis clearly reveals that IS problems have been noted in literature, are acknowledged by prominent members of leading banks, and are further acknowledged by stakeholders. Perhaps with increasing awareness, such leading institutions will set a new standard for national IS, and provide a model for similar developments found to be commonly required across the nation. Studies such as this may promote awareness in a way which forces concerns into perspective for the institutions, facilitating the changes they have otherwise been hesitant to make. If not, the findings suggest that threats growing to breaches, and demands for emergency management, may be the only events capable of inciting these types of changes.

Chapter 8: Discussion, Conclusions, and Final Recommendations

8.1 Introduction

This research effort has expanded the existing knowledge base regarding information security, revealing that even Saudi banks are not immune to the problems located in information security literature; meanwhile, as banks have a greater need for IS amid greater consequences for breached security, the resultant demand for development is greater compared to a scenario where medium sized retail businesses were found to be veritably devoid of: emergency management and disaster recovery plans, organised systems and technology matching threat capacity, or other weaknesses described by this analysis and discussion. The research and analysis led to the formulation of recommendations in line with previous literature (as shown in Chapter 6), with the majority of stakeholders agreeing with this guided direction for development. This chapter provides additional discussion, conclusion, recommendations, and closing commentary relevant to this research effort; through this, the project is summarised, relationships in concepts and theory are explored further, and recommendations for future research and development are described in detail. Clearly, despite the fact that Saudi institutions have generally been safe with existing IS systems, their potential to be overwhelmed by existing threats and to be thrown into an emergency situation without protocol is great enough to warrant substantial awareness and developmental initiatives.

8.2 Discussion

8.2.1 Further Analysis of Findings

The findings support the general findings of literature, despite the obligations of financial institutions (Saudi Gazette, 2007; Abu-Musa, 2009; Muhaya, 2010). With this, many elements of the results and feedback are relevant to the literature conclusions and recommendations, fortunately leading to a near consensus capable of inciting development. The 100 total respondents participating from the ten institutions were thereby representatives of some of the most prestigious institutions with the greatest information security needs, and provided data revealing that the prioritisation of both optimising technology and improving protocol are low. Although banks have the financial and organisational capacities to have implemented the changes recommended in literature and best practices at the time they were published, but both the desire to research these topics while investing in these aspects of IS were found to be low priorities (if considered at all) across the employees observed.

As stated in the results and analysis chapter, the percentages of employees serving in the aforementioned list of organisations was also calculated from provided totals, with approximately 18 per cent from Al-Jazira Bank, 14 per cent from Arab National Bank, 11 per cent from Al-Rajhi Banking & Investment Corp., 14 per cent from Riyadh Bank, 6 per cent from Saudi American Bank, 11 per cent from Saudi British Bank, 6 per cent from Albilad Bank, 6 per cent from Saudi French Bank, 8 per cent from Saudi Hollandi Bank, and 6 per cent from Saudi Investment Bank. Although the percentages of the employees were slightly disproportionate, and the study could have been improved through a larger sample including 30+ members from each organisation (not to mention additional interviews), the results and interviews nonetheless revealed the comparable trends with findings in literature; the validity and reliability of the instruments combined with these facts validates the results, analysis, and recommendations.

Further examining the perspective of employees participating in the study, their respective positions have effectively conveyed knowledge of the inner workings of IS in their respective organisations. With this, the leading position among the respondents was a variation of a computer technician (such as "technical supervisor," "systems operator," and similar titles), while approximately 59 per cent of respondents reported being employed in this position. As more than half of the employees had direct knowledge of operation and development in IS, they were perhaps more aware of the shortcomings, demands, and influential processes than the analysts observing functions of IS in some of the studies included in the literature review. All employees had confirmed having a substantial role in IS prior to participation, and the researcher attempted to be sure in order to best facilitate this meaningfulness and value in perspective, potentially contributing to the existing knowledge base more so than existing studies. In addition to the stated 59 per cent portion of computer technicians in the sample, lower-level management positions were most common, with 24 per cent of employees having some sort of team leader position (with titles including "department supervisor," "assistant manager," "technical supervisor," and others); beyond this, the remaining portion of employees (17 per cent) were members of middle or upper management, with the average time spent at the organisation (listed, time in other similar positions in different organisations was possible) was 7.6 years. This further contributes to the perspective demanded for an effective study, and combined with the validity and reliability emphasised in the strategic development of the instrumentation, the implications of the findings provided through the combination of this sample and instrumentation were indeed significant. Closing the research loop through the stakeholder analysis adds further weight to the implications for those responsible for the current states of development, with a considerable potential for pressuring these organisations to take further action for development. Although their superior significance to findings in other studies is debatable, their comparable significance is clear, with the collaborative implications of all studies being great in the face of threats evolving more rapidly than defences (or even operational protocol).

8.2.2 Relation of Major Findings to Current Literature

As described in the literature review, the trends in Saudi institutions are thought to be a by-product of shared traits across the nation. Whilst Saudi Arabia has the largest economy in the Middle East, it is still commonly described as a ‘developing’ country as opposed to a ‘developed’ one, with this status related to some aspects of technological and organisational development in spite of the national success with oil and foreign investments. While prior plans incited ICT development between 1990 and 2000, emphasising the improvement of education, financial, legal, and technical skills. Unfortunately, however, these plans were not parallel to the IS strategies best practices, technology, and protocol common place in developed nations, while the threats growing in developed nations gained increasing potential to apply to Saudi institutions. The 2005 NCITP plan described required a five year developmental initiative to improve national IT in general, but this too could not parallel the developments in nations such as the United Kingdom, while the threats arising from higher levels of development were entirely applicable to local IS.

According to Alfawaz, Nelson, and Mohannak (2010), “understanding the complex dynamic and uncertain characteristics of organisational employees who perform authorised or unauthorised information security activities is deemed to be a very important and challenging task” (p. 2). While the challenge clearly applies to even the prestigious organisations assessed, the importance of these issues at the organisational level appeared to be lacking, thereby demanding some motivating factor in addition to any assessment of the capacity to implement developmental plans. The power of the banks is assumed to be great enough to implement even major efforts to overhaul IS, but the apathetic attitudes and lack of organisation in certain areas suggested that the developmental initiatives would also require effort to motivate the organisation demanded to carry out such a plan. Alfawaz, Nelson, and Mohannak (2010) also studied three cases in relation to IS: a private organisation with more than 5,000 employees, various participants, from public organisations, and a non-profit organisation employing an estimated 3,600 people. Here, the authors had the opportunity to assess senior managers, information security managers, information technology specialists, and other managers and users. Unexpectedly, the results of this study do not directly compare to the results of the case studies, as the three primary causes of security incident and barriers to improving IS were determined to most commonly include compliance and behavioural issues (Alfawaz, Nelson, and Mohannak, 2010). In the primary research, compliance was not determined to be a major cause of incident, but forms of compliance were directly or indirectly considered responsible for the existing states of development.

Beyond the primary concern of compliance and behaviour, Alfawaz, Nelson, and Mohannak (2010) reported that the next most inhibiting areas included downloading internet software, password sharing, using shortcuts, browsing potentially vulnerable content, ignoring policies, not sharing information regarding security practices, failing to report security violations, and not enforcing IS rules. Here, roughly half of the findings are relevant to the study; despite half of the areas not being mentioned or related to significant influence, this is not to state that these areas do not apply to the organisations on any level, but the failure to share beneficial information, failure to act on compliance violations, and ignoring the relevant procedures outlined in literature were reported to be much more influential. Alfawaz, Nelson, and Mohannak (2010) stated that the most important of the areas isolated in their analysis including the commitment of top management, the training and skill capacities in IT, security awareness programs, the organisational structure of IT, the roles of IS managers, motivation systems, and implementation of security standards. These are the most relevant aspects of literature in the findings of the study, with the results, analysis, and implications directly paralleling these findings throughout the institutions. Central to the remaining areas is the commitment of top management, who generally holds the power to organise or address the other areas, and are thereby at least partially responsible for current states of development despite the opinions of the employees operating within their company. Also in direct parallel with the primary research, their study generated findings which were reportedly consistent with the perspective that individual compliance is not only related to the capacity of that employee's skills, but is related to the environment and organisational structure. While this was assumed throughout the research, it is likely that the managers agreeing that individual compliance and ethics did not contribute to major flaws in IS had similar mentalities (Alfawaz, Nelson, and Mohannak, 2010).

8.2.3 Other Noteworthy Areas and Implications

Although the findings and recommendations for this work have major implications for substantial development across the nation, while some credit to institutions is given for their ability to keep up with the standards across the developing nations, it should not be implied that developed nations have idealised models implemented nationwide. Research and development in the United States has addressed similar issues in comparably significant organisations, with the United States General Accounting Office (GAO) (2003) reviewed the Financial Management Service (FMS) to assess IS measures and controls; the findings of insufficiently assessed risks and weaknesses in controls despite the quantity of controls, leading to recommendations for IS overhaul. Comparable findings from the research conducted in this thesis have similar implications, while it is acknowledged by managers and stakeholders that the institutions generally require investments in resources, time, and organisational development to meet needs which employees are generally aware of. This relates back to the assumption that the commitment of top management has played a significant role in overlooking weaknesses and development, while it may require an initiative just to obtain this commitment prior to any development for successful change.

The relation of the findings to the conclusions of Hunton et al. (2005) is also significant. This author attempted to comprehend, assess, and evaluate the levels by which financial auditors and IS specialists observe differences in the nature and uniqueness of audit risks associated with organisational systems. This study found that financial auditors were substantially less concerned about topics considered critical in IS including network and database security, the security of applications, the interdependence of processes, and general control of risks. This could have an influence on the commitment of top management or the opinions of certain stakeholders (or others), and should be examined by concerned organisations making an effort to implement or manage changes. Meanwhile, in the study by Al-Maghrabi et al. (2009), the findings revealed that perceived usefulness, enjoyment and subjective norms greatly influence both direct and indirect mediated effects on continuance intentions of consumers in the Kingdom of Saudi Arabia (KSA); perhaps this can assist the development of future planning.

Considering the Saudi environment in further detail, and assuming that this environment has been one of the greatest influences on the rate of development or existing concern regarding threats that have yet to physically effect the organisation, the conclusions of the narrow range of literature conducted in the area provide further insight for the direction of efforts attempting to address the results. The general demand for improved IT and IS in Saudi Arabia has nonetheless existed alongside its use of technology, with superior technology generally being preferred, assuming that the investments in time and resources are considered to be worthwhile. In the absence of significant incident to existing IS systems, and the lack of demand for emergency management protocol, herein lies a major issue. Despite making considerable efforts (with many of these being partially successful) to meet these technological demands through government initiatives or other plans, similar technological demands (and clear rationale for their existence) remain common across the nation; many research analyses, governmental analyses, and independent organisations have confirmed this, as was noted in the findings of the Saudi Gazette (2007) and research analysts outlined.

Re-examining one of the most large-scale surveys documenting the demand in the past five years, the Saudi Gazette (2007) reported the results of a global survey comparatively analysing 1,200 organisations across 48 countries, including a portion of prominent Saudi Arabian organisations. Clearly, this is relevant to the current study, and while all the banks taking part in the study described in this thesis had an official information security policy, the level of organisation and integration with areas outlined in modern best practices is lacking; this is true both in terms of the ability to develop the IS systems in accordance with the widely recognised demands (an organisational and managerial issue) and in terms of the emergency management protocol. The recommendations to improve IS were the foundation of recommendations aimed at addressing weaknesses while optimising the systems, as they included a rationale for improved software and applications, improved hardware, improved usage of existing technology, awareness of threats and strategic design, or even improved organisational cultures and training which facilitate enhanced security.

Profit and efficiency of functionality appear to be the primary motivator of developments or change in the observed institutions, with IS seeming to have (and possibly continue to) a much lower priority in the absence of physical security breaches or major threats. In this sense, it appears that Saudi Arabia may need to be in a near panic of certain types of attacks, or otherwise having grossly outdated technology and systems, to warrant the types of overhaul and redesign recommended in modern IS literature. Although this prioritisation appears to make sense in business terms to those involved, literature has also effectively applied theory to explain why IS should maintain a higher priority. This is especially applicable to Saudi Arabia, as the nation must improve and maintain IS to support the development of the entire economy. The current conditions in Saudi Arabia thereby demand improved technology as well as protocol, in addition to a demand from financial institutions and businesses; these demands were noted by Abu-Musa (2003) nearly a decade ago and are (unfortunately) still relevant in the present year.

8.3 Conclusions

As stated in the research methods, 30 questionnaire items were designed to address 10 subareas within the overall inquiry. Restating these subareas prior to discussing the hypotheses, the inquiries are: i) what are the primary threats affecting information security in financial institutions within Saudi Arabia? ii) how are these threats unique to this sector? iii) what policies and procedures are currently in place? iv) how well do employees follow information security policies and procedures? v) what factors affect the willingness of employees to comply with policies and procedures? vi) how do personal ethics affect compliance with policies and procedures? vii) how do various institutional factors impact employees' willingness to comply with policies and procedures? viii) are there aspects of the current information security policies of procedures that make it difficult for employees to comply? ix) how do overall organisational characteristics affect the successful execution of information security success? and x) what improvements can be made to increase effectiveness of information security operations?

Addressing the capacity for the research to address the recommendations and meet the hypothesis, the conclusions of this study are found to be both informative and indicative of a successful research effort. The aims and objectives of the study were to identify specific threats to IS in Saudi financial institutions, further attempting to identify how the threats are impacted by employees; with this, the study attempted to isolate factors which affect employee willingness to following IS policy and procedure. Additional objectives included examining the current methods of organisation and adherence to policy, assessing the importance of organisational characteristics that can affect employee compliance with policies, developing guidelines for the banks to allow them to establish increasingly effective IS systems, and to provide recommendations for policy and practice. Although this research and discussion was capable of reaching the objectives, it did meet each objective equally; here, the 'most accomplished' objective was the isolation of influential factors, followed by the development of recommendations, while the 'least accomplished' recommendation was assessing the significance of characteristics that can affect employee compliance. This weakness was due to the findings that compliance at the level of IS employees did not affect the overall integrity or operation of the system itself, and rather applied to areas that even managers did not feel played a role in the ability for the system to defend the institution from threats. Meanwhile, the other objectives were accomplished to a sufficient degree satisfying the general research aim and intentions of the researcher, further contributing to the goals of providing original research and guidelines for progressive development.

Addressing each research question, and the basic results:

i) The main threats to Saudi IS within financial institutions are lack of emergency plans, the viable capacity to upgrade technology, the threats from external technologies (including hacking, mobile devices, and more), and difficulty in organising and maintaining a structure which facilities the implementation of best practices.

ii) IS threats within the Saudi financial sector are unique, as sensitive information and funds are protected; this creates both a great potential for damage and a great incentive for criminals, and employees generally recognise this. Online banking does seem to pose a particularly unique threat as breaching security may result in distributing the funds without the need for additional action.

iii) Policies and procedures in place require active and passive security measures, employees and managers alike generally agreed here. While policies in most of the organisations are effective to some degree, they generally implement many aspects of best practices.

iv) Employees generally do not have any particular issue or problem following security policies and procedures; however, innovation and developmental efforts suffer. Policies and procedures in place do require some improvements (generally according to law).

v) The factors affecting the willingness for compliance with policies and procedures are generally related to management. Company policy for punishments is generally sufficient to keep employees from neglecting duties altogether; despite this, the policies were reported to be generally lax and only ensure that employees follow a bare minimum of active and passive safeguards against risks or threats.

vi) Personal ethics do not play a major role in policies and procedure. Although the majority of compliance is mandated and punishable by legislation, actions which are not directly observable or recorded are most likely to be reliant on personal ethics.

vii) Institutional factors do not seem to have a major impact on employee willingness to comply with policies and procedures. Such factors affect the nature of the position, and play a role in nature of employee willingness for compliance.

viii) A lack of training and access to resources proved to be considerable factors, while the organisation of the employees and operation facilitates this to some degree.

ix) Organisational characteristics play a major role in affecting the ability of employees to successfully execute information security while experiencing success, in agreement with the hypothesis for this item. The organisation of processes, the incentives and motivation of employees, managerial styles, goals, and allocation of processes and resources all play a major role in achieving and sustaining information security success.

x) There are numerous potential improvements in demand for information security operations; these can be achieved through Saudi financial institution employees, managers, and the government. Employees could receive additional training on a routine basis regarding addressing attacks, and new issues relevant to reducing threats.

While the inquiries and instrumentation were generally successfully addressed to provide meaningful results, with the areas found to have less influence given decreased prioritisation, the research can also be discussed comparing the hypotheses of these inquiries to findings in the analysis and recommendations; these elements also serve as fitting discussion in a concluding analysis of the topics and research design. With this, the hypotheses regarding ethics and compliance were generally incorrect, with the hypotheses regarding other areas being generally correct. According to the hypothesis for the first research inquiry, the main threats to Saudi IS within financial institutions are the viable capacity to upgrade technology, the threats from external technologies (including hacking, mobile devices, and more), and difficulty in organising and maintaining a structure which facilities the implementation of best practices; this was generally found to be true, but the definition of 'viable' had come to imply that development would not take place despite the agreement of managers and stakeholders. Meanwhile, the hypothesis for the second inquiry stated IS threats within the Saudi financial sector are unique, as sensitive information and funds are protected. Moreover, this was assumed to create both a great potential for damage and a great incentive for criminals, while online banking poses a particularly unique threat (as breaching security may result in distributing the funds without the need for additional action). Lastly, the gathering of bank card numbers can allow violators to commit fraud, theft, or outright identity theft, while there is less potential for this to occur in other industries. This was generally assumed to be true, as such crimes have a higher potential than through the information vulnerabilities of other organisations. Additionally, the bank threats are unique in that this potential is great and the motivation for breaching bank security is higher, but the threats capable of creating an incident in these organisations have a high probability of being powerful enough to penetrate IS systems across the country.

The third inquiry hypothesis was generalised and was supported in the study as it is in literature. It stated that policies and procedures in place require active and passive security measures; it further stated while IS in Saudi organisations are effective to some degree, they generally do not (or cannot) use the best resources available, nor do they implement many aspects of best practices. The research clearly confirmed this. Examining the fourth hypothesis, it stated that employees generally do not have any particular issue or problem following security policies and procedures, but innovation and developmental efforts suffer. This assumed that while policies and procedures in place require some improvements (generally according to law), employees play little to no role in improvement and development; the results also showed that this was also true. The fifth hypothesis stated that the factors affecting the willingness for compliance with policies and procedures are mostly related to the law and management, while company policy for punishments is generally sufficient to keep employees from neglecting duties altogether. Aside from the apathy discovered, this was also shown to be true. The sixth hypothesis was shown to be generally true but parts of it would receive less attention in recommendations due to the findings, as it stated personal ethics may play a major role with policies and procedure, while low ethical values make the employees prone to taking the quickest or easiest approach. This latter element is related to the conclusions of the research, as it appears to be the underlying cause of the observed lack of development amid the organisational capacity.

The seventh hypothesis asserted that institutional factors have a major impact on employee willingness to comply with policies and procedures, while the institution determines which areas are considered, the punishment for neglect, the reward for effort and compliance, and the nature of the operation; with this, such factors were assumed to affect the nature of the position, and were hypothesised to play a role in the nature of employee willingness for compliance. Here, the potential for this impact was observed, but the lack of action in some areas revealed that members of management should have greater power in development. Next, the eighth hypothesis simply assumed that a lack of training and access to resources is the greatest factor in challenges to IS, while the organisation of the employees and operation facilitates this to some degree. The latter part of this was proven, although the lack of training was found to be a significant issue, and the access to resources was only proven to be a problem at the level of employees and lower-level management.

Examining the hypotheses of the final two inquiries further reveals the successful direction of the study and correct implications of literature, with the ninth hypothesis stating that organisational characteristics play a major role in affecting the ability of employees to successfully execute information security; here it was assumed that the organisation of processes, the incentives and motivation of employees, managerial styles, goals, and allocation of processes and resources all play a major role in achieving and sustaining information security success. The findings support this assumption, and do not disprove it in any way, but further evidence in each of the areas could serve to show that they each play a significant role. Lastly, the hypothesis for the tenth item asserted that there are numerous potential improvements which could be made to information security operations, and these can be achieved through Saudi financial institution employees, managers, and the government. Meanwhile, employees could receive additional training on a routine basis regarding addressing attacks, and new issues relevant to reducing threats. The research results and depth of recommendations have shown this portion of the hypothesis to be true.

Generally speaking, the research shows that Saudi IS is at a crossroads, while management teams must make more informed decisions, and IT staff should improve service and communication in IS. Meanwhile, facility managers should be mindful of the incompleteness of even modern tools, and research and implementation efforts should be conducted periodically; these would help to ensure that vulnerabilities due to incompleteness do not give rise to breaches. Numerous potential threats have plagued information security specialists in recent years, while these threats evolve alongside the changing uses of developing technology. Future research and development should be ever vigilant to monitor these threats, assess the potential for change in IS, and discern the most effective methods for developing and adopting change strategies. The following section outlines the recommendations for future research and development in greater detail.

8.4 Limitations of Study

The primary limitations of this study will be the accessibility, funds, and time associated with such a project. Ideally, all financial institutions could be included while all employees with sufficient experience could contribute information. Naturally, this is not possible, and the researcher had attempted to optimise available resources in a practical manner. Meanwhile, the study is further bound by the ability of the questionnaire to extract data, and the ability for the employee to respond with complete accuracy, while both areas are assumed to contribute to the slight degradation of the research results and analysis. Moreover, while the researcher has taken effort to ensure no bias exists while remaining objective, additional biases and limitations may nonetheless exist unbeknownst to the development of this study. However, as described in section 3.7-3.8, the researcher maintains that validity and reliability have been sought throughout all points of this study.

8.5 Recommendations for Future Research and Development

8.5.1 Areas in need of change: Potential for progressive development or research

Summarising the findings of the recommendations, the primary research revealed many areas that could benefit from improvement initiatives in IS, with areas importance to stakeholders including demands for i) technological improvements, ii) apathy towards compliance, iii) apathy towards ethics, iv) mixed opinions regarding policies, v) security concerns, vi) the ability for the nation to address issues, and vii) the inability to take action matching the strive for technology. With this, the subsequent stakeholder evaluation suggests that all of these areas are indeed important across the entirety of the stakeholder body for the institutions in question, with the exception of components iii) and vii), which were respectively given less priority and addressed through other means. To address these issues, one of the most general but potentially effective actions for future research and development is increasing awareness, as such leading institutions can set a new standard for national IS while providing a model for similar developments across the nation. Studies such as this may promote awareness in a way which forces concerns into perspective for the managers and other members of the institutions, thereby facilitating the changes they have otherwise been hesitant to make. If this does not take place, then the findings suggest that threats will grow to breaches, with demands for emergency management likely being the only event capable of inciting these types of changes. With this, the organisations are further advised to pursue on-going research, attempt to persuade members of upper management to organise and invest in such developments, and to routinely compare their existing potential with best practices in IS as well as the growing threats. Additionally, upper and lower management must assume additional responsibilities to ensure that the prioritisation recommended in literature, while they should further demand technological improvements and assessments, routine meetings considering potential threats and improvements to systems, altering policies to address employee operations and demands, and removing the apathy towards both threats and compliance. Any limitations to such efforts should be brought to the attention of still higher management, and continually examined in the future. It would be beneficial for all members of management to pursue research in limitations of developments deemed worthy of investment. If the actions attempting to persuade management are not effective, the campaigning individuals may be able to incite changes through appealing to stakeholders.

8.5.2 Tailoring policy

These policies should be tailored to the specifications of the individual organisations, printed and distributed, strictly enforced, and updated (with the cycle repeated) as deemed necessary in periodic analyses. Managers must have a means of making changes prior to these analyses, whether it be through suggestion and assisted research or immediate development pending policy restructuring. Training must also be given additional prioritisation, and the sufficient awareness can be facilitated through this and the inclusion of employees in routine meetings. Amid any major restructuring effort, any institute not participating could also benefit from the inclusion of the ISO 27000 standards; this was not considered in the research amid the emphasis in other areas and growing number of inclusion (less than 30 Saudi organisations in 2011), but it is widely acknowledged that conversion to these standards is beneficial to IS (Compliances Forum, 2008; IsecT Ltd, 2011).

8.5.3 Saudi Arabia and further research

Ultimately, Saudi Arabia is like many other fast-developing countries in that it faces IS problems which are generally of a greater magnitude than the IS issues in developed nations of the world. Despite efforts to improve IS and IT infrastructure in general, the Saudi government has been unable to strategise and implement a sufficiently complete solution, and these attempts should be continually pursued by both the government and organisations. Research should be continually conducted in the area to follow up on previous studies, consider the potential for government assistance or organizational restructuring, and to emulate or integrate the more advanced technologies and developments in literature.

8.6 Closing Commentary

Numerous methods for improving IS have been proposed from and to information security specialists in recent years, and while the threat evolves alongside the changing uses of developing technology, continuous analysis and strategic implementation is in high demand across the entire Saudi economy. Future work should emphasise more specific aspects of existing security systems as well as more specific barriers to development.

Saudi auditors attempt to control the system, and Saudi users use the system according to legislation developed and implemented by the Saudi government; however, no party has been able to address the issues recommended in literature (i.e. Muhaya, 2010) which were confirmed by this analysis. Meanwhile, Saudi security professionals must be mindful of the incompleteness of even modern tools, while research and implementation efforts should be conducted periodically (as well as when needed) to ensure that vulnerabilities due to incompleteness do not give rise to security breaches. Ultimately, the bank IS are at a crossroads, while management teams must make more informed decisions, and IT staff should improve service and communication regarding system security. With this, facility managers must be mindful of the incompleteness of even modern tools, and research and implementation efforts should be conducted periodically. Future research and development should be ever-vigilant to monitor these threats, assess the potential for changes in IS technology and practices, and discern the most effective methods for adopting and managing change.

REFERENCES

Aberdeen Group, (1998), *Evaluating the Cost of Ownership for Digital Certificate Projects*. Boston: Aberdeen Group.

Abu-Musa, A. A. (2001), Evaluating The Security of Computerized Accounting Information Systems: An Empirical Study on Egyptian Banking Industry", *PhD. Thesis*, Aberdeen University, UK.

Abu-Musa, A. A. (2003), "The Perceived Threats to the Security of Computerized Accounting Information Systems", *The Journal of American Academy of Business, Cambridge, USA*, Vol. 3, No.1, September, pp. 9- 20.

Abu-Musa, A. (2010), 'Information security governance in Saudi organizations: an empirical study', *Information Management & Computer Security*, vol. 18, no. 4, pp.226 – 276.

Alfawaz, Salahuddin and Nelson, Karen and Mohannak, Kavoos (2010) Information Security Culture: a behavior compliance conceptual framework. in: Australasian

Alfuraih, F. (2008), 'E-commerce and E-commerce Fraud in Saudi Arabia: A Case Study', [Online] *2008 International Conference on Information Security and Assurance*. Available at: http://ipac.kacst.edu.sa/eDoc/eBook/3513.pdf [Accessed 17th Feb. 2011].

Alhir, S. 1998. *UML in a Nutshell*. Cambridge: O' Reilly.

Alnatheer, Mohammed and Nelson, Karen (2009) A Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context. Proceedings of the 7th Australian Information Security Management Conference. Available online: http://igneous.scis.ecu.edu.au/proceedings/2009/aism/AISMProceedings.pdf

Anderson, R. J. (1996), "From Critics to Coaches", *Bank Management,* (May / Jun.), pp. 26-32.

Anderson, R. J. 1994. *Whither Cryptography. Inf. Management & Com. Security*, Vol. 2, No. 5, pp. 13–20.

Anderson, R. J., Kuhn, M. 1996. *Tamper Resistance — a Cautionary Note*. The 2nd USENIX Workshop on E-commerce Proceedings, pp. 1–11. Berkley: USENIX.

Anderson, R. (2002), 'A security policy model for clinical information systems', [Online] Proceedings of the 1996 IEEE Symposium on Security and Privacy. Available at: http://www.cl.cam.ac.uk/~rja14/Papers/oakpolicy.pdf [Accessed 27th Dec. 2010].

ANSI, 1998. The Elliptic Curve Digital Signature Algorithm (ECDSA). X9.62 standard. Washington, DC: ANSI.

Arce, I., 2002. *Bug Hunting: The Seven Ways of the Security Samurai. Security & Privacy Supplement to IEEE Computer,* pp. 11–15.

Aresenault, A. et al., 2002. Internet X.509 Public Key Infrastructure Roadmap. PKIX Draft Standard. Reston: IETF.

ASC X12, 2001. X12 Standard Release 4050. Washington, DC: ANSI.

Baker & Mc Kenzie, 2002. Global E-Commerce Law. http://www.bmck.com/ecommerce/intlegis-t.htm. Chicago: Baker & Mc Kenize.

Bell, D. and La Padula, L., 1973. Secure Computer Systems: Mathematical Foundations. *ESD-TR-73-278. Washington, DC: MITRE Corp.*.

Bellamy, C., Perri, G., and Raab, C. (2005), 'Joined-up government and privacy in the United Kingdom: managing tensions between data protection and social policy', *Public Administration*, vol. 83, no. 2, pp. 393-415.

Broder, J.F. 2000. *Risk Analysis — The Security Survey*. Woburn: Butterworth- Heinemann.

BSI 1999, Code of practice for information security management. British Standard 7799. London: British Standards Institute.

Burrows, M., Abadi, M., Needham, R. 1990. Logic of Authentication. *ACM Transactions on Comp. Systems,* Vol. 8, No. 1, pp. 18–36.

Carlson, T. (2001), “Information Security Management: Understanding ISO 17799”, Lucent Technologies Worldwide Services, Available online: http://www.netbotz.com/library/ISO_17799.pdf

Carnevale, W. (2003), "Awareness of Computer-Security Threats Is Still Inadequate", *Chronicle of Higher Education*, (Vol. 50, Iss. 12), pp. 30 - 32.

Cheswick, W., Bellovin, S. 1994. *Firewalls and Internet Security*. Reading: Addison-Wesley.

COBIT Steering Committee 1998. Executive Overview (2nd ed.). Rolling Meadows: Information Systems Audit and Control Foundation.

Coffin, R. G. and C. Patilis (2001), "The Internal Auditor's Role in Privacy", *Internal Auditing,*

Collier, P., R. Dixon and C. Marston (1991), "The Role of Internal Auditor in the Prevention and Detection of Computer Fraud", *Public Money and Management,* winter, pp. 53 - 61.

Collis, J. and Hussey, R. (2003), *Business Research: A Practical Guide for Undergraduates and Post-graduates Students, 2nd Edition*; Palgrave Macmillan, Basingstoke, Hampshire, England, UK.

Communications and Information Technology Commission (CITC) (2005), ‘Saudi Arabia - Towards the Information Society’, [Online] http://www.yesser.gov.sa/ar/mediacenter/DocLib1/ksa_to_information_society.pdf [Accessed 17th Feb. 2011].

Compliances Forum (2008), ‘Number institution that adopt ISO 27000 by country’, [Online] Available at: http://www.compliancesforum.com/number-institution-adopt-iso-27000-country [Accessed 9th Mar. 2011].

Corbitt, T. (1996), "Stop, Thief", *Accountancy Age,* (Feb), p. 20.

Crocker, D.H. 1982. Standard For The Format Of Arpa Internet Text Messages. RFC 822. Reston: IETF.

Crosman, P. (2010), 'Botnet Affecting 2,500 Organizations Discovered', [Online] UBM TechWeb. Available at: http://banktech.com/risk-management/showArticle.jhtml?articleID=223000070&_requestid=166450 [Accessed 28th Dec. 2010].

Daud, N., Mamud, N., and Aziz, S. (2011), 'Customer's Perception Towards Information Security in Internet Banking System in Malaysia', *Australian Journal of Basic & Applied Sciences*, vol. 5, no. 9, pp. 101-112.

Davis, C. E. (1996), "Perceived Security Threats to Today's Accounting Information Systems: A Survey of CISAs", *IS Audit & Control Journal,* vol. 3, pp. 38-41.

Davis, C. E. (1997), "An Assessment of Accounting Information Security", *The CPA Journal*, New York (Vol. 67, Iss. 3), pp. 28 - 34.

De Vaus, D.A. (1985) *Surveys in Social Research*, Allen and Unwin, Leonards, NSW, Australia.

Deloitte, T., Tohmatsu. (2005). Global security survey.

DeMaio, H. 2002. Global Trust, Certification and (ISC)2. *Computers & Security* Vol. 21, No. 8, pp. 701–704.

Devargas M.,1999. Survival is Not Compulsory. Elsevier, *Computers & Security*, Vol. 18, No. 1, pp. 35–46.

Devetak, G. 1995. Organization of marketing and marketing information system. Organization and information systems. Aedermannsdorf: Scitec Publications.

Dhillon, G. (1999), "Managing and controlling computer misuse", *Information Management & Computer Security,* (Vol. 7, Number 4), PP. 171-175.

Dhillon, G. (1999). Managing and controlling computer misuse. Information Management & Computer Security, 7(4), 171-175.

Dhillon, G. (2001). Violation of safeguards by trusted personnel and understanding related information security concerns. Computers & Security, 20:165{172.

Dhillon, G., Tejay, G., and Hong, W. (2007). Identifying governance dimensions to evaluate information systems security in organizations. Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS'07), computer security,IEEE.\

Dhillon, G. and Torkzadeh (2006). Value-focused assessment of information system security in organizations. Information Systems Journal, 16:293{314.

Dichter, M.S., Burkhardt, M.S. 2001. Electronic Interaction in the Workplace: Monitoring, Retrieving and Storing Employee Communications. Age. Publications and Seminars. New York: Morgan & Lewis Counselors.http://www.morganlewis.com/art61499.htm.

Dickinson (1990), *Statistical Analysis in Accounting and Finance*, Philip Allan, London.

Dierks, T., Allen, C. 1999. Transport Layer Security. Standard RFC 2246. Reston: IETF.

Doost, R. K. (1990), "Accounting Irregularities and Computer Fraud", *National Public Accountant,* (Vol. 35 Iss. 5), pp. 36 - 39.

Dougan, J. (1994), "Internal Control Checklist for Hospitality Computer Systems", *Bottom Line*, (Vol. 9, Iss. 5), pp. 8 - 11.

Dreben, R.N., Werbach, J.L. 1999. Top 10 Things to Consider in Developing an Electronic Commerce Web Site. Publications and Seminars. New York: Morgan & Lewis Counselors. http://www.morganlewis.com/art8999.htm.

Eastlake, D., Jones, P. 2001. Secure Hash Algorithm — 1. RFC 3174 Standard. Reston: IETF.

EDPACS (1992), "A major International Organization Ignores Computer Security", *EDPACS: The EDP Audit, Control, & Security Newsletter,* (Vol. 20, Iss. 4), pp. 18-19.

EU, 1998. Data Protection Directive. Directive 1998/46/EC, Official Journal of the European Communities. Brussels: November: 1995.

EU, 1999. Electronic Signature Directive. Directive 1999/93/EC, Official Journal of the European Communities. Brussels: December: 1999.

EU, 2000. Directive on Electronic Commerce. Directive 2000/31/EC, Official Journal of the European Communities. Brussels: June 2000.

EU, 2001. Directive on Privacy and Electronic Communications. Directive 2002/58/EC, Official Journal of the European Communities. Brussels: July 2002.

Feeney, K. (1993), "How to Deal with Computer Fraud", *Connecticut CPA Quarterly*, (March), pp. 10-11.

FFIEC (1996) *IS Examination Handbook, Chapter, 14, Security- Physical And Data.*

Fishbein, M. and Ajzen, I. (1975). Belief, attitude, intention and behavior: an introduction to theory and research. Addison-Wesley, Reading, MA.

Foti, J. (Ed.) 2001. Advanced Encryption Standard. FIPS Draft. Washington, DC: DoC.

Foundation for Intelligent Physical Agents (2001). FIPA Security SIG Request For Information. F-OUT-00065 Deliverable. Concord: FIPA.

Freed, N. 1996. Multipurpose Internet Mail Extensions. RFC 2045 Standard. Reston: IETF.

Freier, A.O., et al. 1996. Secure Sockets Layer Protocol (version 3). Mountain View: Netscape Corp. http://wp.netscape.com/eng/ssl3/index.html.

French, A. (2012), ‘A Case Study on E-Banking Security -- When Security Becomes Too Sophisticated for the User to Access Their Information’, *Journal of Internet Banking & Commerce*, vol. 17, no. 2, pp. 1-14.

Fumy, W., 2000. From Common Criteria to Elliptic Curves — ISO / IEC JTC 1/SC 27, IT Security Techniques. *ISO Bulletin*, no. 6, pp. 20–25.

Gong, L., Needham, R., Yahalom, R., 1990. Reasoning about Belief in Cryptographic Protocols. Proc. of the IEEE Computer Society Symposium on Research in Security and Privacy, pp. 234–248. Los Alamitos: IEEE Press.

Grance, T., Hash, J., Stevens, M. (2004), ‘Security Considerations in the Information System Development Life Cycle’, [Online] National Institute of Standards and Technology. Available at: http://www.tulane.edu/~infosec/NIST/NIST-SP800-64.pdf [Accessed 27th Dec. 2010].

Gratton, C. and Jones, I. (2004), *Research Methods for Sport Studies,* Routledge, London, UK.

Green, M. (2003), "Securing the System", *Best's Review*, (Vol. 103, No. 10), pp. 80 - 84.

Group on the Next Generation Internet Policy, 2000. e-Japan Initiative. Tokyo: GNGIP.

Grundy, E., Collier, P. and S., Barry (1994), "Auditing Personnel: A Human Resource Approach to Information System Control", *Managerial Auditing Journal,* (Vol. 9), pp. 10-16.

Gutmann P., 2002. PKI: It’s Not Dead, Just Resting. *IEEE Computer*, Vol. 35, No. 8, pp. 41–49.

Harmon, P., 2001. *Developing E-Business Systems and Architectures*. San Francisco: Morgan Kaufman.

Haugen S. and J. R. Selin (1999), "Identifying and Controlling Computer Crime and Employee Fraud", *Industrial Management and Data Systems*, (Vol. 99, Iss. 8).

Hendry, M., 1997. *Smart Card Security and Application*. London: Artech House.

Hermanson, D. R.; M. C. Hill; and D. M. Ivancevich, (2000) "Information Technology-Related Activities of Internal Auditors", *Journal of Information Systems,* (Supplement, Vol. 14, Issue 1), pp.39-53.

Hessler R. M, 1992, Social Research Methods, West Publishing Company, New York, USA.

Holzmann, J.G., 1991. *Design and validation of computer protocols*. London: Prentice Hall.

Hood, K. L. and J. Yang (1998), "Impact of Banking Information Systems Security on Banking in China: The Case of Large State-Owned Banks in Shenzhen Economic Special Zone - An Introduction", *Journal of Global Information Management,* (Vol. 6, No. 3), pp. 5 - 15.

Hunker, J., 2002. Policy challenges in building dependability in global infrastructures. Elsevier Science, *Computers & Security*, Vol. 21, No. 8, pp. 705–710.

Hunton, J.; A. Wright; and S. Wright, (2005) "Business and Audit Risks Associated With ERP Systems: Knowledge Differences between Information Systems Audit Specialists and Financial Auditors", *Journal of Information Systems*, Forthcoming.

Information Security Conference (AISC), 2010, Brisbane, Australia. QUT Digital Repository. Online available t: http://eprints.qut.edu.au/29221

Internal Auditor, (Vol. 47 Iss. 4), pp. 26 - 33.

IsecT Ltd. (2011), 'ISO 27001 Security Home', [Online] Available at: http://www.iso27001security.com/index.html [Accessed 9th Mar. 2011].

ISO, 1994. IT — Identification Cards. IS 7816 / 1thru 10. Geneva: ISO.

ISO, 1995a. IT, OSI: Security Frameworks in Open Systems. IS 10181 / 1 thru 7. Geneva: ISO.

ISO, 1995b. Quality Systems. Standards IS0 9001 thru 9003. Geneva: ISO.

ISO, 1997. Quality Management and Quality System Elements. Standards IS0 9004 / 1 thru 2. Geneva: ISO.

ISO, 1999. Common Criteria, Security techniques — Evaluation criteria for IT security. IS 15408, parts 1 thru 3. Geneva: ISO.

ISO, 2000. Code of practice for inf. sec. management. ISO 17799 Standard. Geneva: ISO.

ISO, 2002. Z formal specification notation. FDIS 13568. Geneva: ISO.

ISO 27000 Directory (2007), 'Download Destinations', [Online] Available at: http://www.27000.org/countries.htm [Accessed 9th Mar. 2011].

Issociate (2007), ‘ISO 27001 and ISO 27002 Newsletter: Issue 16 Published’, [Online] Available at: http://www.issociate.de/board/post/460244/ISO_27001_and_ISO_27002_Newsletter:_Issue_16_Published.html [Accessed 9th Mar. 2011].

ITU-T, 1997c. IT — Open Systems Interconnection — The Directory: Overview of concepts, models and services. Recommendation X.500. Geneva: ISO.

ITU-T, 2000. Public-key and attribute certificate frameworks. X.509 Standard. Geneva: ISO.

Jenkins, B., P. Cooke and P. Quest (1992), *An Audit Approach to Computers*, Institute of Chartered Accountants In England And Wales, London.

Katz, D. (2000), "Elements of a Comprehensive Security Solution", *Health Management Technology,* (Vol. 21, Iss. 6), pp. 12-16.

Katzenbeisser S., Petitcolas F.A.P., 1999. *Information hiding techniques for steganography and digital watermarking*. London: Artech House.

Kemmerer, R.A., Vigna, G., 2002. Intrusion Detection: A Brief History and Overview. *IEEE Computer*, Security & Privacy, Vol. 35, No. 5, pp. 27–30.

Kocher, P., Jaffe, J., Jun, B., 2000. Differential Power Analysis, White paper. San Francisco: Cryptography Research Inc.

Koops, B.J., 2001. Crypto Law Survey. http://rechten.kub.nl/koops/cryptolaw.

Koskosas, Ioannis V. (2009) Communicating Information Systems Goals: A Case in Internet Banking Security. Department of Information and Communication Technologies Engineering. University of Western Macedonia. Kozani, Greece. Online available at: http://www.doiserbia.nb.rs/img/doi/1820-0214/2009/1820-02140901071K.pdf

KPMG (2000), *Information Security Survey 2000, Executive Summary*, April, KPMG, London.

Kumar, M., Agrawal, R., and Chauhan, D. (2013), ‘Safe as a Bank: Iris Scan Biometrics for Secure Data Access’, *Global Finance*, vol. 27, no. 5, pp. 16-19.

Leinicke, L. M.; W. M. Rexroad and J. D. Ward (1990), "Computer Fraud Auditing: It Works",

Levi, P. (1993), "PC security for accountants - What's Hot and What's New", *Accounting Technology,*

Likar, B., 2001. Inoviranje. Koper: College of Management.

Loch, K. D., Houston H. C. and M. E. Warkentin (1992), "Threats to Information Systems: Today's Reality, Yesterday's Understanding", *MIS Quarterly,* (June), pp. 173 - 186.

Mactaggart M., 2001. Enabling XML security. http://www-106.ibm.com/developerworks/xm. New York: IBM.

Mar/Apr., (Vol.16, Iss.2), PP. 22-28.

Marshall, C. and Rossman, G. (2006) *Designing Qualitative Research*, 4th Edition; Sage Publications, Thousand Oaks, CA. USA

Mau, S. and J. Catlin (1993), "Systems Security in 90's", *Interpreter*, (January), pp. 8-9.

Mclean, G. (2000), "The New Age of Bank Security", *Canadian Banker*, (Vol. 107, Iss. 4), pp. 14 - 19.

Meall, Lesley (1992), "Computer Crime: Foiling the Fraudsters", *Accountancy,* (November), pp. 56 57.

Melville S and W. Goddard (1996) *Research Methodology: An Introduction for Science and Engineering Students*, Juta and Co. Ltd, Kenwyn.

Merriam, S. (1988) *Case Study Research in Education: A Qualitative Approach*, Jossey-Bass, San Francisco, CA., USA.

Miller, D. C. (1991) *Handbook of Research Design and Social Measurement,* (Fifth Edition), SAGE Publications, London.

Miller, S.K., 2001. Facing the Challenge of Wireless Security. *IEEE Computer*, Vol. 35, No. 7, pp. 16–18.

MobileActive (2010), 'BlackBerry Messenger Ban: Hand Us Encryption Code or Face Ban', [Online] Available at: http://www.mobileactive.org/blackberry-messenger-ban [Accessed 28th December 2010].

Moss, N. (1996), "Banks at Mercy of Hackers", *The European*, October 10, N.335, p. 24.

Muhaya, F. (2010), 'An Approach for the Development of National Information Security Policies', [Online] *International Journal of Advanced Science and Technology* Vol. 21, Available at: http://www.sersc.org/journals/IJAST/vol21/1.pdf [Accessed 19 Feb. 2011].

Myler, E., and Broadbent, G. (2006), "ISO 17799: Standard for Security", *Information Management Journal*, Vol. 40, No. 6, pp. 43-52.

National Archives (2010), 'Data Protection Act 1998', [Online] Available at: http://www.legislation.gov.uk/ukpga/1998/29/contents [Accessed 28th Dec. 2010].

National Institute of Standards and Technology (1995), Technology Administration, U.S. Department of Commerce, *An Introduction to Computer Security: The NIST Handbook*, Special Publication 800 12. October 1995

National Institute of Standards and Technology (2003), Computer Security Division, Information Technology Laboratory, *Standards for Security Categorization of Federal Information and Information Systems,* Initial Publication Draft, Version 1.0, May.

NSI (2006), 'IT Security', [Online] Available at: http://www.issociate.de/board/post/460244/ISO_27001_and_ISO_27002_Newsletter:_Issue_16_Published.html [Accessed 9th Mar. 2011].

OECD (Organization for Economic Co-operation and Development) (1992), *Guidelines for the Security of Information Systems,* The Council of the OECD, 26 November.

OECD, 1997. Guidelines for Cryptography Policy. Paris: OECD.

OECD, 1998. Implementing The OECD ”Privacy Guidelines” In The Electronic Environment: Focus On The Internet. Paris: OECD.

OMG, 2001. Unified Modeling Language, v 1.4. Needham: OMG.

Parker, D. B. (1976), *Crime By Computer*, Charles Scribner's sons, New York.

Powers, D.M., 2001. *The Internet Legal Guide: Everything you need to know when doing business online*. New York: John Wiley & Sons.

Presser, S., Rothgeb, J., Couper, M. et al. (2004) *Methods for Testing and Evaluating Survey Questionnaires*, John Wiley and Sons Publications, Inc., Hoboken, NJ., USA.

Qureshi, A. A. and J. G. Siegel (1997), "The Accountant And Computer Security", *The National Public Accountant*, Washington, May, vol. 43, no. 3, pp. 12-15.

Raepple, M., 2001. *Sicherheitskonzepte fuer das Internet*. Heidelberg: dpunkt-Verlag.

Ramsdell, B., 1999. *S/MIME Message Specification. Standard RFC 2633*. Reston: IETF.

Rao, A., Rathan, M., Srinivas, Y., Vijayasekhar, J., Krishna, N., Jaliparthi, R., Shekhar, V., Saggurthi, V., and Rani S. (2012), ‘A Note on Quantum Cryptography’, *International Journal on Computer Science & Engineering*, vol. 4, no. 9, pp. 1540-1544.

Rockwell, R. (1990), "The Advent of Computer Related Crimes", *Secured Lender*, (Jul /Aug), pp. 40 - 42

Roe, M., 1993. CA Requirements. PASSWORD Project R. 2.5 document. Cambridge: Cambridge University.

Roufaiel, N. S. (1990), "Computer Related Crimes: An Educational And Professional Challenge", *Managerial Auditing Journal*, (Vol. 5, Iss. 4), pp. 18 - 25.

RSA Labs, 2002. PKCS — RSA Cryptography Standard, v 2.1. Bedford: RSA Security.

Ryan, S. D. and B. Bordoloi (1997), "Evaluating Security Threats in Mainframe and Client / Server Environments", *Information & Management*, (Vol. 32, Iss. 3), pp. 137 - 142.

Sander, T., Tschudin, C.F., 1998. Protecting Mobile Agents Against Malicious Hosts. Mobile Agent Security, LNCS 1419. Heidelberg: Springer Verlag.

Sandilya, B. (2012), ‘IT and equities operations: 12 best practices’, *Journal of Securities Operations & Custody*, vol. 4, no. 4, pp. 358-363.

Saudi Gazette (2007), ‘Saudi Firms Need to Improve Information Security’ [Online] Retrieved from: http://www.saudigazette.com.sa/index.php?option=co m_content&task=view&id=28541&Itemid=115 [link currently unavailable] Available at: http://www.saudielection.com/en/forum/showthread.php?p=6951 [Accessed 17 Feb. 2011].

Saunders, M., Lewis, P. and Thornhill, A. (2007) *Research Methods for Business Students*, Prentice-Hall, Inc., Upper Saddle River, NJ., USA.

Schneier, B., 1996. *Applied Cryptography*. New York: John Willey & Sons.

Schultz, E. E. (2002), "A Framework for Understanding and Predicting Insider Attacks", Computers & Security, (Vol. 21, Iss. 6), pp. 256 - 531.

Schweitzer, J. A. (1987), *Computers, Business, and Security*, Butterworth Publishers, London.

Security Awareness Index Survey. (2002). Retrieved June 15, 2009, from http://www.netiq.com/news/releases/release.asp?cid=20021213144711QDNH

Siponen, M. T. (2000), "A conceptual Foundation for Organizational Information Security Awareness", *Information Management and Computer Security*, Bradford, (Vol. 8, Iss. 8), PP. 31- 44.

Siponen, M. (2000). Critical analysis of different approaches to minimizing user-related faults in information systems security: implications for research and practice. Information Management & Computer Security, 8(5):197{209.

Siponen, M. and Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. SIGMIS Database, 38(1):6080.

Siponen, Mikko; Mahmood, M. Adam; and Pahnila, Seppo. (2009). Technical Opinion: Are Employees Putting Your Company at Risk by Not following Information Security Policies. Communications of the ACM. Vol. 52, Issue 12, December 2009.

Smith, L. B. (1995), "On The New Beat", *PC Week,* (October30) (Vol. 12, No. 43), pp. E1-2.

Stallings, W., 1999. *Cryptography and Network Security*. London: Prentice Hall.

Stamp, M. (2006), *Information Security: Principles and Practice*. New York: John Wiley and Sons.

Straub, D., Goodman, S., and Baskerville, R. (2008), *Information security: policy, processes, and practices*. Armonk, New York: M.E. Sharpe.

Swann, J. (2004), "Always on the Case: Engaging your Staff in Bank Security", *Community Banker*, (March, Vol. 13, Iss. 3), pp. 44 - 47.

Syverson, P., van Oorschot, P., 1994. On Unifying Some Cryptographic Protocol Logic. Proc. of the Symposium on Security & Privacy, pp. 14–28. Oakland: IEEE.

Teller Vision. (2013), ‘New Cyber Security "Rules of the Road" for the Financial Services Industry’, *Teller Vision*, no. 1428, pp. 2-3.

Thayer R., et al., 1998. IP Security Document Roadmap. RFC 2411. Reston: IETF.

Trèek, D. et al., 2001. Slovene smart card and IP based health-care information system infrastructure. *International journal of medical informatics*. Vol. 61, pp.33–43. Amsterdam: Elsevier.

UN Economic Commission for Europe, 1993. Electronic Data Interchange for Administration, Commerce and Transport — Syntax Rules. ISO 9735. Geneva: ISO.

UNCITRAL, 1996. Model Law on Electronic Commerce. http://www.uncitral.org/english/texts/elect-com/ecommerceindex.htm. Vienna: UNCITRAL.

UNCITRAL, 2001. Model Law on Digital Signatures. http://www.uncitral.org/english/texts/elect-com/ecommerceindex.htm. Vienna: UNCITRAL.

United Nations (2007), ‘National Profile of the Information Society in the Kingdom of Saudi Arabia’, [Online] Available at: http://www.escwa.un.org/wsis/reports/docs/KSA-07-E.pdf [Accessed 17 Feb. 2011].

United States General Accounting Office (GAO) (2003), *Information Security: Computer Controls over Key Treasury Internet Payment System*, Report to Congressional Requesters, July.

US Congress, 1998. Digital Millennium Copyright Act. H. R. 2281, Public Law 105-304. Washington D.C.: January 1998.

Wackerly, D. D., W. Mendenhall and R. L. Scheaffer, (1996) *Mathematical Statistics with Applications*, Duxbury Press, Wadsworth Publishing Company, London.

Warren, M. J. (2002), Security practice: survey evidence from three countries, *Logistics Information Manageme*, (Vol. 15, Iss. 5/6), PP. 347-351.

Weingartner, A. and M. Burton (1991), "PC Security - Don't Be Caught Out", *Computer Security Guide*, pp. 33 - 35.

Wells, J. (2007), ‘Defence in Depth: Strategies for Information Security’, [Online] Oakwood. Available at: http://www.oakwoodsys.com/collaboration/Documents/Defense%20in%20Depth%20-%20Strategies%20for%20Information%20Security.pdf [Accessed 27th Dec. 2010].

White, Gayle Webb and Sheila J Pearson (2001), "Controlling corporate e-mail, PC use and computer security"; *Information Management & Computer Security*, Vol. 9, Iss. 2/3; pp. 88-93.

Williams, P. (1995), "Safe, Secure And Up To Standard", *Accountancy,* p. 60.

WIPO, 2000. Primer On E-commerce And Intellectual Property Issues. Geneva: WIPO.

Wood, C. C. and W. W. Banks (1993), "Human Error: An Overlooked but Significant Information Security Problem", *Computers & Security*, (Vol. 12, Iss. 1), pp. 51 - 60.

Wright, S. and A. Wright (2002), Information system assurance for enterprise resource planning systems: Implementation and unique risk considerations, *Journal of Information Systems*, Vol. 16, Supplement, pp. 99-113.

Wysocki, R.K., DeMichiell, R.L., 1997. *Managing Information Across the Enterprise*. New York: John Willey & Sons.

von Solms, B. and von Solms, R. (2004). The 10 deadly sins of information security management. computers and security. Computers and Security, 23:371{376.

Vroom, C. and von Solms, R. (2004). Towards information security behavioral compliance. Computers & Security, 23(3):191{198.

Zurich (2008), ‘Strategies for managing information security risks’, [Online] Available at: http://helppointdelivered.com/internet/zna/SiteCollectionDocuments/en/media/inthenews/strategiesformanaginginformationsecurityrisks.pdf [Accessed 27th Dec. 2010].

Appendices

Appendix A: Questionnaire

FOR YOUR PROTECTION, ALL INFORMATION OBTAINED WILL BE RESPECTED WITH THE STRICTEST CONFIDENTIALITY. NO NAMES WILL BE RECORDED, AND NO PERSONAL INFORMATION WILL BE SHARED.

Demographic Information

Age:

Gender:

Organisation:

Position:

Time Served at Organisation:

Questionnaire

1) Please rate the level of threat severity to information system security you are currently experiencing, on a scale of 1-10 (with 10 denoting the highest threat level).

2) Is the level indicated in 1) typical? Yes No

3) Please rate the average level of threat severity to information system security you are currently experiencing, on a scale of 1-10 (with 10 denoting the highest threat level).

4) How often is information system security addressed by management in your facility?

5) Are routine upgrades made to software and hardware?

6) Are policies and procedures routinely updated?

7) How effective do you rate the policies and procedures, on a scale of 1-10?

8) In terms of "routinely," "occasionally," or "never," how often are information systems security examined and tested?

9) In terms of "routinely," "occasionally," or "never," how often are employees trained or provided with additional education regarding IS systems?

10) In terms of "excellent," "good," "average," or "poor," how well do managers follow information security policies and procedures?

11) In terms of “excellent,” “good,” “average,” or “poor,” how well do employees follow information security policies and procedures?

12) What is the primary reason that managers may not follow policy?

13) What is the primary reason that employees may not follow policy?

14) Are you aware of any threats that are unique to your institution? Yes No

15) What is the nature of this threat?

16) Are you aware of any threats that are unique to your sector? Yes No

17) What is the nature of this threat?

18) Do you feel personal ethics play a role in managers’ compliance? Yes No

> If there is any reason you wish to explain why you chose ‘Yes’ or ‘No’, your opinion will be taken into consideration:

19) Do you feel personal ethics play a role in employees’ compliance? Yes No

> If there is any reason you wish to explain why you chose ‘Yes’ or ‘No’, your opinion will be taken into consideration:

20) Do you feel information system security is an area which requires more attention in your institution? Yes No

> If there is any reason you wish to explain why you chose ‘Yes’ or ‘No’, your opinion will be taken into consideration:

21) Do you feel information system security is an area which requires more attention in your sector? Yes No

> If there is any reason you wish to explain why you chose ‘Yes’ or ‘No’, your opinion will be taken into consideration:

22) Please name the improvements you feel should be made to managerial functions regarding information security.

____

____

23) Please name the improvements you feel should be made to compliance policy regarding information security.

____

____

____

24) Do you feel employees should be required to undergo additional training regarding information system security? Yes No

25) Do you feel company representatives should devote more effort to information system security and threat awareness?

26) Is the level of information system security technology adequate in your institution? Yes No

27) Please rate the adequacy, on a scale of 1-10, of information systems security technology.

For items 28-30, please rate how important you feel the following topics are in your institution.

28) Information Systems:

29) Information System Security:

30) Information System Security Policy:

Thank you for your participation! Your information will be kept confidential and used in an academic study aimed at informative observation and improvements.

(to be completed by researcher)

Organisation:

Annual turnover:

Number of employees:

Size of IT/IS department:

Appendix B: Interview Transcripts
Riyad Bank Employees (2)

Question 1: ("*What do you feel is the biggest concern for information system security in Saudi Arabia*?")

Response 1: One of the most noticeable concerns experienced often here are viruses and internet security. But, the biggest concern overall is hacking, because of course breaching the system can cause a great amount of damage.

> "What do you feel is the most relevant concern?"
>
> Response: The potential for private technology to exceed internal technology.

Response 2: The biggest nation-wide concern is the growth and use, or misuse, of technology. Mobile technology is a particular concern, and is known to be a threat to bank security in Saudi Arabia.

Question 2: ("*What do you feel is the biggest concern for information system security in your organisation, and do you see variations in concerns between departments?*")

Response 1: We feel very secure compared to the rest of the nation, but our organisation has experienced the most problems with firewall breaches and acquiring viruses. There are problems on our networks more often than projected, and this is evident across all departments.

Response 2: The biggest concern for information system security is always protecting the network, and at this point in time, the most vulnerable technology is the firewall and security software. We hope that both improvements in available software take place at a rate faster than those would wish to break into the network can develop hacking methods, and that we continue to have access to defence technology within a fair amount of time once it becomes available.

Question 3: ("*How do you think concerns can be addressed within the nation, and do you feel your organisation could address the concerns differently*?")

Response 1: There is not much that can be done to address concerns in the nation, organisations can only attempt to access security technology through their own investments. The government can attempt to improve aspects of the public sector, but even with increased resources, this alone would not have the impact on private banking needed for information systems to be directly comparable to those in the US or UK. Our organisation has tried to allocate funds differently for improvements, with mixed results.

Response 2: The nation has tried to address concerns, and as it seems to be trying nearly as hard as possible, progress will likely remain at a steady rate. Improvements have been made, and are continually made, and considering these facts there is little that can be done differently at this point in time.

Question 4: ("*Do you feel that employees and managers need to improve their levels of compliance, and if so, do you see greater compliance in either employees or managers?*")

Response 1: Yes, that is one of the biggest correctable problems that can be seen, but unfortunately concern is also low so little has been done. The best way to make improvements here is through awareness and change management processes. Managers have seemed to be more compliant overall in recent years, but instances of non-compliance have more commonly been greater deviations from what is expected. Of course the nature of management positions involves greater power, so non-compliance is more likely to be more serious in nature. Non-management or 'normal' employees are more commonly non-compliant, but these instances are also more likely less serious.

Response 2: Undoubtedly, compliance has been and continues to be an issue of concern and focus. Managers and employees alike should make sure they are following procedures, but when a manager chooses to be non-compliant in areas related to information systems and security, the results have a greater tendency to be more serious. Managers generally feel that they are 'above' policies and obligation, while employees seem to think they have a greater chance of avoiding detection if they choose to take shortcuts.

Question 5: ("*Does it appear that major reforms are needed within any policies concerned with information security threats?")*

Response 1: I would say reforms are needed in many areas, but that the level of reform needed is normal and changes are always needed. I wouldn't say any 'major' reforms are needed.

Response 2: Change and change management must be emphasised so the organisation can change as needed, and as the company has been successful in security and operation, I do not think 'major reforms' are needed.

Question 6: ("*Are ethics an issue in managers and employees, and if so, what can be done?*")

Response 1: Ethics is always an issue, it is almost a timeless issue, and in that sense, there is little that can be done. Greater incentives and greater consequences can help to insure compliance and ethics remain in all parts of information, security, and operation, but it seems as if it will always still be an issue.

Response 2: Ethics are of course responsible for many non-compliant actions, as well as general actions at work, but it does not seem like much more can be done. The actions already taken have helped with issues in the past, and we can only hope that ethical issues observed now continue to be observed in information security as well as elsewhere.

Question 7: ("*Should there be a greater strive to improve technology within the organisation, and assuming this is always desired, what seems to be the best course of action?*")

Response 1: In my personal opinion information systems and security should have the greatest strive to upgrade technology virtually wherever possible, in an institution like this one. There does not seem to be any real strategy to this, aside from gaining the profits required while ensuring that profits dedicated to technological improvement do not negatively affect other areas.

Response 2: Yes, there should always be a greater strive to technology within our company and others like it. Without that, the threats from those outside that do strive for technology would be incredibly great, with the organisation at great risk.

Question 8: ("*If resources and time were no object, what changes would be most viable and effective?*")

Response 1: Improving hardware and software to top-of-the-line products, then giving the network the best design and security measurable known.

Response 2: Replacing all of the current technology, and then ensuring it is properly supervised, maintained, and upgraded by employees.

Question 9: ("*How do you feel that security-related training should be approached in the future?*")

Response 1: Training sessions should be more involved and given more often.

> "How often do you feel that is necessary?"
>
> Response: that is hard to say, because routine training would offer more while 'as-needed' training sessions may run into similar problems. I would guess every six months, with cancelled sessions if no significant updates have been made, would be ideal.

Response 2: With more consideration given to available technological improvements, outside of the nation as well as within it.

Question 10: ("*Are there any other changes you feel are required to minimise threats to information systems?")*

Response 1: Improved organisation and leadership may help, but that is just theoretical of course, and no paths to such major improvements have been successfully implemented in the past nor appear to be realistically possible now. Companies with this level of success are content though, with security as well as performance.

Response 2: Not really, no. While security could be better, there does not appear to be any real critical threats at the present time.

Al-Rajhi Bank Employees (2)

Question 1: ("*What do you feel is the biggest concern for information system security in Saudi Arabia*?")

Response 1: The biggest concern is the possibility for threats from commercially available technology. People have equal or even greater access to technology that is capable of breaching security, and if it were capable of doing so undetected, there would already be a serious problem.

Response 2: That would be the rates of development, development continues but threats develop at a rate more comparable to developed nations, while internal technology is slightly behind.

Question 2: ("*What do you feel is the biggest concern for information system security in your organisation, and do you see variations in concerns between departments?*")

Response 1: The biggest concern within the organisation is the availability and use of software. Ensuring that the best software is found, updated to address new threats, and otherwise used properly seems to be the greatest concern within the organisation.

Response 2: Maintaining and improving the software. Sometimes threats can develop outside the organisation, while unknown to the information security specialists. This is a concern to all departments.

Question 3: ("*How do you think concerns can be addressed within the nation, and do you feel your organisation could address the concerns differently*?")

Response 1: The nation itself is more concerned with the economy, finance, and development. There is concern for banks, but in terms of development rather than information security. The organisation can only continue to develop in its own way, there is little ways of seeking help in the nation.

Response 2: If the overall national economy improved, then of course it would be easier to develop all departments as needed. Otherwise, organisations will have to address concerns individually.

Question 4: ("*Do you feel that employees and managers need to improve their levels of compliance, and if so, do you see greater compliance in either employees or managers?*")

Response 1: Compliance is somewhat of an issue, but not a major one. Compliance doesn't usually lead to improved threat. Managers seem to feel 'above the law,' but employees feel that there is less risk for the policies that apply to them.

Response 2: Both managers and employees should be advised regarding improved compliance, but the importance of this has not changed much over the past years.

Question 5: ("*Does it appear that major reforms are needed within any policies concerned with information security threats?")*

Response 1: No, the policies mostly seem to be okay.

Response 2: The company might benefit from policies requiring the changes we are discussing.

Question 6: ("*Are ethics an issue in managers and employees, and if so, what can be done?*")

Response 1: Ethics are always an issue, and the only things that can be done are stricter policies and consequences. New changes can also bring new opportunities for ethics to become an issue elsewhere, and it does not appear that any company has found a way to ensure ethics is no issue.

Response 2: Ethics are something that managers should be more mindful of, observing on their own and ensuring proper employee conduct. The best thing that can be done is by being selective when choosing authorities, and being mindful of their actions (and allowances) as they grow with the company.

Question 7: ("*Should there be a greater strive to improve technology within the organisation, and assuming this is always desired, what seems to be the best course of action?*")

Response 1: Security should continue to seek the best technology available yes, so long as the money is invested in truly beneficial improvements. Elsewhere in the organisation, this is more debatable. The best course of action is to simply increase profits while researching the technology on the market.

Response 2: The strive should be 'great,' but it already is, so I would not say that it should be 'greater.' The nation in general has access to effective technology, but it is slightly different than the technology available in developed nations. There is no known practical path to improving technology so that is identical.

Question 8: ("*If resources and time were no object, what changes would be most viable and effective?*")

Response 1: If resources and time were no object, the bank's network infrastructure would be remodelled using the best technology available.

Response 2: An expansion of facilities and the placement of new facilities in new locations could increase profits well enough to have an investment for the future, and this could then be used to address the areas we have discussed. That, to me, would be the most effective change and path forward.

Question 9: ("*How do you feel that security-related training should be approached in the future?*")

Response 1: It should be more in-depth, and carried out more often, so that employees are aware of what is available, in terms of both threats and defences.

Response 2: It should be more technical in nature, so that employees are more aware of the tools and features available to them.

Question 10: ("*Are there any other changes you feel are required to minimise threats to information systems?")*

Response 1: Aside from the obvious technology and network changes that could help, the company could also benefit from

Response 2: Changes to the overall company structure could help, but that is not assured.

National Commercial Bank Employees (2)

Question 1: ("*What do you feel is the biggest concern for information system security in Saudi Arabia*?")

Response 1: The biggest concern would be a combination of technological development outside of institutions needing security and a lack of awareness of general technology within the institutions.

Response 2: The largest concern is the ability to develop at a greater rate while the economy develops at a similar rate.

> "Do you think the current level of development will lead to greater issues?"
>
> Response: Not necessarily, but of course the potential is there.

Question 2: ("*What do you feel is the biggest concern for information system security in your organisation, and do you see variations in concerns between departments?*")

Response 1: The greatest concern here at the National Commercial Bank is the size of the data and funds stored, compared to the nature of upgrades and organisation. The bank attempts to address departments as needed, so there does not appear to be critical variations between departments.

Response 2: The network and some technological components are not always improved at the same rate of the bank's development, which can produce changes to threats.

Question 3: ("*How do you think concerns can be addressed within the nation, and do you feel your organisation could address the concerns differently*?")

Response 1: There is little that can be done on a national level, so the organisation could address concerns differently by applying change how it is needed and as changes become available.

Response 2: No, and yes because the organisation is capable of making changes as needed.

Question 4: ("*Do you feel that employees and managers need to improve their levels of compliance, and if so, do you see greater compliance in either employees or managers?*")

Response 1: Yes, but this is always true, it is almost human nature to some extent, but it is never plainly accepted. Managers have set examples for employees here in most relevant areas, including compliance with policies.

Response 2: In information security-related positions compliance is generally not a problem, neither within manager-based positions or normal employee positions.

Question 5: ("*Does it appear that major reforms are needed within any policies concerned with information security threats?")*

Response 1: Major reforms could better protect against threats, but policies alone do not need ‘major’ changes at this time.

Response 2: Policies requiring updates and development, including technological development, could better ensure that the organisation’s security develops on a level more comparable with the development of the technology itself, but it then would likely not be able to make decisions or have discretion. Discretion seems to be the best approach at this point, despite the possible issues with motivation and freedom stemming from it.

Question 6: (“*Are ethics an issue in managers and employees, and if so, what can be done?*”)

Response 1: Ethics are always an issue. They do not seem to be responsible for any increased threat or critical issues here, though.

Response 2: The only thing that can realistically be done about ethical problems is to examine each instance of ethical violation on a case by case basis. In information security, this seems to be less of a problem than within other areas of the bank.

Question 7: (“*Should there be a greater strive to improve technology within the organisation, and assuming this is always desired, what seems to be the best course of action?*”)

Response 1: In the organisation overall yes, but within the organisations’ security-related areas (I assume this is what you intend to ask), the existing level of ‘striving’ should simply continue. The emphasis on technological improvements in these areas is already great, and little else could be done, as far as I am aware.

Response 2: The current course of action seems effective, despite the issues in technology described in existing articles and publications, the company has not experienced major breaches or threats that seem to jeopardise the company’s integrity in any major way. It is a concern but not on a level near crises, in this organisation anyhow.

Question 8: ("*If resources and time were no object, what changes would be most viable and effective?*")

Response 1: We could always improve everything and expand, reaching more customers and being sure that all of their information is safe, and this would truly be effective. The most viable change would be to ensure employees have a higher level of education and training in the future.

Response 2: Additional paid employees providing additional labour and ideas would certainly benefit the organisation if money and wages were no object, but this is not 'viable' under normal circumstances (although it would be effective).

Question 9: ("*How do you feel that security-related training should be approached in the future?*")

Response 1: It should be more thorough and more often.

Response 2: Training should be more considerate of technical aspects and technological potential, it seems to be too general now.

Question 10: ("*Are there any other changes you feel are required to minimise threats to information systems?")*

Response 1: Not other than those discussed, none come to mind.

Response 2: Improving leadership may help… but I could not say that it actually 'required' because of the current circumstances.

Arab National Bank Employees (2)

Question 1: ("*What do you feel is the biggest concern for information system security in Saudi Arabia*?")

Response 1: The biggest concern is the English technology, which the company has a hard time 'keeping up with' and then using with the employees and customers. This is mostly in terms of software, as it is easier to ensure that the company has some of the best hardware available.

Response 2: Software is a concern from what I have seen, but I do not feel that I can speak for the whole nation.

Question 2: ("*What do you feel is the biggest concern for information system security in your organisation, and do you see variations in concerns between departments?*")

Response 1: Software and the English technology is undoubtedly a concern in the organisation, and the acts of convincing those with greater power that improvements are needed is difficult, as well as the processes of integrating and using the technology within the organisation as often as would be beneficial. This is less of a problem for security or online banking, but is a concern nonetheless.

Response 2: As I mentioned in my last response, software is a concern for the organisation, and others like it from what I have seen. This appears to be evident across all related departments, although somewhat differently as departments may rely on different software and tools.

Question 3: ("*How do you think concerns can be addressed within the nation, and do you feel your organisation could address the concerns differently*?")

Response 1: There is little that can be done on a national level, aside from national improvements which only indirectly affect the concerns you are discussing with me.

Response 2: The organisation can take actions independently of the nation, which relies on greater forces. This is both a benefit and limitation, although the company can seek help outside of the nation at times when desired.

Question 4: ("*Do you feel that employees and managers need to improve their levels of compliance, and if so, do you see greater compliance in either employees or managers?*")

Response 1: Compliance is always a concern, but is always considered, so no major improvements seem to be needed. A neglect of compliance or reviews would be bad, though. Employees seem to be more compliant, because they are more likely to lose their jobs and remain unemployed for such actions.

Response 2: Both managers and employees should improve, but managers should strive for flawless compliance.

Question 5: ("*Does it appear that major reforms are needed within any policies concerned with information security threats?")*

Response 1: No, threats become part of awareness issues and discussion when they become apparent, and actions are taken if it is determined that this is needed.

Response 2: Policies regarding training and software or network upgrades could be more demanding, but especially as discretion would be required, the changes would not really be 'major.'

Question 6: ("*Are ethics an issue in managers and employees, and if so, what can be done?*")

Response 1: Not to any substantial extent, policies and reviews should just be sure to be considerate of this and all areas.

Response 2: Ethics could improve information security defences as well as any other areas, but compliance and ethics generally do not directly affect the defence itself.

> "What areas do you observe it affecting?"
>
> Observation and maintenance, usually because the employees feel that the system or others will detect what they overlook. Despite breaching protocol, they are often correct

to a large extent.

Question 7: ("*Should there be a greater strive to improve technology within the organisation, and assuming this is always desired, what seems to be the best course of action?*")

Response 1: No, the 'strive' should continue, but it need not become greater. There is already a strong desire to improve technology wherever possible, as the people here are quite fond of it.

Response 2: The ability to improve technology could improve, but I would not consider this to be an 'increased strive' because the desire to improve technology has existed.

Question 8: ("*If resources and time were no object, what changes would be most viable and effective?*")

Response 1: Our network connections and the main software used could be improved, and more employees could be used to improve the network for security effectiveness. General information system effectiveness could be improved by hiring a team of more qualified (in technology) expert professionals to choose technology best fit for the organisation and remodelling it accordingly.

Response 2: Firewalls, anti-virus software, and better encryptions would be the most effective security upgrades, but decent versions of this technology exist already.

Question 9: ("*How do you feel that security-related training should be approached in the future?*")

Response 1: Training for managers is probably something that should improve, employees have more resources and could ask managers for assistance at any time. The requirements for hiring employees could be improved, though, and help to minimise these issues.

Response 2: It should be conducted formally more often, most training is not in-depth or detailed on the level that it should be. Both resources and time have been challenging (as training in this way removes employees from work), so this would need to be considered in the future.

Question 10: (“*Are there any other changes you feel are required to minimise threats to information systems?”)*

Response 1: No, the above statements may even be exaggerations, although I understand the reasoning behind sources stating that information security has been a challenge. The above changes alone would lead to a situation that could be considered ‘ideal.’

Response 2: Restricting tools which are generally used for breaching security may be more helpful, but I am unsure how further details would be approached.

Saudi American Bank Employees (2)

Question 1: (“*What do you feel is the biggest concern for information system security in Saudi Arabia*?”)

Response 1: Saudi Arabia has to worry about technology developing at different rates, and there are a lot of travellers in the country, and technology capable of breaching security can be brought in rather easily.

Response 2: Currently, most actions that are capable of violating information security can be detected, but improving technology (especially some of the mobile technology) seems to have potential for hacking without the same kind of detection, so it is a concern.

Question 2: (“*What do you feel is the biggest concern for information system security in your organisation, and do you see variations in concerns between departments?*”)

Response 1: There are no real differences in security concerns between departments. The biggest concern at the present is meeting customer concerns with technology that we can safely secure.

Response 2: The concerns for the organisation are the same mentioned for Saudi Arabia. The threat of improving private technology threatens this organisation as well as others.

Question 3: ("*How do you think concerns can be addressed within the nation, and do you feel your organisation could address the concerns differently*?")

Response 1: There is really nothing that the nation can do, security depends on private developments.

Response 2: The organisation can attempt to invest in improvements or even research and development, and although there is more incentive for the nation to do this, it is generally not deemed practical by the company.

Question 4: ("*Do you feel that employees and managers need to improve their levels of compliance, and if so, do you see greater compliance in either employees or managers?*")

Response 1: No, compliance is not perfect, but it is not a major issue either.

Response 2: Compliance could always be better, but I would not call it a problem. Managers are usually more compliant.

Question 5: ("*Does it appear that major reforms are needed within any policies concerned with information security threats?")*

Response 1: There could be stricter requirements to improve technology, but there are times where this policy may seem to 'get in the way' and need discretion anyhow.

Response 2: There could be more policies and procedures in place for detecting existing and potential threats, but that would be an improvement and not a 'major reform' in all likelihood.

Question 6: ("*Are ethics an issue in managers and employees, and if so, what can be done?*")

Response 1: Ethics are an issue, but they are not considered to be the cause of any major failures or problems.

Response 2: Ethical issues in managers are more serious on a higher level, while ethical issues in employees are more serious on the lower levels. Both result in problems, and though ethics has seemed to play a role in some problems, other aspects of the company are prioritised in development.

> "What are these aspects?"
>
> Response: Most of them are actually not related to security, and are part of normal business development, but security is considered as the company continues to improve technology and electronic services.

Question 7: ("*Should there be a greater strive to improve technology within the organisation, and assuming this is always desired, what seems to be the best course of action?*")

Response 1: The desire for technology is usually there, but perhaps changes in research and strategy for acquisition could be improved. The company could benefit from charging some employees with researching security elements more vigorously, and this is something that is discussed from time to time.

Response 2: There is usually an extremely competitive strive to improve technology in terms of services to customers, and changes to security technology change in response to this as well as to changes to internal technology. The strive to improve service-related to technology will always be the greatest, because it is competitive.

Question 8: ("*If resources and time were no object, what changes would be most viable and effective?*")

Response 1: If resources and time were no object…the changes that would be most effective would be rebuilding the internal network for internal processes and services with the best technology available.

Response 2: There is some technology that could be changed to help security a little bit, but most changes that would be effective in that situation are related to information systems (alone) and general business.

Question 9: ("*How do you feel that security-related training should be approached in the future?*")

Response 1: It should be more frequent, and detailed, and more relevant.

"Has it been irrelevant in the past?"

Response: In that it has been too general in some cases, yes.

Response 2: It should be more technical in nature, having more emphasis on the best tools and best practices. Literature could also have more of a part in training development.

Question 10: ("*Are there any other changes you feel are required to minimise threats to information systems?")*

Response 1: Not really, if even the changes discussed were possible, the company would be much better off.

Response 2: An increased number of employees, but that does not seem to be practical at this point in time.

Saudi British Bank Employees (2)

Question 1: ("*What do you feel is the biggest concern for information system security in Saudi Arabia*?")

Response 1: The availability of software and materials that can be approached with the language barriers, an information technology specialist that can make the most use of the best available tools often has be fluently bi-lingual and skilled in the technology.

Response 2: The biggest concern is the lack of concern itself, it seems, because some people don't seem to realise the potential of existing threats.

Question 2: ("*What do you feel is the biggest concern for information system security in your organisation, and do you see variations in concerns between departments?*")

Response 1: The biggest concern is developing security for an information system that assists such a wide range of customers with a wide range of services.

Response 2: Our system is complex in itself, and building security that is both effective and versatile is challenging.

Question 3: ("*How do you think concerns can be addressed within the nation, and do you feel your organisation could address the concerns differently*?")

Response 1: Concerns cannot really be addressed within the nation, at least not directly. The best thing that can happen on a nation-wide level is economic improvement, but even this would affect the organisations differently.

Response 2: The organisation's actions being different from the rate of the development of the nation is the only real way to gain a competitive advantage, and this organisation has the benefit of being one of the more successful companies of its kind. Beyond that there is no planned way of acting differently to get ahead with concerns, but it is possible, and hopefully this gives you some information regarding the question.

Question 4: ("*Do you feel that employees and managers need to improve their levels of compliance, and if so, do you see greater compliance in either employees or managers?*")

Response 1: Compliance is not much of a concern within the company in past years, but employees have had more violations. There are more employees than managers of course, but they also seem to be more prone to violating security and other protocol.

> "What do you think the reason for that is?"
>
> Response: I think the reason is a combination of there being less consequence (generally) and less of a chance that their negligence will be realised.

Response 2: Compliance doesn't seem to be an unusual concern anyway, and it seems to be comparable across the company as well as in comparison to other companies.

Question 5: ("*Does it appear that major reforms are needed within any policies concerned with information security threats?")*

Response 1: It has been hard to create policies that are both detailed and not in need of discretion as variables change. Security and the nature of the system could be reformed for the clear benefit, such as through network restructuring, advanced software use, and other ways, but there doesn't seem to be a good way to improve security through major policy reform.

Response 2: Policies regarding training, researching and upgrading technology, and improving the nature of organisation (such as through increased dedication and staff) could reduce threats, but unfortunately their does not seem to be a definite path to 'major' improvements with any practical investment.

Question 6: ("*Are ethics an issue in managers and employees, and if so, what can be done?*")

Response 1: Ethics, like compliance, are not a major concern with the company. The company has no major plans for change in this area.

Response 2: Not really. Ethical issues seem to be an underlying cause with some concerns, such as compliance and basic employee conduct, but it is one of the least prioritised areas within the company's plans for development.

Question 7: ("*Should there be a greater strive to improve technology within the organisation, and assuming this is always desired, what seems to be the best course of action?*")

Response 1: I think the company could stand to invest a little more funding and effort into improving technology, especially in terms of researching the market for possible improvements, but the current processes seem to be good enough to create a considerable competitive advantage.

Response 2: The best course of action appears to be to approach technology mindful of potential, without making unnecessary upgrades or upgrading before a new line of products comes onto the market. Beyond this, there is little that we can do.

Question 8: ("*If resources and time were no object, what changes would be most viable and effective?*")

Response 1: Educating employees, improving the network structure, and improving software would be the most effective actions.

Response 2: The security system could be best improved using new firewalls, and plans should be created for things like disaster recovery. Our SSL would also be improved, or even replaced.

Question 9: ("*How do you feel that security-related training should be approached in the future?*")

Response 1: It should be revised completely, many parts of it have just been put together without the effort required, often times with important information not realised until later.

Response 2: It should place more emphasis on the concerned realised by experts, rather than considering mostly corporate concerns.

Question 10: (“*Are there any other changes you feel are required to minimise threats to information systems?”)*

Response 1: Firewall protection should have more effort devoted to it, to make sure there are no loopholes and that it is updated as needed.

Response 2: A general investment of human and material resources in security would be an ideal first start, allowing the other areas discussed to be more possible.

Albilad Bank Employee

Question 1: (“*What do you feel is the biggest concern for information system security in Saudi Arabia*?”)

Response: Acquiring and improving defensive software at a rate which is ahead of the potential for threats seems to be the main concern, both inside the company and protecting the services offered to clients.

Question 2: (“*What do you feel is the biggest concern for information system security in your organisation, and do you see variations in concerns between departments?*”)

Response: The same basic threat to the nation is observable in the organisation, but the organisation faces more of a struggle with upgrading technology as needed, because that requires private funding.

Question 3: (“*How do you think concerns can be addressed within the nation, and do you feel your organisation could address the concerns differently*?”)

Response: The government could help itself improve security for information systems in the public sector, but that would not have much of an impact on concerns within financial institutions. This organisation could simply choose to improve security to the highest level, investing considerable money in the process, but that would not cater to the competitive advantage. The competitive advantage takes the greatest priority within most decisions regarding those kinds of investments.

Question 4: ("*Do you feel that employees and managers need to improve their levels of compliance, and if so, do you see greater compliance in either employees or managers?*")

Response: Employee non-compliance is handled by managers on a regular basis, but there is less action taken for managers in similar situations. Some improvement is needed in both areas, but it is hard to measure the extent or develop a strategy to achieve perfect compliance.

Question 5: ("*Does it appear that major reforms are needed within any policies concerned with information security threats?")*

Response: No, I would say that the systems and security could benefit from major reform, but the policies themselves cannot have the discretion required for technological improvements as technology changes. The only developments in policy which would have the greatest influence would be improvements for crisis plans or disaster recovery, which is given little consideration in existing policy.

Question 6: ("*Are ethics an issue in managers and employees, and if so, what can be done?*")

Response: Ethics do not seem to be much of an issue outside of compliance, and as I cannot say compliance is a major concern, I would not say any serious new level of attention needs to be given to compliance.

Question 7: ("*Should there be a greater strive to improve technology within the organisation, and assuming this is always desired, what seems to be the best course of action?*")

Response: There should be a major strive to improve technology wherever possible, but it already exists. The emphasis on competitive advantage through services will always remain, and technological improvements outside of this area does not seem to be practical.

Question 8: ("*If resources and time were no object, what changes would be most viable and effective?*")

Response: If resources were no object, then I would say that the continuing optimisation of technology would be effective. Expanding the staff would also be effective.

Question 9: ("*How do you feel that security-related training should be approached in the future?*")

Response: Training needs to be improved all around, specifically in terms of technical applications and upgrades, but it could use improvement in just about every area.

Question 10: ("*Are there any other changes you feel are required to minimise threats to information systems?")*

Response: Some employee should be charged with the task of improved continual research in terms threats, developing defences, and developed best practices.

Saudi French Bank Employee

Question 1: ("*What do you feel is the biggest concern for information system security in Saudi Arabia*?")

Response: The biggest concern is keeping up with the technology and practices, which continue to change at fast rates.

Question 2: (“*What do you feel is the biggest concern for information system security in your organisation, and do you see variations in concerns between departments?*”)

Response: Firewalls and SSL have the most security-related issues here. These issues generally affect the company equally.

Question 3: (“*How do you think concerns can be addressed within the nation, and do you feel your organisation could address the concerns differently*?”)

Response: There doesn’t seem like there is anything that could be done on a national level, but people here could generally try to improve standards and practices for security. This applies to the technology as much as strategic development. Many people need better plans for how to react to certain threats, because no planning in these areas leaves them especially vulnerable.

Question 4: (“*Do you feel that employees and managers need to improve their levels of compliance, and if so, do you see greater compliance in either employees or managers?*”)

Response: Compliance will always be a minor issue with any policy, so it will always be a concern but will not likely have any increased emphasis.

Question 5: (“*Does it appear that major reforms are needed within any policies concerned with information security threats?”)*

Response: No, there are no ‘major’ reforms that are needed for policy as far as I am concerned, but slight improvements could be made in most departments.

> “Do you have an example?”
>
> Response: There is little protocol for emergency plans, if something were to go wrong with the network or services, much time would likely be lost since there are none of these plans.

Question 6: (“*Are ethics an issue in managers and employees, and if so, what can be done?*”)

Response: Ethics are an issue, yes, and policies and new strategies often try to improve ethics in many ways. It is not considered a serious issue, even though ethics could be a lot higher. Unfortunately it takes major problems in ethics for ethics to gain great attention.

Question 7: ("*Should there be a greater strive to improve technology within the organisation, and assuming this is always desired, what seems to be the best course of action?*")

Response: Ideally, the organisation would have the best technology, so in this sense there is a 'strive,' but the lack of further action is based on resources, strategy, policy, etc. I think the only increased actions which should take place are in firewalls and protection software, because the networks are sufficient and the service technology has evolved at a decent rate.

Question 8: ("*If resources and time were no object, what changes would be most viable and effective?*")

Response: Restructuring technology and organisation seem to have the most potential, aside from expanding.

Question 9: ("*How do you feel that security-related training should be approached in the future?*")

Response: It should be more thorough, especially in terms of development beyond systems and procedures in place.

Question 10: ("*Are there any other changes you feel are required to minimise threats to information systems?")*

Response: Nothing specific.

Saudi Hollandi Bank Employee

Question 1: ("*What do you feel is the biggest concern for information system security in Saudi Arabia*?")

Response: Technology, practices, and planning.

Question 2: ("*What do you feel is the biggest concern for information system security in your organisation, and do you see variations in concerns between departments?*")

Response: The organisation has had problems with dedicating the time and resources suggested from threat implications, and may be more vulnerable than is realised. The fact that many employees simply don't know the answer regarding threat potential in certain areas is something that should be considered.

Question 3: ("*How do you think concerns can be addressed within the nation, and do you feel your organisation could address the concerns differently*?")

Response: There doesn't seem to be much that people can do in the national in terms of strategy, each organisation should simply invest in improvements as they become available. No superior strategy has been realised.

Question 4: ("*Do you feel that employees and managers need to improve their levels of compliance, and if so, do you see greater compliance in either employees or managers?*")

Response: Compliance always needs improvement because it is almost always less than perfect, especially over a given time. There should be greater incentives for developing security and greater consequences for breaching policy.

Question 5: (“*Does it appear that major reforms are needed within any policies concerned with information security threats?”)*

Response: In terms of backup and recovery planning, yes, but aside from that no ‘major’ reforms seem to be needed.

Question 6: (“*Are ethics an issue in managers and employees, and if so, what can be done?*”)

Response: Ethics are something that we value, but we mostly emphasise compliance with policy and procedure. Ethics could be improved with greater incentives, or consequences, but the emphasis will remain in other areas.

Question 7: (“*Should there be a greater strive to improve technology within the organisation, and assuming this is always desired, what seems to be the best course of action?*”)

Response: I think so, but there is a debate about that across the company.

Question 8: (“*If resources and time were no object, what changes would be most viable and effective?*”)

Response: A new network with new services, thereby improving competitive advantage and potential for future development.

Question 9: (“*How do you feel that security-related training should be approached in the future?*”)

Response: It should be carefully planned, and not just ‘dealt with,’ as the mentality seems to be.

Question 10: (“*Are there any other changes you feel are required to minimise threats to information systems?”)*

Response: A greater emphasis on security as a field might lead to new improvements, but outside of that, it seems to already be a developing topic of emphasis.

Saudi Investment Bank Employee

Question 1: ("*What do you feel is the biggest concern for information system security in Saudi Arabia*?")

Response: Competition and demand, because security must always accompany these changes. Growing technology without the security to match is basically 'asking for trouble.'

Question 2: ("*What do you feel is the biggest concern for information system security in your organisation, and do you see variations in concerns between departments?*")

Response: Firewall problems, or 'loopholes,' are one. High levels of encryption are another. Those two areas are common topics in recent concerns.

Question 3: ("*How do you think concerns can be addressed within the nation, and do you feel your organisation could address the concerns differently*?")

Response: Experts could cooperate in attempt to improve information security as a field, but it doesn't seem like there will be enough of an incentive for that any time soon, either within the nation or within the organisation.

Question 4: ("*Do you feel that employees and managers need to improve their levels of compliance, and if so, do you see greater compliance in either employees or managers?*")

Response: They both do, technically, since it is less than perfect. Compliance is rarely a serious concern.

Question 5: ("*Does it appear that major reforms are needed within any policies concerned with information security threats?")*

Response: Some reforms for improvement and protocol for emergency procedures could help, but no major reforms appear necessary in routine operations.

Question 6: (“*Are ethics an issue in managers and employees, and if so, what can be done?*”)

Response: Ethics, like compliance, are rarely a serious issue. Employees have different ideas about what it means to be ethical, and the company is only demanding in certain areas.

Question 7: (“*Should there be a greater strive to improve technology within the organisation, and assuming this is always desired, what seems to be the best course of action?*”)

Response: It already exists, and the company implies it cannot afford to divert efforts any farther.

Question 8: (“*If resources and time were no object, what changes would be most viable and effective?*”)

Response: Expansion could help quite a bit, and so could remodelling all information technology and networks. They would both be practical for their own reasons.

Question 9: (“*How do you feel that security-related training should be approached in the future?*”)

Response: It should become more of an educational process and less of a quick attempt to change bare-minimum processes as they are realised.

Question 10: (“*Are there any other changes you feel are required to minimise threats to information systems?”)*

Response: No, I think there will always be threats, and only the most innovative people can conceive defences to threats that have yet to exist.