Information Security Policy

The National Payment System in Libya

A Thesis submitted at the University of Bedfordshire

In partial fulfilment for the degree of

Master of Science

In

Information Management and Security

Emad Sherif

1032226

Supervisor: **Dr Xiaohua Feng**

Department of Computer Science & Technology

University of Bedfordshire

May 2012

The proper mind is likely the result of Literature, and good work likely the result of science.
- Al-Khwarizmi

Abstract

Information security officers, practitioners and academics agree that information security policy is the basis of any organisation's information security. Information security practitioners share and agree that it is rare that information security policy bring out the desirable results. In order to study and analyse this problem, academics have focused on various methods to motivate employees toward policy compliance, however, they have not paid much attention on employees' expectations and how they perceive the information security policy. Also, employees' satisfaction and awareness of information security policy is critical as it may improve the security level by decreasing the internal threat risks. In this thesis, analysing organisation's employees' expectation about information security policies based on a framework that is formed regarding internal threat motivation, consequences, security behaviour and security countermeasures. Therefore, single case study was adopted in this thesis. The study outcomes along with the case study findings state that organisation's employees' expectations toward an information security policy should be paid much attention during forming security regulations and even during implementation of information security policy within organisations. The thesis concludes that employees' security behaviour is related to their information security background and awareness, as well as, security countermeasures, where if the countermeasures perceived negatively, it may negatively help to increase the risk in terms of internal threat. Finally, security countermeasures must be defined before taking negative actions toward employees, as well as, information security training should be scheduled regularly within organisation and they should be arranged regarding to the organisational groups' professions.

Keywords: Information Security, Security Policy, internal threat, external threat, the National Payment System in Libya

Preface

This thesis was submitted for a Master of Science in Information Management and Security degree at University of Bedfordshire, at the Department of Computer Science and Technology. The study was supervised by Dr Xiaohua Feng (PhD, PGCerTHE, MBCS, MIEEE), University of Bedfordshire, at the Department of Computer Science and Technology, between March 2012 and May 2012.

I would like to express my thankful feeling to all the participants from the CBL and especially to Mohammed Ellafi and Omran Elshaibi for participating in this thesis. I really appreciate the precious time you have given me for discussions and support. I also would like to thank Xiaohua Feng for all the support I have ever needed plus valuable information, comments, suggestions and advices from either, our meetings or questions and enquiries by Email.

Luton, May 2012

Emad Sherif

Contents

Figures

Tables

Abbreviations

IS – Information Security
ISP – Information Security Policy
ISO – Information Security Officer
NPS – National Payment System
CBL – Central Bank of Libya

1 Introduction

Information security field has been a hot topic recently, where studies and researches have taken a place regarding this field. The field of information security has changed from just technical issues, technology point of view, into a completely different point of view, where information security has become a more widely term concerning an organisation's assets secure management (Pearlson & Saunders 2009). The organisation's assets secure management comprises the organisational procedures, structures, people, and processes. The basis for this assumptions, as presented by researches and professionals (e.g., Pearlson & Saunders 2009; Siponen & Vance 2010; Von Solms, Thomson & Maninjwa 2011), and information security important considerations (Ward & Peppard 2002) in an organisational point of view is an IS (Information Security) policy. Considering this basis to build an organisational information security plan to secure the management of its assets is a challenge for itself (Tipton & Krause 2008). Also, organisations dedicate important resources to implement IS plans and policies, these plans are rarely achieve the desired goals or objectives (Klaic & Hadjina 2011). The obstacles are mainly caused by the employees whom rarely follow the IS policies (Waugh 2008).

While information security (hereafter IS) professionals seek suggestions for better implantations to there is plans and policies from international IS organisations of security, academics criticise this methodology for letting the requirements of an organisation dependant (Peltier 2002), concentrating on the existence of IS plan or policy more than its contents and procedures, and unable to offer guidance on how IS plan or policy has been implemented practically (Klaic & Hadjina 2011). Taking another IS policy which has been implemented for another organisation and formulating it to your organisation is not serving the organisation's approach, goals, and objective neither the employees (Von Solms, Thomson & Maninjwa 2011). Based on the value and the significance of the structural contents of IS policy, attempting to implement them as a general approach or form does not guarantee successful results in the end when applying these type of IS policies implementation in practice (Siponen & Vance 2010). IS has become an employees and organisations issue, the IS policy should be implemented according to the needs of the employees in the organisation (Siponen & Vance 2010).

Information security policy is mainly implemented to influence the people perceptions in organisations about IS (Caruso 2003) and to raise awareness amongst them about the critical factors and risks that involved in the IS. The information security policy is a significant element in any organisation, even more; it's affected by the social environment in any organisation, therefore; information security policy is subject to change (Peltier 2002). If people in any organisation perceive the information security policy in different way from the organisations information security officers or experts, information security policy will not be effective, more importantly; overall objectives cannot be achieved (Pearlson & Saunders 2009). Also; (Siponen & Vance 2010) have suggested that in order to improve the IS police in any organisation, studying the people perceptions in the organisation is needed.

How people inside an organisation perceive is related to the each individual's references. References of an individual of a specific fact reflects the way of each perceive of that fact and let the others know how to deal with this kind of facts (Von Solms, Thomson & Maninjwa

2011). These references comprise background knowledge. Also, people references inside an organisation is directly related to the information security policy; background knowledge that people have built based on familiarising against the information security policy plans and documents, involving in IS trainings, considering others ideas and following the behaviour effect towards the information security policy (Ward & Peppard 2002). The term individual's references in the information systems has been presented to describe obstacles in the acceptance process of the new technologies, it even includes the understanding of information systems compliance (Peltier 2002). Specifically, since information security policy has a crucial role in organisation's IS, it would be significant to formulate the individual's references about the information security policies and include them when implementing information security policy. Even more; information security policy's various issues and obstacles are directly related to people compliance towards it (Tipton & Krause 2008).

Therefore; analysing employees' visions and perceptions of information security policies are needed equally along with declaring the individual's references that concern information security policies.

1.1 Research Objectives and Questions

Based on what's mentioned above, the main objective of the study is to raise awareness amongst an organisation's employees about the insider and the external threats impact on the organisation's IS policy towards achieving quality understanding of this impact of an organisation's employees' perceptions of IS policy on IS policy planning.

Q1: How do various organisations' employees perceive the organisations IS policy?
Q2: How do internal and external threats affect the IS within organisations?
Q3: What is the impact of an organisation's employees' perception of ISP on IS?

Based on the objectives and questions of the study, case study interpretation is needed. The proposed framework is derived from analysing case study of the National Payment System's IS policy and IS international standardisations. The framework assists in forming a new IS policy that helps to improve awareness, understanding and consequences of the IS policy perceptions towards insider and external threat. Information system's references can be useful for this particular IS research.

1.2 Delimitations description

The study objectives and questions mentioned above refer to the delimitations in this research study. Delimitation's description is as follows:

Perception

The research is concerned about the employees perceptions and their point of view towards the IS policy, instead of concerning about how information security policy is framed or processed.

References

The research is concerned about the structure of the IS policy and the consequences toward the IS policy use, internal, and external threats, instead of concerning about the organisation has used the original references.

1.3 Concepts

The used concepts in this research study are listed below. The aim of this is to provide a better understanding.

References

This includes the understanding of, perceptions, accepting of a specific fact (i.e., information security policy).

Information security policy

IS policy comprises number of documents used by an institution or organisation to refer to a set of rules in order to secure the organisation's assets. IS policy is concerned about the organisation's assets rather than the level of security of IS technically.

Perception

Perceptions describe the underrating and expectation of a fact (i.e., information security policy) gained by experience.

Internal and external threats

Internal threat is originating within an organisation, and often caused by undisciplined employees. External threat is originating out of an organisation.

1.4 Thesis Structure

Following what has been mentioned earlier, the rest starts from chapter two, and the structure is as follows. Chapter two comprises an overview of IS policies roles. Chapter three comprises a theoretical framework of the research by presenting the National Payment System (hereafter NPS) in Libya case study discussion of references. Chapter four comprises internal and external threats influence along with building on the ideas provided in the second and third chapters. Chapter five comprises the methodology of the research: Selection of analysing methodologies for evaluation. Chapter six comprises the NPS case study. Chapter seven comprises analysing the questions of the research. Chapter eight comprises the study's results and limitations. Finally, conclusions, recommendations and future studies about internet banking security for the Central Bank of Libya.

2 Information Security Policies Review

This chapter comprises IS policies roles and literature reviews, IS polices applications and how various organisations' employees perceive these applications. Literature reviews are provided for forming the framework of the study.

2.1 Introduction

The technology has been the main basis to form or establish an IS literature (Fugini, & Bellettini 2004; Quigley 2005), it has been presented that developing the IS technology has been in a much complicated advanced levels. Security technologies themselves are not going to solve IS issues as various problems are listed from information assets management (Straub, Goodman & Baskerville 2008). Information security policies form the basis for organisation's work to provide security to these information assets (Quigley 2005). It has been suggested (Tipton & Krause 2008) that without an IS policy, IS practice will be implemented without a proper understanding of goals and responsibilities. Therefore, information security policies describe the organisation's framework and roles of IS managements (BSI 2005, p. 9).

Various organisations implement information security policies in order to develop their IS efforts to protect the assets of their information and resources (Fugini, & Bellettini 2004). Also, there are agreements between academics and professionals that IS policy is the basis of IS in any organisation. Deploying the information security policies is a vital part of IS controls (BSI 2005, p. 7) and as an important section of IS governance (Von Solms, Thomson & Maninjwa 2011). Even more, there should be a linkage between organisation's goals and information security policies (Klaic & Hadjina 2011). The objective of the information security policies is to influence the perceptions or point of view of the employees about IS to achieve better thoughts through the security and protecting assets of the organisation (Siponen & Vance 2010).

2.2 Information Security Policy Applications

The IS policies application may be split into implementation stages, processes, and feedbacks that can be used as input of information that assist in formulating the IS policies (Klaic & Hadjina 2011). Formulating the IS policy is difficult mission for organisations as it is achieved through complicated set of processes (Siponen & Vance 2010). While professionals look for suggestions to implement and form the IS policies from international IS standards, academics criticise this kind of methods where professionals are not concerned fully about the requirements of the organisation (Pearlson & Saunders 2009; Von Solms, Thomson & Maninjwa 2011) and concentrating about the current IS policies more than what these IS policies contain (Siponen & Vance 2010). The approaches that based on copying other successful information security policies to form the organisation's IS policy are not likely gives a successful outcome, nor the organisation's employees may be able to rely on or may achieve the overall objectives (Peltier 2002). Information security policies applications successful deployments are not about what they contain nor defining universal factors as this approach does not succeed the applications (Tipton & Krause 2008), information security policies must be set based on the organisation's specific requirements. (Klaic & Hadjina 2011) have studied that management, cultural, contents, awareness and educating of employees in organisational context, and including the employees in the process of formulating the information security policy are the crucial factors that affect the successful deployment and implementation of the information security policy.

Information security policies formulation is not enough; information security policies should be deployed and accepted by employees. Information security policy must be deployed on all over the organisation and training should be provided as if the employees are not familiar or aware of the contents (Caruso 2003), and possibilities are that employees will forget it. Therefore; all employees must use information security policy (Quigley 2005). Unfortunately, the employee incompliance has been an issue in various organisations. Academics have been studying incompliant behaviour of some employees; therefore, various methods have been presented in order to assist in raising the degree of commitment. This study focuses on employees, internal, external threats as end users to the IS of an organisation and, also, the most crucial questions in managing IS should include is how to guarantee employees commitment to the information security policy. Furthermore, it is beneficial to explain or set up what are the factors that affect the employee behavioural compliant as they are directly connected to employees point of views towards the information security policy. (Tipton & Krause 2008) have presented that IS awareness concept relates to 'a situation where end users are familiar, committed, and aware their tasks along with the security rules' (p. 43). (Klaic & Hadjina 2011) have suggested that end users' IS awareness has affected their behaviour towards the information security policy compliance. According to Klaic & Hadjina (2011), awareness of IS comprises IS awareness and information security policy awareness. The results from their study, which were recommendations about the employees behaviour change, advice that employee's behaviour affects his desire to commit himself to the information security policy, whereas attitude is affected by assessing the employee's compliant s and consequences individually. Siponen & Vance (2010) have concluded that others perceptions affect the employees' attitude and that how the affected expectations of these employees influence their desire to commit to the information security policy. Even more, (Kant, Meixing & Jajodia 2011) have concluded that employee's expectations of the quality of information security policies affect their compliant towards the information security policy. Practically, the information in information security policy should be updated,

appropriate, and available for the employees and that every employee may look for the needed information from the information policy document easily. Their results have shown also the language used in information security policy may affect the attitude of the employees, where employees may not be able to understand the information security policy documents easily in case if they are not formulated in the native language of the employees. Also, according to Von Solms, Thomson & Maninjwa (2011), invisible or unclear information security policy may affect the commitment of the employees towards the information security policies. Even more, (Peltier 2002) has concluded that employee's good expectation of their valuable actions toward the IS gives them a positive motivation to commit to the information security policy. As for some IS professionals, these findings advice that communication methods are equally important when informing employees that IS has a crucial role for any organisation and that employee's attitude may affect or succeed the IS in that organisation. Actually, Kant, Meixing & Jajodia (2011) argued that information security policy compliant must be studied as part of end users missions and incompliance of the information security policy must be studied as undone work or irresponsibility from the end users or employees. In the end, whether to comply with the information security policy or not is the employee's options to commit.

2.3 Expectations of Information Security Policy

As administration always concern about the IS policies at the organisation, the information security policies might represent the management of IS point of view from various organisations more than considering just the groups' approach at an organisation from managing IS point of views. Also, Pearlson and Saunders (2009) have presented that many IS policies have been affected by the technology would view of managing IS. This might affect the implementation stages of the information security policy as it may create new factors that need to be included in the information security in order to keep the information security policy updated and effective. Even more; academics suggest that in order to secure the resources and information in the organisation that could be achieved or increased by the organisation's employees itself (Kant, Meixing & Jajodia 2011), traditionally employees have been considered as enemies or a threat to managing IS (Sun, Li & Bertino, 2011) and such type of threats as so called insider threats have been a hot topic for researchers, academics, and professionals as it oppose a serious threat to IS management and to the information security in any organisation in general (e.g., Gibler & Douglas 2010; Siponen & Vance 2010).

Recent studies and researches advice that there is still a device between IS officers and the organisation's employees on each one's views or expectations and experience about IS practices (Waugh 2008) and that an employee might form a different opinions than the IS officers (Klaic & Hadjina 2011). Also, these IS officers or IS must be able to implement the information security policy that is accepted for the basics, beliefs of various groups' backgrounds in any organisation (Ward & Peppard 2002). Practically, IS officers usually fail to consider various employees views toward IS and mostly just considering their views and perceptions of how these employees might perceive information security (Grama 2011). IS officers must include the employees' views and expectations of IS as those employees are the basis for following and protecting the IS when implementing the information security policy in any organisation (Siponen & Vance 2010).

Whereas academic acknowledge that information security policy plays a main important role, and various methods to improve employees commitment have been suggested, an employee's views and expectations of information security policies has not been given enough attention. There have not been wide researches focusing on perceptions and expectations of information security policies, some researches have mentioned it or consider it briefly recently, basically employees' expectations and perceptions have been mentioned in some topics as small part to touch on not a proper studies or researches that considering it as a whole topic to work on. Caruso (2003) have discussed that end-users' perception on IS's formulated by individual, technology, and organisation's internal factors. According to Tipton and Krause (2008) end-user is likely to has a resistant view on information security policy if he sees that information security policy forms an obstacle to his day to day tasks, (Kant, Meixing & Jajodia 2011) have suggested that end-users might perceive information security policy as an obstacle to the communications flow. When end-users and employees do not have a shared interests or common ideas about the IS procedures, businesses and work efficiency may be given a higher priority than the IS (Pak & Cannady 2009). Even more; Grama (2011) has discussed that end-user is likely to has a better perception of information security policies when the information security policy is implemented along with his work objectives and contribution. If end-user perceives that his actions may lead to better benefits for the organisation, the opportunity is that his behaviour on information security policies would be better (Tipton & Krause 2008). Therefore, the IS awareness level of the end-users and employees would affect these expectations Grama (2011).

To conclude, the information security policies' applications have been always a challenge for managing IS. IS officers and end-users might perceive IS policies in various ways, these various ways could be different and IS officer might has a different means and views of how to manage IS. Also, IS officers usually fail to consider others idea such as employees and end-users. In the other hand, academics have suggested various factors that need to be considered when implementing the information security policy as they might affect employees' attitude to commit to the information security policy, employee's views and expectations of information security policies have been a less attention topic.

3 Theoretical Bases

Chapter three presents the basis of the study's theory – NPS information security policy reference. It starts with theory discussion. NPS information security policy is then discussed in three subsections: (1) how employees at the central bank of Libya use it; (2) contents of the NPS information security policy; (3) Consequences and employees compliance. In the end the theoretical framework can be formed for this study.

3.1 Theory Selection

The theory selection for this study begun several months ago, it is related to the current information security policy at the central bank of Libya in which it would be valuable to contribute in improving the information security policies efficiency to secure an organisation's resources and information in general along with paying a closer view specifically for the NPS at the central bank of Libya from an employee point of view. Bashir (2008) has presented an information security policy for NPS, however, there has been a less attention considering internal threats, in the other hand, external threat has not been mentioned at all. Therefore; this study has been needed to increase the awareness of internal and external threats amongst the employees about these kinds of threats and to improve managing information security better.

Thorough this study, the knowledge of various theories have been into study stages varies from recent studies and researches considering this topic to the current applied NPS information security policy, later, the understanding has been widened. These two factors have been the reason behind the theory selection. In the very beginning of this study such frameworks as contextualised study (DeRose 2009) influences the way of thinking, but with some experience in the information security fields and working in an organisation for time as a responsible leader, then, the knowledge and the expectations toward securing the organisation's resources and information become clear. Even though, contextualisation may affect the background knowledge in terms of considering or thinking about making changes to the organisation structure, which may leads to making some changes to the information security policy of the organisation.

Bashir (2008) has presented an information security policy for the NPS at the central bank of Libya; however, he has not mentioned or considered the internal and external threats. Therefore; this is the main motivation and basis for this study. Paying more attention to such threats, especially, internal threat that caused by employees as it has not been main topic or main wide study recently. The current information security policy at the bank contains strict roles about how to protect hardware and software components mainly in the date centre for the NPS; however, internal and external threats have not been mentioned, therefore; the policy has failed due to employees' noncompliance. According to Kant, Meixing & Jajodia (2011), managing IS in data centres is critical and vital, they have argued that employees and data centre staff play the main role in securing the resources and information in data centres. Also, (Gritzalis 2003) has suggested that end-users, data centre staff, and employees in general should be included when planning and implementing information security policy, their expectation and views should be sought.

Therefore, employees should be consulted or considered when planning and implementing an information security policy in any organisation as they are the main factor that may contribute to succeed the policy or cause failure.

4 Study Frameworks

Chapter four comprises literature reviews and bases of the theory that presented earlier, however, expanding the ideas and knowledge of previous literature on IS policies, internal and external threats. Also; present the consequences of the internal threats to the organisation. In the end, these frameworks will be used to as guidance.

4.1 Introduction

Internal threat has been a serious obstacle for many organisations recently (Gibler 2010); he has suggested that internal threat should be dealt with carefully. However, academics have argued about what should be addressed as internal threat and why and how would IS be affected by insiders. Few of researches concentrated on insiders with malicious desire (e.g., Siponen & Vance 2010) have illustrated that most of the insiders were planning to do a negative actions. Few of them did violate the information security policy.

According to Sun & Bertino (2011), internal threat can be described in three categories; these three categories are based on intent and employees' motivation:

- Steal information for money,
- Steal information for personal gain,
- Sabotage Information Technology or Information System.

In the other hand, (Cole & Ring 2006) have studied internal threat and presented other motives for the internal threat, such as, steal information for business gain, accidental, and even cultural differences.

Furthermore, (Fugini & Bellettini 2004) have argued that there are insiders without malicious desire in the same time as others have, however, these type on insiders or internal threat does not deal with IS issues properly. In the other hand, (Waugh 2008) has defined insiders as not just an internal action with malicious desire, but more widely, any person or employee who caused that incident or threat in general, including his mistakes. Even more; (Von Solms, Thomson & Maninjwa 2011) have categorised insiders into malicious type of persons by nature and non-malicious type of persons that may accidentally do any harm. According to Quigley (2005), poor or noncompliant behaviour of the employees is the main cause for security issues in any organisation. Also, careless employees could be considered as internal threat in some cases when they actions cause security mistakes or lead to security breach.

4.2 Internal Threat Behaviour

According to Siponen & Vance (2010), careless security behaviour and noncompliance mostly cause or oppose a threat within organisations and this kind of threat is called internal threat. Siponen & Vance have suggested that in order to mitigate this kind of threats which is the most dangerous and affected threat is to study the behaviour of the organisation's employees. It is important to inform the employees about the security countermeasures when deploying the information security policy as this action influences the employee's attitude and behaviour to commit to the information security policy and help to mitigate the internal

threats even before it happens (Sun, Li & Bertino, 2011), also, employees' acceptance is equally important.

Many academics described that human being has emotions and this may affect their behaviour to comply in some point. Few researches described that human behaviour is directly connected to his attitude, and attitude is mainly based on the humans' emotions (Siponen & Vance 2010).

Furthermore; (Tipton & Krause 2008) have proposed and illustrated a model that represent employees' attitude toward IS issues, known as ABC (see Figure 1). This figure contains three components as shown below:

A – Attitude emotional component.
B – Behavioural component.
C – Cognitive.

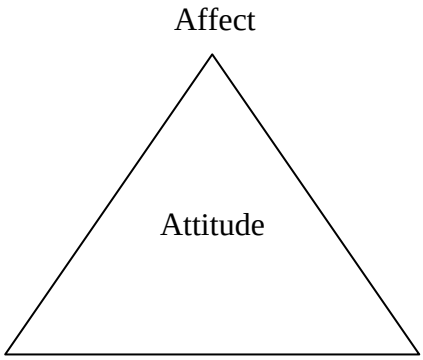


Figure 1: *ABC framework, cited from Tipton and Krause (2008)*

There have been other researches that suggested another factors to be considers and categorised, these factors may affect the employees' behaviour as well. A study by Alfawaz, Nelson and Mohannak (2010) concluded that employees' behaviour toward IS may be affected by positive and negative motivations. Positive motivations may be achieved through rewards that would be given to hard workers, while, negative motivation may occur when punishing or given out penalties to employees.

4.3 Behaviour Compliance Frameworks

The behaviour of the employees has been and always be a vital and important factor for any organisation that looks forward to maintain and improve the IS resources and management (Carroll 2006), he has suggested that in order to avoid or mitigate the IS risks employees' behaviour and security countermeasures should be identified before implementation. According to Carroll (2006), behaviour of humans can be classified based on four factors as follows: internal or external and not stable or stable. These human factors or feelings may determine the behaviour of the employees.

Furthermore, (Montelibano & Moore 2012) have argued that there have been another factors may affect the behaviour of the employees, these factors can be classified into two classes; 1st class comprises the background knowledge and what do they can give to the organisation. And 2nd class comprises the employees' compliance and commitments.
Even more, According to Alfawaz, Nelson and Mohannak (2010), employees' knowledge of the IS objectives and rules along with having the basic skills to achieve specific tasks are vital and equally important within any organisation. (Alfawaz, Nelson & Mohannak 2010) have categorised the employee's behaviour towards the IS into 4 modes as follows:

- Knowing/Doing,
- Knowing/Not doing,
- Not knowing/Doing,
- Not knowing/Not doing.

Furthermore, table 1 consists of the 4 modes summary with description and real world examples for these 4 modes of the employees' behaviour as follows.

Table 1: *The Modes if IS Behaviour, adopted from Alfawaz, Nelson and Mohannak (2010)*

Modes (Behaviour)	**Description**	**Examples**
Mode One	The employees doesn't know the IS objectives and the requirements of the organisation and doesn't have IS knowledge. And he's not doing the right by not following the rules.	IS policy hasn't been deployed and shared with the employees properly
Mode Two	The employees doesn't know the IS objectives and the requirements of the organisation and doesn't have IS knowledge but he's doing the proper IS behaviour by following the rules.	Although no support is being offered, employees volunteer to do the right things.
Mode Three	The employees know the IS objectives and the requirements of the organisation, but they aren't doing the right thing by violating the IS rules.	Although the deployment of the IS policy, employees aren't compliant to the IS rules (Risk)
Mode Four	The employees know the IS objectives and the requirements of the organisation and they're doing the right thing by following the IS rules.	IS Policy is deployed and shared. And employees are compliant.

Even more, figure 2 below shows the 4 modes and the relationship between each other. The arrows define the dynamic relationship between the 4 modes, which draws the knowledge and skills that may affect the behaviour, and then the outcomes as follows.

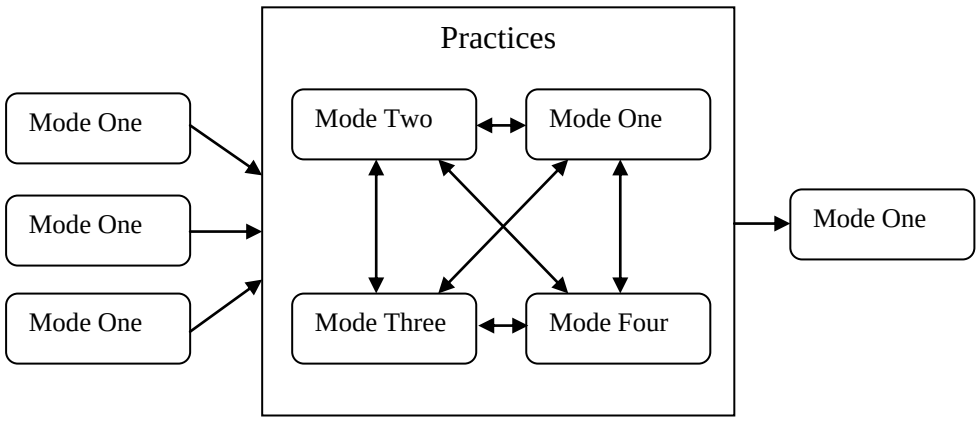


Figure 2: *The Modes of IS Behaviour, adopted from Alfawaz, Nelson and Mohannak (2010)*

4.4 Internal Threat Consequences

Researchers say that after analysis and studies, most of internal threats come from end-users as result of their human errors' actions or mistakes, while, the minority of internal threats come from employees who work in the technical field, sector, or departments (Martinez-Moyano, Conrad, Rich & Andersen 2006), they have illustrated that most of the insiders are legitimate employees. It is worried that some of the employees are not abiding the IS rules and they are not following the information security policy compliance. Also, (Carroll 2006) has argued that some of the insiders who committed or violated the information security policy within the organisation have been convicted or suspected in bad actions before.

4.4.1 Motivation

In the other hand, what has been the motivation behind such actions to violate the organisation's policies by not following the information security rules? According to Alexander, French, Taylor, and Sutton (2008), the motivation or reasons behind such actions or behaviour is; financial advantages, revenge purposes, or disagree and dissatisfaction with the organisation's management and policy. Even more, particular events or actions may be behind such actions too, such as, contract termination, punishing, forcing not to take holiday, or undesirable department transfers.

Although most of the researchers just focused on insiders or employees with malicious desire, other reasons that may cause or lead to internal threats may be the result of carelessness towards the employees that may leave them as useless workers, this factor should be studied and get more attention from researchers, professionals, and people with a decision making positions within organisations (Von Solms, Thomson & Maninjwa 2011).

Human errors or mistakes may be considered as an internal threat, as well as, they may be categorised (Siponen & Vance 2010). According to Siponen and Vance (2010), human errors can be described as follows; human error that is caused because of a mistake from a skilled user or employee, and human error that is caused because of not fully aware of how to follow a specific rule, also, that may happen when an user or employee is not able to troubleshoot, or solve problems within the organisation.

Few researchers have gone further (Sun & Bertino 2011) in analysing the human errors and user mistakes into defining interrelationships elements and factors that could lead to cause these kind of mistakes, these elements or factors could be workplace, organisational, task factors or elements, these additional factors may cause IS violations. In the other hand, (Cole & Ring 2006) have argued that human errors and user mistake may be recognised by technology professionals within the organisation, such as, network, database and system administrators in order with security officers. Therefore; this argument or model could be only used or applied to spot, mitigate or prevent human errors that may be caused by end users. Unfortunately, this model or suggestion does not applicable for the other kinds of human errors or mistakes, such as, non-technology issues, ethical issues, temporary workers, and ordinary visitors within the organisation. Therefore; this model or suggestion could not be applied as general model or multipurpose.

4.4.2 Information Security Compliance

How organisation makes its employees to abide with the information security rule and change the behaviour of the employees to achieve information security compliance?

This question is one of the main commonly asked questions within organisations recently, and indeed it is one of the main reasons behind this study. Employees' knowledge background, awareness and quality training of information security are the main aspects to positively change employees' security behaviour towards information security behaviour (Klaic & Hadjina 2011). According to Fugini, and Bellettini (2004), employees' background knowledge is the main aspect that positively change the employee's behaviour toward information security compliance. Academics say that end-users, administrators, and security officers agree with the necessity of IS training courses in order to raise the awareness and knowledge about the emerging threats and countermeasures (Quigley 2005).

Also, (Straub, Goodman & Baskerville 2008) have argued that definition of knowledge differs from the security knowledge in terms of information security compliance and information security polices documents. Security knowledge is an important aspect in this study as it is directly related to the security behaviour that needed to achieve the information security compliance. In the other hand, educating only the information security officers and professionals about the information security and not all the end-users and employees can be ineffective, where, end-users and employees are one of the main elements and the people who are dealing, working, and contributing within the organisations, therefore, they are always should be included and their view about the information security should be sought (Klaic & Hadjina 2011).

According to Fugini, and Bellettini (2004), the people who are responsible about the organisation's information security, such as, information security officers and professionals should set up a list of punishments if any user or employees think or act wrongly as deterrent to their future actions, for example; fear of being caught and being fined.

In the other hand, rewards should be equally set up for the employees' who have commitments and abide the information security rules as motivation (Quigley 2005). Also, (Waugh 2008) has suggested that rewarding the positive security behaviour employees is one of the successful ways to improve the security behaviour for the awarded employee and for the others where this rewards give the others motivations to improve themselves and change their security behaviour positively.

Sometimes, focusing on success is better than focusing on mitigating the security risk (Tipton & Krause 2008). In the other hand, some researchers disagree that the motivation aspect can reducing security violations from some users or employees (Caruso 2003), even more; According to Caruso (2003), managing information security may result in unclear output where these kind of outcomes are unmeasured as sometimes security issues and risks cannot be predicted. Therefore; punishments and rewards system or framework is difficult to achieve.

4.5 Information Security Countermeasures

In order to minimise the effect of the internal threat, risk analysis and information security management is the solution (Al-Hamdani 2009), he has suggested that risk analysis must be implemented and managed by information security professionals or IS officers. According to Bodin, Gordon, and Loeb (2008), risk analysis comprises identifying the risks and controlling or managing the risk.

Some risk management methods which have been applied caused or created another type of risks, specifically the internal threat (Schneider 2010). Therefore, many countermeasures techniques have been applied to help in minimising the internal threat within organisations.

According to Peng, Yingwu, Sen and Guoqing (2011), minimising the harmful effect of the insiders or internal threat is not impossible, however, it is complicated method to implement or apply where it needs a multifactor methodology that is based on the cultural, technical, procedural, and political factors within the organisation. They discussed that there are many recent and on-going ways that could be applied within the organisation that lead to internal threat detection. These ways represent the security countermeasures that could be given to employees and end-users within the organisation. (Bodin, Gordon and Loeb 2008) have suggested that it is very important to implement and deploy an information security policy within the organisation to control the employees behaviour towards the security rules and what are the forbidden actions that they may take and cause a threat or harm the organisation in any way so that the employees will be informed of the consequences in taking such action or trying to violate the information security policy in purpose or not. Regular training courses onsite or outside about the information security policy goals and organisation's objective in order to protect the information assets is equally important so that end-users will be kept informed about the emerged security standards and to raise their awareness of security requirements.

Also, implementing such security countermeasures could be helpful in detecting threats not just minimising the caused effects and preventing the threat from happening. Detecting threats in other words means monitoring the employees and end-users in case of suspicious or malicious behavioural changes (Breier and Hudec 2011). According to Breier and Hudec (2011), monitoring or such actions should be applied not only on the current employees and end-users, it should even applied during the employment process to find out and track the future employees and end-users that may be employed by examining their background of security, work history, behaviour instability, and financial shortages in order to prevent or minimise the internal threat. Implementing these types of security countermeasure help to detect or prevent end-users when they get their hands on confidential data by accident or even on purpose. As well as, end-users activities on the web should be monitored regularly (Peng, Yingwu, Sen and Guoqing 2011).

In the other hand, (Schneider 2010) has found that choosing such security countermeasures in monitoring the employees and end-users activities either online or normal regularly could

affect the employees and end-users privacy which may lead to security risk in case of one or some of the employees or end-users turn into an insider that cause an internal threat.

Furthermore; in order to protect the organisation's information assets, there is need to consider all aspects of information, data, and assets in general, not just documents and confidential information, it is equally vital to protect the data as well (Al-Hamdani 2009). (Miles, Rogers, Fuller and Hoagberg 2004) have argued that it is vital to set up security rules for the organisation's hardware assets in order to protect the data. Therefore; Hardware assets must be protected physically in order to minimise the risk that may be caused by an insider with an authorised access as an employee or end-user.

Even more; (Miles, Rogers, Fuller and Hoagberg 2004) have suggested that forcing employees and end-users to set up or create a strong periodic passwords may enhance the level of security within the organisation. Also, (Bodin, Gordon and Loeb 2008) have illustrated that deploying account management groups with different roles, privileges, and power level for the employees and end-users are well known ways in order to control and monitor employees and end-users access to the organisation's systems.

Furthermore, in order to minimise the internal threat in another important aspect or scenario, when an employee wants to leave the organisation in case of a resignation or contract termination, the employee's account or end-user's workstations needs to be deactivated immediately (Peng, Yingwu, Sen and Guoqing 2011).

Shigematsu, Bin-Hui Chou, Hori and Sakurai (2008) have presented that security countermeasures could be categorised into two categories – technical security countermeasures and non-technical security countermeasures. Technical security countermeasures comprises software, data, network and hardware security techniques, while, non-technical security countermeasures comprises regulations, physical locations, and risk analysis security methods. Some researchers have argued about successful security countermeasures, (Tipton and Krause 2008) have argued that there is no an effective method or mechanism that can be implemented or followed in order to minimise the internal threat risk, because security countermeasures are not a technical system or material, they are rather concept or set of rules that needed to be followed in order to ensure the secure management of risk or information assets within the organisation. Also, (Pak and Cannady 2009) have argued that end-user security behaviour could be enhanced when the users understand and aware of the security rules and information security policy. Furthermore; (Miles, Rogers, Fuller and Hoagberg 2004) have studied and suggested that security countermeasures should be implemented based on all aspects of security, they have presented that typical security countermeasures should contain the following five elements as follows:

- Risk analysis,
- Technical security countermeasures,
- Non-technical security countermeasures,
- Monitor,
- Control.

According to Waugh (2008), carious technical and non-technical security countermeasures are required to either prevent or minimise the internal threat risks. (Siponen & Vance 2010) have suggested that control mechanisms are vital in order to improve the information security policy regarding this topic and information security policy could be considered as a control mechanism. Also, risk analysis is equally important, not only to define expected risks or threats, it is very important to define and recognise points of control internally (Breier and Hudec 2011). Technical security countermeasures track and maintain the flow of technical tasks within the organisation (Grama 2011). Even more; (Kant, Meixing Le and Jajodia 2011) have illustrated and concluded that firewalls, intrusion detection systems, proxy, and anti-virus programs are somehow old technologies for nowadays risks and threats. (Kant, Meixing Le and Jajodia 2011) have suggested that forensics, intrusion detection and prevention systems, and filtering are some of the modern technologies for preventing and minimising the risks and threats.

Therefore, managing IS and risks depends on the implemented information security countermeasures as this directly affect the end-users' security behaviour (Ward & Peppard 2002).

4.5.1 Security Countermeasures and Behaviour Interrelationship

Therefore; (Klaic & Hadjina 2011) have studied that there is a relationship between employee's knowledge, informal rules, and organisation's information security policy so that when employee's knowledge is poor, IS policy and informal rules are key aspects to control the employee's security behaviour, while, without a strict IS policy and informal rules is poor, employee's knowledge is the main control key.

In order to minimise the internal threat risks, the employees' security behaviour needed to be studied against the security countermeasures, this may affect the employees' security behaviour as some employees may not fully understand it. Therefore, (Pieters and Coles-Kemp 2011) have illustrated that there is a strong relation amongst human being factors, internal threats and security behaviour& countermeasures. Figure 3 below simply shows this relationship.

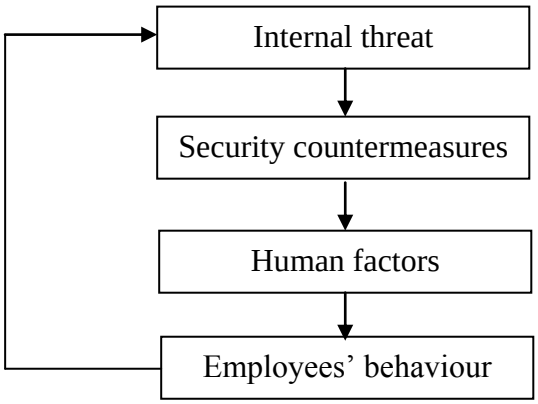


Figure 3: *internal threat, security countermeasures, human factors, and security behaviour relationship, adopted from Pieters and Coles-Kemp (2011)*

5 Methodologies

The fifth chapter comprises the research methodologies that have been used to verify and evaluate the data and why is it effective to choose one specific method regarding this study.

This chapter consists of assumption discussions, the basis behind choosing case studies option, the national payment system in Libya. According to Berndtsson, Hansson, Olsson, Lundell (2008), choosing a case study as an approach requires site selection, academics or professionals' roles, and analysing & evaluation of data. Table 2 consists of the thesis methodology summary.

Table 2: *thesis methodology summary*

Task	*Description*
Goal of the research	The goal of this is to improve and raise awareness about the IS policies, internal and external threats within organisations.
Study methodology	Case study.
Research method	Organisation's employees' expectations, behaviour toward their expectations and the security countermeasures.
Analysis method	Empirical studies analysing techniques.
Organisation's case study selection	The selection of the case study is based on my personal experience as an organisation's employee with colleagues willing to participate in this study.
Information sources	Literature reviews Personal experience Informal interviews Internal documentations
Thesis evaluation criteria	Adopted principles for evaluating case studies (Kaplan, Truex, Watell, Wood-Harper and DeGross 2004; Klein and Myers 1999)

5.1 Considerations

Every individual has his own expectations, assumptions, and perceptions that could be based on what he has experienced. When studying and doing a study or research, these perceptions 'drive and lead the way of observing and studying the objects' (Kaplan, Truex, Watell, Wood-Harper and DeGross 2004, p. 257), basically it is kind of driving the beliefs (Klein and Myers 1999). While expectations affect the method's selection by which background could be formed and analysed (Huang, Yang, and Calmet 2006), the beliefs affects the real life thinking (Subramanian 2008). In the other hand, there are different considerations for the information systems fields of studies. (Vacca 2009) has presented that interpretive, positive and vital are the considerations factors for the information systems studies. In this research, academics usually choose the interpretive factor so that we concentrate on this approach.

5.2 Selecting the Case Study

The criteria of choosing the research methods is based on decision making choices that is related to the knowledge, beliefs and expectations as discussed above. Also, the study or thesis questions could affect the way of selection (Berndtsson, Hansson, Olsson, and Lundell 2008). Even more; case study method is concerned about a specific aspect, system, or organisation (Mardziel, Magill, Hicks and Srivatsa 2011), as well as, it is specifically useful in case of studying less understandable situations (Vacca 2009).

Quantitative and qualitative research methods could be chosen or selected based on the research or study methodology (Huang, Yang, and Calmet 2006). Also, (Subramanian 2008) has presented that knowledge, expectations and perceptions of individuals are important, and ideal study approach for the information systems studies is the qualitative approach. Therefore, in this research, case study methodology is meant to be the typical approach.

Interpretive is part of many philosophy science types of researches (Matsumoto, Hayano, Kudo, Yoshida, Imai and Ohshima 1991). According to Kaplan, Truex, Watell, Wood-Harper and DeGross (2004), academics must try to make their thanking basis and ideas of their researches easy to ready in the customer or reader side. Also, the case study research method in this thesis is following the default framework that is used worldwide by following the peer reviewed documents (Klein and Myers 1999), along with, the background knowledge that has been earned during the postgraduate study and the work experience that had been earned during working as information systems (IT engineer and team leader) professional in the selected site as case study for this research, during the twenty first century via high level of education and super intensive work experience around the same field of study (information systems) have reflected the views, way of thinking and expectations.

The main part in the case study is the case. Khosrowpour (2000) presents it as ‘a phenomena that occurs in the texture’ (p. 945). Practically, a case is in the heart of analysing a study. According to Chakrabarty, and Tan (2008), the analysing samples could be humans, software, companies, or even incidents. Few employees or end-users could be chosen as analysing samples when there are many critical and shared characteristics (Khosrowpour 2000). In this study, we would like to study employees’ and end-users’ expectations of information security policies within the organisation. It is better to study various groups of employees as a single case study rather than study one specific group of employees in many case studies. Therefore, this study focuses on the understanding and awareness of employees and end-users toward the information security policy, security countermeasures, internal and external threats. This is along with deploying a case study in seeking for better explanatory study, so that, studying one case with detailed concentration is better than studying various ones (Subramanian 2008).

Therefore, this study comprises theoretical framework which concentrates on analysing the internal threat in order to minimise the risks, along with, studying end-users’ expectations towards the security countermeasures. In the other hand, an empirical study concerned about a single case study where IS policy is currently deployed within a chosen organisation.

5.3 Organisation's case study selection

The case study's location was chosen based on my own experience as an employee (Since December 2004) at the selected site, along with, colleagues willing to participate in this study. The organisation, the central bank of Libya (hereafter, CBL), has an national payment system that was a project around ten years ago and took place as a live system around four years ago, however, there have been security concerns about the NPS information assets as it had been transformed from just a project to a live system serving many banks with their branches around the country in a centralised huge data centre. Also, employees, end-user and even decision making persons have been suffering a lack of information security awareness. Even more, culture, lack of security roles, penalty fines, and many more factors are still affecting the employees compliant toward the information security policy. Furthermore, security professionals and officers are not qualified to manage security at the bank; training about security has not been offered to employees neither security officers, as well as, knowledge background about security is poor.

Although Bashir (2008) implemented and deployed an information security policy around four years ago, there have been security concerns due to security breaches that happened either accidentally and on purpose. Also, internal threat and security threat has not been mentioned in the existing information security policy.

Therefore, conducting this study is essential, as well as, employees' participation in the study is important, this reflects the employees and end-users expectations about the information security policy importance, along with, their awareness about the internal and external threats risks and the importance of the regular training about security.

As an early step towards understanding the study, choosing four groups of the organisation's employees whom work in different positions to study is typical (Barratt, Choi, and Li 2011). Three employees have been selected as group of the responsible employees; system administration duties are critical for the CBL either database or production servers administrators. These employees have information system and security's experience, and they are responsible for ensuring the secure management of the CBL's information assets. Some of them are located in the main datacentre which is at the CBL's main headquarter, and others are located in the backup site. The group forms 3 various organisation's levels: IT manager, system administrator and end-user (see Figure 4).

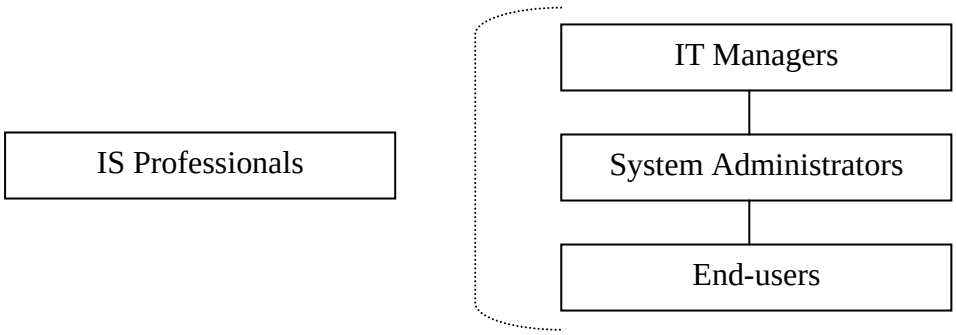


Figure 4: *groups of the organisation's structure, adopted from Ward and Peppard (2002)*

Later, I realised that at least one security professional employee should be consider along with the others, and it would be ideal if an inside look from the information security policy could be provided by one an information security policy's creator. Although IS professionals work at the CBL's headquarter, there is no IS professionals or officers at the bank up site.

When choosing an interpretive research, academics must define their roles relating to the case study (Bloom and Van Reenen 2010). (Bloom and Van Reenen 2010) have presented that academics included in the interpretive researches could be considered as observers to a legitimate researchers. It is meant to be said that although informants' understanding or participated employees within an organisation usually influenced by researchers (Ward and Peppard 2002), in this very situation, the researcher is a colleague of informants. However, I cannot consider the observer term for me as the study was initiated by IS professionals; these employees have been suffering lack of training along with the employees within the CBL. Therefore, the interviews that were conducted for this study were friendly and transparent.

5.4 Data Sources

Klein and Myers (1999) suggest that main source of information for a case study research is conducting interviews. Also, interviews are the main source of information in this thesis, as well as, personal experience at the CBL as a responsible IT engineer and team leader, informal contacts and documentation at the CBL. Furthermore, I had noticed myself how some employees dealt with the information security policy for the NPS, so that, observation was onsite by the researcher in this study. Table 3 shows the study's data sources summary gathered in the period between January and May 2012.

Table 3: *the study's data sources summary (between January and May 2012)*

Task	*Description*
Literature reviews	Reviews of literature on internal & external threat and IS policy. Security countermeasures and principles peer-reviewed journals.
Personal experience	Own experience at the selected site for this research as a case study from a technology point of view (IT engineer and team leader) for six years.
Informal interviews	Informal conversations and interviews about the NPS information security policy with employees from within the organisation.
Internal documentations	Access to the internal documentation of the NPS and the information security policy.

Interviews are considered to offer a qualitative method for researches that are set to study the understanding and awareness of informants or employees and to express their field or work experience in particular field or area (Kaplan, Truex, Watell, Wood-Harper and DeGross 2004). In this research, including the different employees' expectations in various positions

of the information security policy for the NPS along with considering the personal experience at the CBL assisted perfectly to a better understanding, as well as, the conducted interviews helped in picturing the whole ideas about the background knowledge of the informants or even for the organisation. According to Cagiltay, Aydin, Aydin, Kara and Alexandru (2011), informal interviews should not be too friendly nor high weight questions. So that, the conducted informal interview is either a telephone conversation or light weight questions by Email. Also, these conducted interviews present a basic framework and highlight the subject and tasks that need to be covered; this may better improve the quality of information given by informants, employees or interviewees Klein and Myers (1999). This approach is perfect for this research as the relationship between the interviewer and the interviewee is good and based on a long term relationships as colleagues. In the other hand, without a good relationship between the interviewer and the interviewee and experience mostly do not lead to consistent data or lack of information to finish the purpose of the research (Kaplan, Truex, Watell, Wood-Harper and DeGross 2004).

Informal interviews and the documentations of the CBL along with my personal experience at the bank for around six years in the information system field have offered me a complete background about this specific organisation. Even more; myself and the informant whom have been in contact to offer informal interviews are aware of the existing information security policy at the bank which has been implemented for the national payment system before it has been implemented during the NPS implementation stages as a huge project until it has been gone live. The documentation of the NPS – documentations of finance and the CBL presentation documentation have been useful for this research as key and vital areas have been spotted, these areas could be used or in other words included during the informal interviews. Therefore; these informal interviews with these documentations along with my personal experience were all used in gathering information and data collections as data sources which lead to a better understanding of the weak points in the current information security policy for this organisation.

According to Becker and Burke (2012), in order to receive better results to do the analysis and comparison more accurately from the informal discussions, a better knowledge and understanding of the organisation's objectives and information security policies along with using various techniques to do such informal interviews were essential. Even more, one short highlighted interview and one long detailed interview were made with two system administrators to practice the different techniques and gather some data for this research in the system administrator point of view. Five semi-long interviews, around thirty minutes each, were made between March and April 2012. All the informal discussions took place during more or less one month, in a friendly and frankly manner, were close to the organisation's information assets and security management. Also, individuals were chosen from different positions based on the variety to receive a different data to achieve a better comparison. Even more, (Sinkovics and Penz 2011) have suggested and concluded that using an interview guide when conducting informal discussions are essential, so that, indirect and direct queries were used.

5.5 Analysis of the Gathered Data

Data sources have offered informal discussions and interviews documents along with the personal experience as practical notes right on-site. Understanding and Background knowledge amongst the all the sides of the data sources and literature reviews and peer-reviewed journals of the analysis if the gathered data all together helped in forming the theoretical framework for this research. Also, one of the most used data analysis techniques in researches that use interviews and documentation as data source is matrix (Miller and Horowitz 2006); matrix technique could be done in case of visualisations needed. During the analysing process, queries have been made against the results, data sources, and conclusion in the end and reform was necessary to make as data appeared to be inconsistent with the output when a better understanding was achieved in a short time according to the university schedule for this study semester, the research was set up and scheduled for around thirteen week.

Regarding the theoretical basis for this research, security countermeasures, internal and external threats were included in the interviews as questions and queries to consider the employees' understanding, background knowledge and expectations toward these aspects when implementing the information security policy within the organisation. Various informant or employees were selected and interviewed based on the variety of positions (Gershman, Fink, Bin Fu and Carbonell 2009), the applied variety offered a various sources of data to be taken from the individual point of view based on his own job description starting from an end-user to a decision making officer which allowed categories to be created based on the individual's position or job description. These categories were studied separately and then comparison was made between these categories to find out the difference and variety of data sources from different views. Furthermore, these categories were studied along with their given data against the analytical templates (Lindgren 2009). The comparison and study resulted into three categories that used to refer to the previous categories.

According to Cohene and Easterbrook (2005), analysing the gathered data must be achieved by examination, studying, testing and categorising the gathered data from the data sources. Therefore, analytical patterns have been used in this study. As mentioned earlier, countermeasures, internal and external threats were the main purpose and under focus during the conducted informal discussions and interviews, so that, individual's expectations and security countermeasures were analysed against the categorised analytical pattern templates and resulted into two set of data identified in tables that contain categories and descriptions. These tables comprise categories and their given data. The analysis resulted in, given data was less identical. Categories along with the presented ideas and discussions were discussed with the individuals with the goal of examining the proposed solutions and ideas to the problem (Kemp and Ots 1998). In the end, the theoretical framework in this study was used to analyse and study these categories against the security countermeasures, internal and external threats aspects.

5.6 Study Evaluation Criteria

Academics have advised various ways to evaluate the case study researches. The key point in the information security field of science is to form a group of principles for this type of researches (Kaplan, Truex, Watell, Wood-Harper and DeGross 2004; Klein and Myers 1999). These method has been a standard to evaluate this type of researches recently, case study researches always need to be examined to verify the quality of this type of research, the set up method or principles are directly related to case studies (Kaplan, Truex, Watell, Wood-Harper and DeGross 2004). According to (Klein and Myers 1999), discovering the right goal is needed along with validation and examination of the study results. Also, the interpretive research does not have specific goals in the nature of science (Kemp and Ots 1998). Therefore, regarding this research, the results of this research are based on our understanding, background knowledge, studies and researches and then the goals of this study. Despite of the researcher introduction and the set up goals of the researches, also in the valuable useful researches, the researcher's point of view may have been seen as unbiased point of view in terms of the study as a whole research, but rather it should be considered positively (Sinkovics and Penz, 2011). This may affect in finding or examining the outcomes of the study negatively, also, in this assumption, it would not be appropriate to use validation to evaluate. In the other hand, positive studies 'valuable efforts are widened in order to increase the quality of validation of the results and outcomes', in interpretive studies 'valuable efforts are widened to raise awareness of own expectations, so that, the object idea becomes transparent and clear' (Kaplan, Truex, Watell, Wood-Harper and DeGross 2004, p. 84).

This research and its outcomes must be validated via various criteria. Although using some criteria to validate interpretive study may violate the nature of such research (Kaplan, Truex, Watell, Wood-Harper and DeGross 2004), this type of researches are still should be evaluated and validated, this could be achieved by using standard principles (Klein and Myers 1999). Even more, (Kemp and Ots 1998) have argued that using and applying any standard principles or criteria decrease the risk of validation the interpretive research inappropriately. Researchers have followed various criteria for interpretive researches; however, the standard worldwide principles used in this research have been suggested by (Kaplan, Truex, Watell, Wood-Harper and DeGross 2004; Klein and Myers 1999). Also, these principles are typically sat up for case study of interpretive research evaluation (Kemp and Ots 1998). Even more, from a former employee point of view, this type of studies or researches need the researcher to live and practice in the selected research site for as long periods as possible in order to do a better study those researches and get more accurate information about the selected site and individual, such criteria is suitable in this case as the researcher is a former employee of the studied organisation.

Klein and Myers (1999) and Kaplan, Truex, Watell, Wood-Harper and DeGross (2004) have presented seven principles for interpretive case study research analysis, validating and evaluation. Klein and Myers (1999) have developed the following seven principles: [1] the basis; [2] contextual; [3] academics and subjects interactions; [4] generalisation; [5] dialogue logic; [6] multi translations; and [7] suspiciousness principles (Klein and Myers 1999). Even more, I think that [8] internal objects principle should be added to these seven principles in

this case study specifically as I personally was a former employee at the organisation. Therefore, this point of view should be considered during the evaluation process.

The first principle is the basis of these criteria; all other principles are based on the fundamental principle. This principle is based on the philosophy of the studies and it was discussed earlier in this chapter. Principles two and three represent the pros and cons of the study in specific situations. The fourth principle represents the study socially in order to explain to the viewer's how this this research was emerged. Inter-relationships amongst organisation, information systems and employees are not static, as well as, organisations are dynamic in nature, not fixed; every research is different. Therefore, the interaction principle needs the interviewee, individual, and researcher to be in a social situation. The interpretive studies do not just offer a sort type of data to be gathered, but these types of data is a result of social communications amongst the interviewees, individuals and researchers (Klein and Myers 1999). Also, the principle needs vital study about how the study's documentations or information are socially conducted during the interviewees, individuals and researchers interactions (Kaplan, Truex, Watell, Wood-Harper and DeGross 2004). The generalisation principle is dependant to the general context of the research outcomes. The dialogue logic principle is dependent on the interpretive research understanding and expectation, as well as, background knowledge and all of these factors are essential (Klein and Myers 1999). Also, the researcher must be unbiased and present the research's philosophy in a transparent manner and clear understandable material to the viewer or to the other researchers, as well as, for the researcher (Kaplan, Truex, Watell, Wood-Harper and DeGross 2004). Furthermore, this principle says that there are possible conflicts between the final outcomes and the study's theoretical basis, so that, the researcher must be keep this in mind. The multi translation principle, in other words interpretation, it needs considering all aspects of the interviewees on how they may perceive the same question in different cases. The seventh principle, it represents discovering the untrue expectations and conceptions, it asks the researchers to clear the unclear aspects that were caused due to social or cultural reasons of the interviewees or the participants (Kemp and Ots 1998).

In the other hand, the thesis was scheduled and managed for thirteen week due to the university schedule and regulations for this study semester. Therefore, the evaluation process may not be optimal or ideal due to the short time that has been offered to gather the data, as well as, to analyse and evaluate the data afterwards. However, this could be achieved quite well in terms of doing a primary research that needs future work and further reading in the near future.

6 Case Studies

Chapter six comprises the theoretical and practical parts of the research. According to the contextual principle by Klein (1999) and his colleague, the chapter introduces the context of the research by presenting the organisation briefly, as well as, presenting a glance about the information security policy of the organisation. By following the proposed presentation briefly, the reader or the viewer of this study could understand the existed state at the organisation and how educating the organisation's employees about the internal and external threats, along with, presenting the studying targeted groups at the organisation should give out a clear understanding about this study.

Furthermore, how well this study could be for improving the current information security policy since it was implemented lacking enough information about the information security policies standards, as well as, lack of awareness about the internal threats and security training courses. In addition, this chapter comprises the targeted groups to be studied in order to understand their behaviour toward the IS policy at the organisation.

6.1 CBL

The main purpose of the case study is to present and study the expectations of the targeted groups toward the IS policy of the organisation in the biggest data centre in Libya. The NPS is a national payment system that comprises three different systems within; Real-time gross settlement, automated clearing house, automatic check processing, automated teller machines and point of sales. These systems hardware reside in a large main and backup data centres.
These systems offer banking services to more than four banks with more than three hundred branches all over the Libyan cities, as well as, the located data centre at the Central Bank of Libya provides network access and support services.

The NPS went live in 2008 (The Central Bank of Libya, 2008), so that, an information security policy was needed in order to secure management of these systems (Bashir 2008) and to secure the information of the NPS in general from the various threats. Although the information security policy was implemented in 2008 (Bashir 2008), it has not been improved since then, as well as, internal threat has not been included in the information security policy.

Even more, there has been a great concern about the securing the NPS information assets sue to lack of security awareness due to lack of regular information security trainings (CBL 2008). CBL has a small department looking after security as a whole, however, there many huge systems that running under the central bank organisation, as well as, the inside own core system for the central bank branches.

6.2 Information Security Policies at the CBL

In this study, the study is concerned about the NPS system as a sample or sector of the CBL organisation due to the limited time that has been offered on behalf of the university in order to start in finish the study in thirteen months. Generally, the adoption of the information security policy for the central bank was initiated by the CBL's governor in 2008 (Bashir 2008), Bashir has presented that in order to secure the information assets of the central bank,

all the systems and processes, hardware, software and resources need to be secured by setting up roles and attach responsibility to every role.

Furthermore, information security policy based on the international standards is essential and crucial in this case in order to secure the management of the information assets in the central bank, therefore, he suggested a security plan that comprises seventeen items representing the terms of the security plan for the central bank (Bashir 2008). According to Bashir (2008), the security plan terms consist of; security policies for employees and contractors, information assets protection levels, access control, password and users management, physical security, Email server accounts security, personal security, encryption, remote access, maintenance, anti-virus, backup systems, response management, network security, continuity, telecommunication security, and security monitoring.

Various important aspects have been mentioned and included in the information security policy. However, countermeasures, training, internal and external threats have not been under the scope when the information security policy was implemented in 2008. Therefore, changes and improvement in the current information security policy for the CBL in general are needed urgently as precautions, as well as, risk analysis.

The information security policy is issued by a separate department that concerns about securing the information assets of the central bank. The information security policy instructions, or in this case study, the security plan terms have been approved and in place for around four years, these instructions or terms are in the security plan document version one, so that, it has not been improved nor changed for around four years.

The information security policy in the CBL was initiated by the CBL's governor due to the nature of banking businesses and services in the modern's information systems field. There has not been a systematic methodology or process to follow this information security policy within the organisation, but as a guidance to follow the security international standards. However, these set of term and security regulations have not considered the internal and external threats.

Also, there has been just one general information security policy for the CBL concerning all the information assets of the central bank in general, but not specifically, this means that there are no separate documents or guidance dedicated to the various sectors within the bank, such as group security guidance; separating the security regulations and guidance based on the nature of the job description, department or position (Klein and Myers 1999).

There have not been a clear security countermeasures and punishment system in case of a security breach employee's incompliance behaviour towards the information security policy.

However, the security of key information systems have been checked regularly through team leader and line managers in terms of information technology processes and tasks, such as, password management, backup operations, health system check and maintenance.

6.3 The CBL Organisation's Groups

There various organisational groups in the central bank of Libya, however, due to the short time that has been offers for this study as well as the available informants that have been contacted from the central bank to participate in this study led to categorising the participants into four categories based on the study of their expectations about the current information security policy as well as their positions at the central bank. This study is specifically concerned about the information security policy for the NPS at the central bank, therefore, all the informants and participants are either responsible about the security, or managing information systems for the NPS. These informants and participants represent various organisational levels at the central bank. These employees are described as; information technology officer or manager, system administrator, and end-user. These are the job description roles, or positions related to the information systems, as well as, the information security policy. Information security officers would be the fourth level in this case, they are responsible for securing the organisation's information assets, as well as, they are responsible for information security policy implementation and management (see Figure 4). All participants and informants are located at the central bank headquarter.

Information security officers are employees of the central bank and they are located at the central bank headquarter, however, the backup site for the NPS information systems are located in another location where there no information security officers at that location. Choosing in informant or participant from the security department (IS Officer) was necessary (Kaplan, Truex, Watell, Wood-Harper and DeGross 2004), so that, information security experience was needed for this study as the rest of the informants and participants suffer a lack of information security experience or security background as this study is concerned about the information security policy and information systems, therefore, choosing both experiences informants each one in his field was important for this study.

IT managers as well as team leaders at the central bank are the ones who responsible for information systems at the organisation; hardware, software, programs, systems, databases, and network maintenance and upgrades. This point of view comes from a personal experience at the central bank where I used to work as team leader and system administrator, even more, I worked as coordinator between the information technology department whose responsible about the NPS system's implementation and the third executive party whose responsible of executing the project and building the data centres for the whole project. Since the team leaders have been reporting the security status, the understanding of reporting about security has been based on an IT point of view due to lack of information security background.

System administrators were expecting that information security policies would bring up advantages for me and them, saying that, the expected outcome was seen as truth moment and these information security policies would help discovering the amount of responsibilities that are related to managing the information security and how critical that could be. They only viewed the information security policy for once when they had to declare and sign that they aware of the new information security policies that need to be applied for the NPS.

IT team leaders have been concerned about the information security policy in terms of that these policies should offer ways to guarantee that information systems are secured, so that, they would be less worried and less nervous in terms of the amount of responsibilities that related to the security issues and risks. Their perception is seen as they think that information security policies are widely related to the information systems, rather than, the organisation's assets as general.

End-users have been the suffering in terms of information security awareness as they have not had any training about information security. They have not been following the information security policy as there have not been a strict security countermeasures and fines.

- **Documentation**

The documentations that have been used for this study are; CBL information security handbook (Arabic version) and web documents that are available on the CBL web page (i.e. security plan's terms and NPS information page (Bashir 2008)).

- **Informal interviews**

In order to define the internal threat, interviewing the organisation's employees was necessary. The interviews were made informally, either by informal emails and conversations with three different levels of employees in terms of responsibilities. End-user, system administrator and team leader were interviewed and asked by the same questionnaire in order to find out the employee's background knowledge and expectations of the security countermeasures if applied, as well as, the internal and external threats awareness.

- **Observations**

Due to my personal experience as a former employee at the selected organisation as case study for this research, my personal previous observations along with interviewing the participants who are already working there currently together helped to perform accepted and useful observations (See Appendix B, C).

Analyses

In this study, my personal experience at the chosen case study, along with, the selected groups that were willing to participate in this study toward the expectations of the information security policy are analysed via the theoretical framework that is based on literature reviews of information security policies standards, security countermeasure, internal and external threats awareness. The analysis has been performed using the gathered data that is based on the information on Chapter six.

The organisation is a bank, in face, the central bank of Libya, it regulates, monitors, provides services to all the banks in Libya either, public and private banks with their branches. The central bank comprises various production systems, however, in this study; the focus has been on the NPS systems due to my personal experience working for around six years at the bank regarding this system's implementations.

Since, we are concerned about information security in this study; there has been a great concern about the information assets and managing information security in terms of information security policy at the bank. Also, there has been a great concern about information security at the bank due to all information is centralised in a big data centre which located at the bank headquarter where I personally worked. Therefore, security countermeasures along with internal and external threats awareness amongst the employees and how they expect and perceive toward the information security policy was necessary.

The IT department of the organisation has various sub-departments related to the various production systems, however, the security department which responsible for the security regulation's issuing and monitoring is separate.

NPS department comprises of three different departments; each sup-department comprises end-users, database administrators, system administrators, and team leaders, however, there are no information security officers, so that, the team leaders are responsible of secure management of the systems. The number of employees in the NPS department is around twenty five employees.

There has not been a security breach reported so to speak, however, there has been a great concern about the organisation's information assets security due to lack of background information about information security, security countermeasures, internal and external threats. This concern is understandable as malicious actions from insiders and security breaches happen at any time.

Therefore, the organisation should be concerned about it and care about it by following the international standards of security in general and information security policies standards particularly (Kemp and Ots 1998).

Furthermore, after analysing the gathered information from the informants about these aspects of this study, we found out that, employees are not fully aware of the risk of the internal and external threats may cause, as well as, there has been no employee fined or punished of security incompliance.

Despite the organisation was founded around fifty years ago, as well as, the NPS system was set around ten years ago, the information security policy was approved, implemented, and distributed only in 2008 (Bashir 2008). Information security officer was not expert enough to implement an information security policy within the organisation, so that, various aspects

have not been included in the information security policy such as, security countermeasures, internal and external threats, as well as, there have not been any improvements on the information security policy since it was implemented in 2008.

In this case, the lost data or information is considered a financial loss, so that, this is very critical. Also, failing to deliver is considered a financial loss in terms of banking services and systems. Therefore, security countermeasures and safety should be considered, approved and applied to all departments, services, processes and businesses in order to achieve risk mitigation.

The interviews along with my personal experience helped to understand that a set of security related documents are needed in order to explain to the employees that they would be hold against a security breach.

These documents are security related and should be distributed amongst the organisations employees who are working in the IT field in order to mitigate the risk and improve the level of security within the organisation.

According to my personal experience and some interviews, the leaving employees rate is very low or almost zero, so that, most or even we could say all the employees work in the organisation until they retire, therefore, there has not been a security regulations in the information security policy concerning the fired or left employees case which I believe now there has to be mentioned in the information security policy as some fired or employees that leave the organisation may commit a security breach in order to gain a finical advantage or even as a revenge.

Regarding physical countermeasures, according to my personal experience and the interviews, many countermeasures have been defined; username/password, access control, physical security to the organisation's datacentre, network monitoring and CCTV cameras.

According to the interviews, they have not had regular information security training, as well as, personally, I did not have any information security training during six years working between IT engineer, system administrator, and team leader. Also, decision making persons within the organisation are not fully aware of the need of organising regular information security training for the IT employees, user-entry, system administrators and even employees in general in order to educate them about the modern threats and secure management of the organisation's information assets in general.

According to the ISO, he has had an information security training three years ago, there was not a regular scheduled training, and however, the rest of the different employees have not had any regular scheduled information security training.

Each employee has been offered a training about his job description, in some departments and cases, some employees are offered a regular training about his job position either, once every year or two years, such as, database administration, server maintenance, backup and upgrades. However, there has not been regular information security training.

According to the interviews, the security culture within the organisation is tight and strong, as well as, number of employees is small and quit or fire rate is small. Therefore, this affected the information security policy within the organisation in a good way, where, employees' security behaviour is stable. However, the security department is separated from the IT department, and the IT department itself is dispersed in terms of management level and administration level.

According to the interviews, as well as, my personal experience, IS has not been on great focus in the CBL due to the physical separation between administration, security, employees' departments. Therefore, IS behaviour is difficult to monitor, end-users do not feel the importance of the information security policy. Also, there has not been an annual rewarding system to motivate the employees. However, the rewarding system improves the employees' production, knowledge, security behaviour, as well as, it improves the level of security within the organisation.

Four different groups have been selected to participate in this study, some of them they understand the importance of information security policies within the organisation in order to protect the organisation's information assets. According to the interviews, as well as, my personal experience, table 4 shows the employees' expectations of the information security policy and differences of these different groups within the organisation.

Table 4: *Employees' expectations of the information security policy and differences*

Group	*Interview's Information*	*Description*
IT Managers	*I think that my security background tells me that everything is alright. I have a lot of work to do and always busy with the paper work and meetings. I believe that we have a good level of information security.*	IT managers or in this interview team leaders expect that information security policy offers a tool to check and ensure the proper level of information security within the organisation.
System Administrator	*As System Administrator pint of view how is looking after the production servers, I can tell you that information security policy is essential to inform and force employees to comply.*	IT level engineers are more aware of the information security policy as they are in direct contact with critical systems as a daily job work nature. Also, some of them manage user accounts such as DBAs.
End-users	*Honestly, I do not have a security background; however, I think that doing the daily housekeeping job is just fine.*	End-users expected that imposing the information security policy would not affect their work in anyway.
Information Security Officers	*Well, I am working in a separate department with few employees looking after the security as whole, so that, we have to spot any incompliance to the information security policy and fix it by educating the employees about this specific security issue.*	IS Officers were expecting that information security policy would help to improve the employees' security behaviour by informing them that these instructions are 'a must follow', so that, they will comply with it.

IT Manager or IT team leader in this case has read the information security policy from his own point of view and perceived it from a narrow perspective, he expected that information security policy would provide and offer some tools that lead to a steady state of the information security state within the organisation.

IT level engineers are more aware of the information security policy as they are in direct contact with critical systems as a daily job work nature. Also, some of them manage user accounts such as DBAs.

End-users expected that imposing the information security policy would not affect their work in anyway. Finally, IS Officers were expecting that information security policy would help to improve the employees' security behaviour by informing them that these instructions are 'a must follow', so that, they will comply with it.

Therefore, after all these different expectations, of course, all of them have been concerned about the responsibility matter and who should be held accountable when a security breach happens.

The participants in this study have been working for five to seven years at the organisation. Two of them stated that employees have never been a threat to the organisation's information assets; however, another two employees stated that employees could be a threat to the organisation's information assets without having background knowledge about the term internal threats.

There has not even been a single security breach reported from an insider within the organisation so far, however, some employees believe that employees could impose a threat. In the other hand, there has been some level of threat due to some careless employees mainly because lack of awareness about the information security goals, objectives and policies.

According to the interviews, expectations and awareness of the security countermeasures are shown in the table below (See Table 5).

Table 5: *Security countermeasures awareness and comparison*

Group	Awareness	*Rewards*	*IS Policy*
IT Managers	Training Achieved	Yearly	Viewed Once, when received
System Administrator	Never	Usually	Viewed Once, when received
End-users	Never	Never	Never
Information Security Officers	Regular Training	Never	Issued Once since 2008

Security countermeasures have been only applied in terms of technology, such as; access control, physical control, passwords, etc… however, it has never been applied in terms of punishments, such as; fines and firing.

Even more, as noticed from my own experience and interviews, the current information security policy has never been updated nor improved since it was implemented in 2008, as well as, most of the employees who were ordered to hand over and sign the information security plan within the organisation are either, have viewed it once or have never received one.

Also, the employees' security behaviour is related to their own experience and learning from the others. However, lack of awareness about information security is a fact within the organisation as most of the employees have never had training about information security.

Furthermore, the security behaviour mainly comes from their experience working as IT engineer, database administrators, and system administrator as well as their skills in these aspects. However, these employees who work mainly in the IT field, they are not fully ware about the modern threats such as; internal and external threats, as well as, attacker's techniques due to lack of awareness.

Therefore, information security training should be scheduled in a regular basis.

8 Conclusions

The main goal of this thesis is to increase the employees' awareness and understanding of information security policy through studying their expectations of the information security policy within organisations, as well as, how security countermeasures and employees' awareness may help to decrease the internal threat risk within organisations. In order to achieve this goal, I have used the literature on information security policies and collected data from the selected case study.

The answers to the research questions in the beginning of the study have been solved and clarified through this thesis by adopting a case study. Interviews were conducted with employees within the organisation to clarify, verify, and evaluate this study. Therefore, security countermeasures must implemented and applied along with clear statements of tasks and fines or penalties in case of security incompliance, so that, employees will be informed clearly as their satisfaction and contribution is essential to decrease the internal threat risk as well as security breaches in order to achieve a better level of security within organisations.

Although many organisations (e.g. CBL) worry more about external threat rather internal threat, internal threat impact could be vital within organisations. Therefore, considering employees' perceptions when planning and implementing information security policies is essential, as well as, information security training should be scheduled in a regular basis considering employees' profession; IT Managers, IT engineers, end-users, etc…

The findings and conclusions from the selected case study; without a regular awareness and training about information security goals and objectives within the organisation, information security policy itself is useless as well as employees' security behaviour is affected in negative way. Security countermeasures have been only applied in terms of technology, such as; access control, physical control, passwords, etc… however, it has never been applied properly in terms of punishments, such as; fines and penalties in the critical cases. Most of end-users and user entry employees have never seen nor received an information security policy or information security terms plan, however, they have been following the information security policy due to informal norms and cultural factors. Furthermore, privacy issue in terms of information security in case of their work would be monitored by various tools has been discussed with the interviewees and they agreed that these tools are useful and help in

protecting the organisation's information assets in a certain way, we would accept after discussion and under our knowledge.

Finally, Deploying and distributing a successful information security policy within organisations is not easy and studying new ways that lead to practical improvements to the information security policy has been always a concern amongst academics and information security professionals. Information security policies have been shared and concerned amongst executives and high level managements, however, academics have been focusing more on the lower levels within organisations, such as end-users and how they perceive the information security policy by suggesting methods to motivate them to comply to the information security policy, so that, they do not turn into an internal threat, or even help to decrease the internal threat risk.

Therefore, in this thesis, the final conclusion is, employees' perception of information security policy should be sought and included when implementing information security policy within organisations, as well as, information security training should be scheduled in a regular basis.

8.1 Research Limitations

In this thesis, research and study schedule has been made to start and finish in around three months' time only. This time window has been set by the university for this semester from March 2012 to May 2012. Therefore, I managed to interview four interviewees regarding the selected case study, there has not been enough time to consider and ask more informants who are willing to participate in this study from the selected case. Also, I focused on one particular department within the selected organisation to study in terms of information security policy and employees' security behaviour, however, if I had more time, I would have included at least another department or even another branch of the organisation that is physically located in a different location than the headquarter to be able to make a comparison and better quality findings.

Even more, the selection of the case study was based on my personal experience and observation as I was a former employee at the selected organisation for this study, so that, I was the best to spot the problems and obstacles in terms of information security policy as well as to conduct those interviews. However, I also have been facing some difficulties in contacting some more informants due to the situation in Libya.

Finally, the findings in this study may not be considered as general or global outcomes that could be used worldwide, because of the selection of a single case study, as well as, small number of interviews. However, these outcomes could be used for some countries that share similar culture.

8.2 Further Study

Researches usually result in more inquires than answers. Of course, after answering the three main questions in this thesis, more questions and inquiries have come up. However, this could be considered as a positive matter as it inspires materials for future work or further study. So that, some questions related to this study's topic that worthy to establish studies for are; In this study, I focused on employees' expectations as general or shared point of view for all within the organisation, however, research on ISPs should be deeper, that means different organisational employees should be split into different groups so that studying employees' expectations of ISP deeply would result in a better understanding.

Since, the selected case study for this thesis was the CBL, and the CBL itself has not implemented online banking system so far so to speak, therefore, in terms of this study's topic, there is a need to further studies and future work about the external threat risk (Caruso 2003). Although the internal threat has been considered more harmful impact on organisations than external threat, external threat risk's impact, effect, and analysis should be performed before announcing the internet banking service or even before implementation.

Furthermore, according to (Gibler and Douglas 2010), 'some external threat risks affect potential politics specifically' (p. 54). Since, the CBL is a large central organisation that offers banking services to the entire banks in Libya as well as the CBL manages and regulates them, therefore, in this aspect, external threat is considered a vital threat as this type of risks could happen from overseas.

References and bibliography

Al-Hamdani, W. (2009), Non risk assessment information security assurance model, *ACM proceeding Information Security Curriculum Development Conference*, (25-26 September), pp. 84-90

Alexander, D., French, A., Taylor, A. and Sutton, D. (2008), Information Security Management Principles, Swindon, UK: *The British Computer Society*

Alfawaz, S., Nelson, K. and Mohannak, K. (2010), Information security culture: a behaviour compliance conceptual framework, *ACM AISC '10 Proceedings of the Eighth Australasian Conference on Information Security*, (Volume 105), pp. 47-55

Barratt, M., Choi, T. and Li, M. (2011), Qualitative case studies in operations management: Trends, research outcomes, and future research implications, *Business Source Premier Journal of Operations Management*, (Volume 29, Issue 4, May), p329-342

Bashir A. (2008), Information Security policy in the Central Bank of Libya, *The Central Bank of Libya*. [WWW] Available from: http://cbl.gov.ly/eg/index.php?option=com_content&view=article&id=61&Itemid=68 [Accessed 05/04/12]

Becker, W. and Burke, M. (2012), the Staff Ride: An Approach to Qualitative Data Generation and Analysis, *Business Source Premier Organizational Research Methods*, (Volume 15, Issue 2, April), pp. 316-335

Berndtsson, M., Hansson, J., Olsson, B., Lundell, B. (2008), Thesis Projects A Guide for Students in Computer Science and Information Systems. 2nd ed. London: Springer-Verlag

Bertino, E. (2011), Protecting information systems from insider threats - concepts and issues, *IEEE International Conference on Information Reuse and Integration*, pp. xxiv-xxv

Bloom, N. and Van Reenen, J. (2010), New Approaches to Surveying Organizations, *Business Source Premier American Economic Review*, (Vol. 100, Issue 2, May), p105-109

Bodin, L., Gordon, L. and Loeb, M. (2008), Information security and risk management, Magazine Communications of the *ACM - The psychology of security: why do good users make bad decisions?* (Volume 51 Issue 4, April), pp. 64-68

Breier, J. and Hudec, L. (2011), Risk analysis supported by information security metrics, *ACM Proceedings of the 12th International Conference on Computer Systems and Technologies*, (16-17 June), pp. 393-398

British Standards Institution (2005), Information technology – Security techniques – Information security management systems – Requirements, *British Standards Institution* BS ISO/IEC 27001:2005

Cagiltay, N.E., Aydin, E., Aydin, C.C., Kara, A. and Alexandru, M. (2011), Seven Principles of Instructional Content Design for a Remote Laboratory: A Case Study on ERRL, *IEEE*, (Volume 54, Issue 2, May), pp. 320-327

Carroll, M. (2006), Information security: examining and managing the insider threat, *ACM InfoSecCD '06 Proceedings of the 3rd annual conference on Information security curriculum development*, pp. 156-158

Caruso J. (2003), Information Technology Security Policy: Keys to Success, *University of Wisconsin*, volume 2003, issue 23, November.

Chakrabarty, A. and Tan, K.C. (2008), Case study analysis of Six Sigma in Singapore service organizations, *IEEE International Conference on Service Systems and Service Management*, (June 30-July 2), pp. 1-6

Cohene, T. and Easterbrook, S. (2005), Contextual risk analysis for interview design, *IEEE International Conference on Requirements Engineering*, (29 August-2 September), pp. 95-104

Cole, E and Ring, S. (2006), Insider Threat Protecting the Enterprise from Sabotage, Spying, and Theft, Canada: Syngress Publishing Inc.

DeRose, K. (2009), the Case for Contextualism, New York: Oxford University Press

Fugini, M. and Bellettini, C. (2004), information Security Policies and Actions in Modern Integrated Systems. Idea Group Inc.

Gershman, A., Fink, E., Bin Fu and Carbonell, J.G. (2009), Analysis of uncertain data: Selection of probes for information gathering, *IEEE International Conference on Systems*, (11-14 October), pp. 2227-2232

Gibler and Douglas M. (2010), Outside-In: The Effects of External Threat on State Centralization, *Business Source Premier Journal of Conflict Resolution*; Aug, Vol. 54 Issue 4, p519-542

Grama, J. (2011), Legal Issues in Information Security, Toronto: Jones & Bartlett

Gritzalis, D. (2003), Security and Privacy in the Age of Uncertainty, New York: International Federation for Information Processing

Huang, D., Yang, Y. and Calmet, J. (2006), A Knowledge-based Security Policy Framework for Business Process Management, *IEEE International Conference on Computational Intelligence for Modelling, Control and Automation, 2006 and International Conference on Intelligent Agents, Web Technologies and Internet Commerce*, (28 November-1 December), pp. 154-154

Jajodia, S. and Mazumdar, C. (2011), Information Systems Security: 7th International Conference, Berlin: Springer Verlag Berlin Heidelberg

Kaplan, B., Truex, D., Watell, D., Wood-Harper, T. and DeGross, J. (2004), Information Systems Research: Relevant Theory and Informed Practice, Boston: Springer Science Inc.

Kant, K., Meixing Le and Jajodia, S. (2011), Security considerations in data center configuration management. *IEEE 4th Symposium on Configuration Analytics and Automation (SAFECONFIG)*, Oct. 31-Nov. 1, pp. 1-9

Kemp, E.A. and Ots, S. (1998), Evaluating user interfaces using techniques from qualitative data analysis, *IEEE International Conference on Software Engineering*, (26-29 January), pp. 222-229

Khosrowpour, M. (2000), Challenges of Information Technology Management in the 21st Century, Idea Group Publishing, [WWW] Available from: http://books.google.co.uk/books?id=J1u7Mb5kmWgC&pg=PA361&dq=case+study+research+method+evaluation+in+organisations&hl=en&sa=X&ei=KbeiT6DdLumX0QWmx_DbDw&ved=0CDMQ6AEwAA#v=onepage&q=Central%20component%20to%20case%20studies&f=false [Accessed 03/05/12]

Klaic, A. and Hadjina, N. (2011), Methods and tools for the development of information security policy — A comparative literature review, *IEEE MIPRO, 2011 Proceedings of the 34th International Convention*, (23-27 May), pp. 1532 – 1537

Klein, H. and Myers, M. (1999), a Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems, *MIS Quarterly*,(Volume 23, 1st March), pp. 67–94

Li, Z., Yongchun, W. and Xuexia, W. (2009), Research of Information Security Risk Management Based on Statistical Learning Theory, *IEEE International Forum on Computer Science-Technology and Applications*, (Volume 3, 25-27 December), pp. 436-438

Lindgren, A. (2009), towards new methods for mobility data gathering: content, sources, incentives. *Proceedings of the 1st ACM International Workshop on Hot Topics of Planet-Scale Mobility Measurements*, pp. 1-5

Mardziel, P., Magill, S. and Hicks, M. and Srivatsa, M. (2011), Dynamic Enforcement of Knowledge-Based Security Policies, *IEEE 24th International Conference on Computer Security Foundations Symposium*, (27-29 June), pp. 114-128

Martinez-Moyano, I.J., Conrad, S.H., Rich, E.H. and Andersen, D.F. (2006), Modelling the Emergence of Insider Threat Vulnerabilities, *IEEE Proceeding of Simulation Conference WSC 06*, pp. 562-568

Martinez-Moyano, I.J., Samsa, M.E., Burke, J.F. and Akcam, B.K. (2008), Toward a Generic Model of Security in an Organizational Context: Exploring Insider Threats to Information Infrastructure, *IEEE 45th Hawaii Proceedings of the 41st Annual*, pp. 267-267

Matsumoto, M., Hayano, A., Kudo, T., Yoshida, H., Imai, S. and Ohshima, K. (1991), Specifications reuse process modelling and case study-based evaluations, *IEEE International Conference on Proceedings of the Fifteenth Annual International Computer Software and Applications Conference*, (11-13 Sep), pp. 499-506

Miles, G., Rogers, R., Fuller, E. and Hoagberg, M. (2004), Security Assessment Case Studies for Implementing the NSA IAM, USA: Syngress Publishing Inc.

Miller, J. and Horowitz, E. (2006), Algorithms for real-time gathering and analysis of continuous-flow traffic data, *IEEE Intelligent Transportation Systems Conference*, (17-20 September), pp. 1454-1459

Montelibano, J. and Moore, A. (2012), Insider Threat Security Reference Architecture, *IEEE 45th Hawaii International Conference on System Science*, pp. 2412-2421

Neville, C. (2007), Writing Your Management Dissertation or Project Report, University of Bradford, School of Management. [WWW] Available from: http://www.brad.ac.uk/acad/management/external/els/pdf/writingyourmanagementprojectreport.pdf [Accessed 09/03/12]

Pak, C. and Cannady, J. (2009), Asset Priority Risk Assessment Using Hidden Markov Models, ACM Proceedings of the 10th *ACM conference on SIG-information technology education*, October 22–24, pp. 65-73

Pearlson, K. and Saunders, C. (2009), Strategic Management of Information Systems, John Wiley & Sons; 4th Edition (Mar 2009)

Peltier, T. (2002), Information Security Policies, Procedures, and Standards, CRC Press

Peng, W., Yingwu, C., Sen, C. and Guoqing, Y. (2011), an information security risk management oriented multi-agent system, *IEEE 3rd International Conference on Communication Software and Networks*, (27-29 May), pp. 356-359

Pieters, W. and Coles-Kemp, L. (2011), Reducing normative conflicts in information security, *ACM Proceedings of the 2011 workshop on New security paradigms workshop*, (12-15 September), pp. 11-23

Quigley, M. (2005), Information Security and Ethics: Social and Organizational Issues, IRM Press

Schneider, R. (2010), a comparison of information security risk analysis in the context of e-government to criminological threat assessment techniques, *ACM Proceeding Information Security Curriculum Development Conference*, (1-2 Oct.), pp. 107-116

Shigematsu, T., Bin-Hui C., Hori, Y. and Sakurai, K. (2008), Methodology for Evaluating Information Security Countermeasures of a System, *IEEE International Conference on Information Security and Assurance*, (24-26 April), pp. 433-438

Sinkovics, R. and Penz, E. (2011), multilingual elite-interviews and software-based analysis, *Business Source Premier International Journal of Market Research*, (Volume 53, Issue 5), pp. 705-724

Siponen M. and Vance A. (2010), NEUTRALIZATION: NEW INSIGHTS INTO THE PROBLEM OF EMPLOYEE INFORMATION SYSTEMS SECURITY POLICY VIOLATIONS, *MIS Quarterly*, (Vol. 34, Issue 3, September), p487-A12

Straub, D., Goodman, S. and Baskerville, R. (2008), Information Security: Policy, Processes, and Practices, M. E. Sharpe, Inc.

Subramanian, R. (2008), Computer Security, Privacy, and Politics: Current Issues, Challenges, and Solutions, New York: IGI Global

Sun, Y., Li, N. and Bertino, E. (2011), Proactive defence of insider threats through authorization management, *ACM Proceedings of 2011 international workshop on Ubiquitous affective awareness and intelligent interaction*, (September), pp. 9-16

The Information Security Policies, [WWW] Available from: http://www.information-security-policies-and-standards.com/ [Accessed 06/03/12]

The National Payment System, the Central Bank of Libya. [WWW] Available from: http://cbl.gov.ly/en/home/index.php?cid=70 [Accessed 01/05/12]

Tipton, H. and Krause, M. (2008), Information Security Management Handbook, Taylor & Francis Group; 6th Edition (2008)

Vacca, J. (2009), Computer and Information Security Handbook, Burlington: Elsevier Inc.

Von Solms, R., Thomson, K. and Maninjwa, M. (2011), Information Security Governance control through comprehensive policy architectures. *IEEE Information Security South Africa (ISSA)*, 15-17 Aug, pp. 1-6

Ward, J. and Peppard, J. (2002), Strategic Planning for Information Systems, John Wiley & Sons; 3rd Edition (Mar 2009)

Waugh B. (2008), Information Security Policy for Small Business, Information Security Writers. [WWW] Available from: http://www.infosecwriters.com/text_resources/pdf/BWaugh_Policy.pdf [Accessed 07/03/12]

Appendix A: Project Schedule

Tasks	Feb-12				Mar-12				Apr-12				May-12			
	W 1	W 2	W 3	W 4	W 1	W 2	W 3	W 4	W 1	W 2	W 3	W 4	W 1	W 2	W 3	W 4
Planning		√														
Staff Interests		√														
Contacting Supervisor			√	√			√	√				√	√			
Meeting the Supervisor					√	√								√		
Proposal Prep.					√	√										
Project Proposal Agreement						√										
Secondary Research					√	√										
Comparative Analysis					√	√										
Interim Report							√									
Planning a research project								√								
Literature Review								√	√							
Primary Research								√	√							
Informal Interviews								√	√	√						
Final Report Write up									√	√	√	√	√	√	√	
Analysis and Evaluation													√	√		
Future Work Suggestions															√	

Appendix B: Interview Questionnaire

The interview questionnaire was adopted from (Klein and Myers 1999).

Background

- Roles and responsibilities.
- What is your background knowledge about information security?
- How do you rate the security at the CBL?
- What is the relation of your work toward information security?

Day2day work

- Could you describe, how do you follow the security plan terms at the CBL?
- How do you describe your information security experience?
- How security instructions may affect your data to day work?

Information security importance

- Do you agree with CBL's information security plan terms? (Why)
- Are you satisfied with CBL's information security plan terms? (Why)
- What do you know about CBL's information asset secure management?
- Do you think your decisions have ever been affected by the CBL's security terms?
- How important do you think to follow security plan?
- How do you follow the security plan terms?
- Do you think your security behaviour may influence your colleague?
- Do you know how your colleagues think about security plan terms?

The new set of security plan terms

- What would you do to improve the current security plan terms?
- How would these new improvements benefit the CBL's services and you work as well?
- Can you give me alternatives to the current security plan terms?
- What type of security plan terms could be beneficial for the information security?

Debriefing

- Ask the interviewee to highlight the interview in number of points and let him/her comment about them.

Appendix C: ISP Interviews Summary

Title	*Interviewee*	*Notes*
Information Security Policy (ISP) Use	*IT Manager*	- ISP is useful in protecting the organisation's Business - It is a part of day to day work within the organisation - It is a clear and understandable plan that contains set of rules
	System Administrator	- ISP should be used, followed, and distributed to all over the organisation - It is used for information systems to ensure that IT administration tasks is secured - It should be practically suitable for day to day tasks
	End-user	- None
	Information Security Officer	- ISP is useful for the organisation's security image - It is an important part of my job as an ISO - It should include security countermeasures concerning the internal threat

Appendix D: MSc Project Proposal Form

AY11/12, Semester 2

Student Number	1032226	
Student Name	Emad Sherif	
Degree Course	MSc	
Supervisor Name	Dr Xiaohua Feng	
Title of Project	Information Security Policy The National Payment System in Libya	
Description of your artefact	• Information Security policies for the National Payment System in Libya. • Educate the Central Bank of Libya's employees about the insider and external threats. • Improve the level of information security and privacy at the Central Bank • Insider and external threat's intellectual phalanges • Executive board awareness	
What methodology (structured process) will you be following to realise your artefact?	Developing the Information Security Policy will follow the Information Security international standards with what the Libyan National Payment System needs by firstly redeveloping the existing policy to meet the information security international standard with considering the insider and external threats.	
How does your project relate to your degree course and build upon the units/knowledge you have studied/acquired	The thesis is related to my degree course as I am doing MSc Information Management and Security. Some units are directly related to the thesis, such as Managing Information systems and Security, Computer Security and Project Management units.	
Resources	I will make use of resources that I have been using during my studies at the University of Bedfordshire, such as Managing Information Systems and Security Risks module resources that I studied during the 2nd semester, such as books, peer-reviewed journals	
Have you completed & submitted your ethics form?	Yes √	

Appendix E: Form for Research Ethics Projects (CATSethicsform)

1. Student Name	Emad Sherif
2. Student Number:	1032226
3. Degree Pathway:	MSc Information Management and Security
4. Supervisor's name	Dr Xiaohua Feng
5. Supervisor Signature	XF
6. Working title of project	Information Security Policy The National Payment System in Libya

SECTION A: Proposal

Please summarise below the ethical issues involved in the research proposal and how they will be addressed. In any proposal involving human participant's clear explanation of how informed consent will be obtained, how confidentiality will be observed, how the nature of the research and the means of dissemination of the outcomes will be communicated to participants must be provided.

I had been working for the CBL (Central Bank of Libya) since 2004 for six years; I had seen the implementation stages of the NPS, the information security policies have not been set properly. The current information security policy at the Central Bank has not been effective. Even more; the expected outcome has not been satisfactory as the insider and external threats have not been addressed in the information security policy. Therefore; the information security police needs to be improved.

SECTION B Check List

Please answer the following questions by circling YES or NO as appropriate.

Does the study involve vulnerable participants or those unable to give informed consent (e.g. children, people with learning disabilities, your own students)?

NO

Will the study require permission of a gatekeeper for access to participants (e.g. schools, self-help groups, residential homes)?

NO

Will it be necessary for participants to be involved without consent (e.g. covert observation in non-public places)?
NO

Will the study involve sensitive topics (e.g. obtaining information about sexual activity, substance abuse)?
NO

Will blood, tissue samples or any other substances be taken from participants?
NO

Will the research involve intrusive interventions (e.g. the administration of drugs, hypnosis, and physical exercise)?
NO

Will financial or other inducements be offered to participants (except reasonable expenses or small tokens of appreciation)?
NO

Will the research investigate any aspect of illegal activity (e.g. drugs, crime, underage alcohol consumption or sexual activity)?
NO

Will participants be stressed beyond what is considered normal for them?
NO

Will the study involve participants from the NHS (patients or staff) or will data be obtained from NHS premises?
NO

If the answer to any of the questions above is "Yes", or if there are any other significant ethical issues, then further ethical consideration is required. Please document carefully how these issues will be addressed.

Signed (student): Emad Sherif Date: 08/03/2012
Countersigned (Supervisor): XF Date: 08/03/2012

Appendix F: Thesis Poster

University of Bedfordshire

Name: **Emad Sherif**
Student ID: 1032226
Supervisor: **Dr Xiaohua Feng**
Course: MSc Information Management & Security

Information Security Policy

The National Payment System in Libya

Introduction

Information security field has been a hot topic recently, where studies and researches have taken a place regarding this field. The field of information security has changed from just technical issues, technology point of view, into a completely different point of view, where information security has become a more widely term concerning an organisation's assets secure. The organisation's assets secure management comprises the organisational procedures, structures, people, and processes. This is known as Information Security policy. Also, organisations dedicate important resources to implement ISP's; these policies are rarely achieving the desired objectives. The obstacles are mainly caused by employees whom rarely follow the ISPs. Therefore, studying the employees' security behaviour in terms of internal threat is important.

Background

My studies at the University of Bedfordshire along with my personal experience at the central bank of Libya working as system administrator for approximately 6 years have given me the background about how information security level should be for this specific organisation.

Aims and Objectives

The main objective of the study is to raise awareness amongst an organisation's employees about the internal threats impact on the organisation towards achieving quality understanding of this impact through considering organisation's employees' perceptions of IS policy when implementing the ISP.

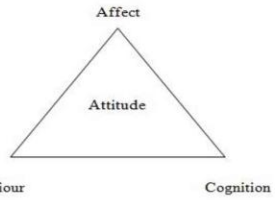
Methodology

Case Study, the case study was chosen based on my own experience as an employee at the selected site, along with, colleagues willing to participate in this study. The organisation; the CBL has an national payment system that was a project around ten years ago and took place as a live system around four years ago, however, there have been security concerns about the security of the organisation's information assets.

Analysis & Evaluation

Klein and Myers (1999) have developed the following seven principles for interpretive case study research analysis: [1] the basis; [2] contextual; [3] academics and subjects interactions; [4] generalisation; [5] dialogue logic; [6] multi translations; and [7] suspiciousness principles. Even more, I think that [8] internal objects principle should be added to these seven principles in this case study specifically as I personally was a former employee at the organisation. Therefore, this point of view should be considered during the evaluation process.

Group	*Interview's Information*
IT Managers	*I think that my security background tells me that everything is alright. I have a lot of work to do and always busy with the paper work and meetings. I believe that we have a good level of information security.*
System Administrator	*As System Administrator pint of view how is looking after the production servers, I can tell you that information security policy is essential to inform and force employees to comply.*
End-users	*Honestly, I do not have a security background; however, I think that doing the daily housekeeping job is just fine.*
Information Security Officers	*Well, I am working in a separate department with few employees looking after the security as whole, so that, we have to spot any incompliance to the information security policy and fix it by educating the employees about this specific security issue.*



ABC framework, adopted from Tipton and Krause (2008)

Conclusions

Therefore, in this thesis, the final conclusion is, employees' perception of information security policy should be sought and included when implementing information security policy within organisations, as well as, information security training should be scheduled in a regular basis.

Future Work

Since, the selected case study for this thesis was the CBL, and the CBL itself has not implemented online banking system so far, therefore, in terms of this study's topic, there is a need to further studies and future work about the external threat risk.