THE ROLE OF 'PERCEPTIONS OF INFORMATION VALUE' IN INFORMATION SECURITY COMPLIANCE BEHAVIOUR:

A STUDY IN BRUNEI DARUSSALAM'S PUBLIC ORGANISATIONS

by

Sharul Tajuddin

A Doctoral Thesis

Submitted in Partial Fulfilment of the Requirements for the Award of

Doctor of Philosophy of Loughborough University

Abstract

It has been widely accepted that information is an asset and it needs to be protected. Many types of countermeasures were developed and implemented to ensure continuous protection of information where it is deemed necessary. Unfortunately, in many cases, breaches of security are the result of non-compliance behaviours of users or stakeholders of the system. These non-compliance behaviours increase the vulnerability of such system. Organisations are trying to improve their stakeholders' compliance behaviour through different ways for example by providing necessary awareness, education and training and to the extent of providing rewards for healthy behaviours and reprimanding and penalising stakeholders for breaches of security. Despite all these efforts, information security breaches are still on the rise and many types of research have been done to understand this issue. It is postulated that an object is protected if it is appreciated. Appreciation of an object might relate to a value perceived by the owner in association with the object.

For the similar reason, this thesis investigates the role of 'perceptions of information value' in the context of its security. It is postulated that 'perceptions of information value' could become an alternative way to understand information security compliance behaviour. Utilising a conceptual framework deduced from current literature to structurally analyse a list of research objectives, empirical evidence of the potential role of information 'perceived value' in promoting better compliance behaviour have indeed been discovered. There is evidence that a perception of information value is developed through a systematic process of value assignment or 'information value assignment' process. These processes are significant to the development of stakeholders' intention to behave. The finding of this process has provided a platform for the organisation to understand the casual behind the information security behaviours displayed by stakeholders in the organisation. Further evidence has also suggested that the 'information value assignment' is fuelled or influenced by several factors. These factors have provided a unique opportunity for the organisation to manipulate and nurture to have maximum impact on their information value assignment process, resulting in a possible improved intention to behave, thus, subsequently might affect the actual information security compliance behaviour.

Publications

Relationship between stakeholder's information value perception and information security behaviour - **Tajuddin**, Sharul and **Olphert**, Wendy and **Doherty**, Neil, AIP Conference Proceedings, 1644, 69-77 (2015), DOI:http://dx.doi.org/10.1063/1.4907819

Acknowledgement

In the Name of Allāh, the Most Gracious, the Most Merciful

Alhamdullilah, all praises to Allah for all the trials and tribulation that resulted in strength and knowledge in completing this thesis.

My first and sincere thanks and gratitude's go to my beloved wife Dr Hjh Nor Zainah Haji Siau, without whom I would not have reached this stage and my three beautiful daughters; Nurul Sa'Nazirah, Nurul Farzana and Nurul Imanina that have become my backbone throughout this study. Through high and lows (mainly lows) your presence and supports have become the motivations to finish this work.

This work is especially dedicated to my father, Haji Tajuddin Parang, my mother Hjh Nur Rahimah Hussin and my parent's in-law Haji Siau Miramit and Hjh Kolam Asmat. Thank you for all your prayers and support throughout.

I am blessed to have been placed under the supervision of these great mentors; Professor Neil Doherty, Dr Wendy Olphert and Dr Jenny Fry. My thanks go to them for all the guides, continuous supports and guidance, encouragement and their trust in me for doing this research.

My appreciation also goes to all my friends, who were with me during this journey, for the friendships and all the support. The Department of information science, Loughborough University for all the excellent and efficient services and last but not the least, the government of Brunei Darussalam for sponsoring this study.

Table of Contents

List of figures

List of tables

Abbreviations

AET	Awareness, education and training
APIV	Antecedent Perception of information value
CIA	confidentiality, integrity, availability
IP	Individual Priorities
OP	Organisational priorities
EGNC	E-government National Centre (Brunei Darussalam)
ISACA	Information systems audit and control associations
PKI	Public/private key infrastructure
PSM	Protective security manual
PIV	Perception of information value
ISB	Information Security Behavior
IS	Information Security
IT	Information Technology
IA	Information Assurance
WPIV	Workgroup Perception of information value

1. Introduction

This chapter outlines the contextual background of the research. The chapter begins with a presentation of the driving factors and the initial interest for the research. This will include a detailed rationale underlying the research and its position in the real world. The broad objectives of the research are also presented. This chapter concludes with a conceptual map, which demonstrates how this whole thesis is structured.

1.1 Information security in organisations

Organisations view information as one of their most valuable assets (Orna, 2005). Davenport and Prusak (2000) emphasised the importance of information for organisations by realising that there is a market for information. In a similar way to markets for goods and services, information is exchanged, bought, bartered, found, generated and applied to work. Organization creates information products either to support the products and/ or services, which they are in business to offer, or as their primary market offering (Orna, 2005). Information products are knowledge made visible, communicated and exchanged in the form of outputs such as print on paper or electronic formats. According to Itami and Roehl (1991), how organisations create and use information can be indicative of the actual value of that organisation, and without access to information, organisations may lose their competitive edge, which can have a detrimental effect on their business processes (Van Niekerk and Von Solms, 2010).

Increasingly, organisations see information security as an integral part of the design and operation of their business processes, rather than a separate issue. Due to the importance of information for the growth of their businesses, organisations see protecting their information as the main priority (Bunker, 2012). With the growing importance of information, the threats to it, and the systems supporting it, from criminals and terrorists are also increasing. One way to protect information is by setting up an appropriate security strategy (Castano et al., 1994). Furthermore, changes in the information communication technology and risk landscape have forced organisations to consider the issue of information security more seriously. For example, the advances in information

communication technology such as Cloud Computing have brought changes to the way in which information is created, stored and communicated (Mell and Grance, 2011). The characteristics provided by Cloud Computing such as resource pooling, broad network access and on-demand self-services have not only provided advantages for its users but at the same time have exposed the host organisation to new vulnerabilities.

Incidents and attacks are reported to be on the rise (CSI, 2011) but not all incidents and breaches of information security are caused by technological vulnerability and failures alone. Widman (2011) reported that among the ten biggest security breaches reported by organisations worldwide between the years 2005 to 2009 are errors and negligence on the part of humans. Specific examples of breaches initiated by employees include: stealing customer records and selling them to a data broker; misplaced and stolen unencrypted portable storage devices; and employees not following proper security procedures. According to Widman (2011), these breaches lead to loss of information, personal records, or other data. Some resulted in the loss of millions of data records, some affect millions of people, and some cost the affected businesses financially. Similarly, survey reports from organisations such as PriceWaterhouseCoopers (2012) indicate concern regarding the rising number of incidents and breaches related to human vulnerabilities. Among the human related incidents and breaches reported were: confidentiality breaches; computer fraud; staff misuse of information systems; and virus infections or disruptive software, rather than technical problems.

1.2 Locating the problem conceptually

The reliance of organisations on information and information technology (IT) to support their business processes is very important; it is said that only one in six small companies could continue their business without access to their information and IT (DTI, 2006). As a result of this reliance on IT, the need for better controls to protect both information systems and the information that they hold has emerged as a primary consideration. This is partly due to the vulnerabilities brought by the adopted technology; for example, the provision of access to information from remote systems. The need to protect information, held

electronically, from the threat of attack (for example, from hacking) is now a major organisational priority. Coupled with the reliance on IT and an understanding of its weaknesses is the recognition of the value of information held within an organisation (from customer details to business strategies, for example).

Information security has also become a key focus of businesses and governments., This is in part due to the importance of establishing and maintaining customer trust, through the provision of appropriate information protection thus upholding the reputation of their organisation, but also because of the need to adhere to regulations and legislation. For example the following key pieces of legislation have all been introduced in recent years:

- the Data Protection Act was introduced in the United Kingdom to govern the protection of personal data;
- the Financial Services Authority regulations (replaced by Prudential Regulation Authority regulations from April 2013) introduced in the United Kingdom to regulate financial services that include the handling procedures for financial information;
- the European Commission (EC) Data Protection Directive which is also implemented as the Organisation for Economic Co-operation and Development (OECD); Privacy Principles;
- the Sarbanes-Oxley Act (a United States federal law which aims to protect investors by improving the accuracy and reliability of corporate disclosures according to the securities law); and
- the Computer Misuse Act (1990) introduced in the UK and which has been adopted by other countries including Brunei Darussalam.

It is also a de facto standard for an organisation's business processes and corporate governances to conform to the International Organisation for Standardisation (ISO) to be recognised internationally. Having achieved a certain standard, in this context the information security Management standard (ISO 27001, ISO 27002) the organisation may be seen to have enhanced their reputation, through their commitment to upholding information security and providing appropriate protection for their information. Doherty & Fulford (2006), and Von Solms (1998) postulate that working towards international

standards such as ISO 27001 will help improve the organisation's information security. One important outcome of this initiative has been that the once specialised field of information security is now the responsibility of the organisation, as a whole, rather than being confined to the IT Department. Due to legal, regulatory and policy requirements it is also now mandatory in many industries and across Government departments that employees receive on-going information regarding security awareness, education and training (AET). For example, Santander UK enforces mandatory training for their new starters and contractors on data protection and information security, and the same precautionary measures are also observed in many universities across the UK (Santander, 2016). While in the United States, the US General Service Administration introduced compulsory IT security training for all their agency and contractor employees (GSA, 2010).

A number of information security leaders which include the Director of Security and Privacy at Deloitte and the Security Architecture and Engineering advisor of the U.S. Department of Treasury, sharing their insights and experience on brightalk.com, appreciate that the landscape of current information security has evolved from a technology focus to a process focus, i.e. a shift from what do we need to deploy and implement to what do we focus on and why? (Pfost et al., 2012). Information flow is no longer restricted within the boundaries of the organisation; rather information is shared with other people and establishments linked to the organisation, which may be located in other countries. The evolution of information security may increase the possibility of vulnerabilities in business processes and information security approaches. Despite the growing appreciation of the need for effective information security and the more proactive approaches by organisations towards achieving appropriate information security, information security breaches and incidents are still on the rise (Garrison and Ncube, 2011).This may in part be because many organisations have taken steps to upgrade their technical approach towards information security, without realising that employees' inappropriate information security behaviours are also a source of vulnerability. With the upgraded technical developments against threats and vulnerability to information security, a false sense of security and complacency may arise (Parsons et al., 2010).

Turning now to Brunei Darussalam, the context for this study, the practice of 'acceptable' information security behaviour is seen as a major issue (Juned, 2013; Seyal and Rahim, 2011). This practice denotes that any level of security is acceptable as long as there is security in placed. Poor information security (staff do not employ appropriate security to information) and information leaks (i.e. accessibility of sensitive data to non-authorised personnel) were the two primary reasons that deterred Bruneians from making use of e-government services in the Sultanate (AITI, 2010). Furthermore, the e-Business Interim Committee of Brunei Darussalam in 2009 reports that the main problem in the development of e-business in Brunei Darussalam is the lack of security awareness among employees. Two examples are the uncontrolled use of USB storage (such as flash or USB drives) and the uncontrolled installation of unverified/trusted software or applications (EBLF, 2009). Despite these issues many organisations do not see the provision of information security training as a top priority. Indeed, some organisations only provide training for employees whose tasks directly involve information technology and information systems (EBLF, 2009).

1.3 Research problem statement

Information Security is a concept that formed from the recognition that information is valuable and that there is a need for it to be protected. The ISO 27002 defines information as an asset, which, like other important business assets, is essential to an organisation's business and consequently needs to be appropriately protected. By definition, an asset has a value to the organisation, hence it requires protection (Gerber & Von Solms, 2005). For individuals, protecting information is vital to avoid harm and distress caused by personal information security breaches (ICO, 2010). Personal information security breaches are mainly caused by the loss or abuse of personal data that leads to identity fraud. For example, fake credit card transactions and mortgage fraud. Because of this, it has become increasingly important for consumers, organisations and information technology and information security specialists to share responsibility for protecting information as well as the resources that facilitate the information exchange.

Information protection is typically accomplished through the implementation of countermeasures[1] against the threats and vulnerabilities to information security, for example, implementation of technological processes and mechanisms such as: firewalls and authentication systems; deterrence procedures; and the enforcement of organisational policies on information handling procedures. The efficiency of the implemented processes and mechanism depends on a lot on the user's decision as to whether they use the processes and mechanisms or not. To help ensure that users are willing to use the countermeasures in place, organisations are spending large sums of money to train and educate their users and to set up an information security awareness environment in the organisation.

Information security revolves around the notion of providing protection to information held within an organisation or information owned individually. In an organisation, information is protected from either external threats or internal threats or both (Dewa and Maglaras, 2013). External threats include threats from outsiders; for example, threats from hackers and vulnerability caused by external users from other establishments linked to the organisation. Internally, organisations' information security is prone to threats from vulnerability caused by users as well as ineffective countermeasures (Wang, 2015). Figure 1.0 further illustrates how information security is defined from the view of different stakeholders of the information security assets. There are two main stakeholders in an information security setting: the owner[2] of the information asset who may also well be a user; and the user[3] who does not own the information asset. Between these two main

[1] Countermeasures means the mix of procedural and technical controls such as security policies, AET programs and monitoring software used to deter misuse of information and information system implemented or exercised against threats, risks and vulnerabilities posed to information security. The definition of countermeasure is adopted from D'Arcy et al. (2009) and Straub (1990).

[2] Owner/owners here, and throughout the thesis, denote the owner of information asset(s) and they can also become the user/users of their information asset(s).

[3] User/users here, and throughout the thesis, denote employees or staff that have access to the information asset(s).

stakeholders, different views may arise as to the underlying value of the information asset. According to Beautement et al. (2008) individual users and owners place different values on the cost and benefits of behaviour associated with information security countermeasures.

The owner of the information asset typically has specific views about it. for example, the owner may view the information asset as providing a potential competitive edge, whereby appropriate and strategic use of information could earn the organisation profits. For this matter, to the owner it is essential to protect the information assets from threats. According to Rainer et al. (2007) organisations are looking for appropriate information security to protect their organisation from litigation, financial losses, damage to brands, loss of customer confidence, loss of business partner confidence, and even going out of business. For these reasons, the main priorities, for most information owners, are to set up appropriate protection for their information asset and to ensure that other users comply with the protection measures that are established. A key element of these countermeasures, seen as valuable to the owner, is the AET initiative (Soomro et al., 2016). Users sometimes see countermeasures as obstacles, but to the owner of the information asset these are necessary barriers to ensure the security of their information assets. The need for information protection is not only seen as necessary for avoiding loss in cases of breaches and incidents but the owner of information assets are obliged to adhere to specific rules and regulations governed nationally and internationally. Failure to setup necessary preventative measures might cause owners of information assets to incur hefty fines by authorised bodies.

The users of the information assets, on the other hand, may have a different view of the issues surrounding the security of information. It is important for security designers and managers to realise that individual users can make a choice as to whether to comply with information security countermeasures, or not. The privilege to choose is always influenced by several factors such as the individual's own goals, perceptions and attitudes and the norms that govern the individual's behaviour (Adams and Sasse, 1999; Weirich and Sasse, 2001; Weirich, 2005). Other issues that need to be considered are that users can be placed into different categories - a user can be an individual user or a group of users (Bélanger & Crossler 2011). Users have a different level of responsibility and thus have different needs

relating to various forms of information. For example, users working in the Human Resources department will need to have access to the personal information of the organisation's employees, and the users in the R&D department will need access to the different genres of information such as the organisation's trade secrets and propriety information.

The categories of user and their different needs of access to different types of information might impact on the perception of users regarding the issues surrounding information security. To users, the most important thing is to accomplish their tasks in the most efficient and effective ways possible. At times countermeasures are seen as huge obstacles to accomplishing their duties (Furnell et al., 2008); this perception might encourage users to find ways to circumvent the countermeasures. It is expected that users who received any form of AET initiatives should demonstrate higher security behaviour than users who did not receive any (Puhakainen and Siponen 2010; Jenkins et al. 2012)(Puhakainen and Siponen, 2010)(Puhakainen and Siponen, 2010). Unfortunately, to many others practising what they learned from AET initiatives is considered as obstacles and becomes a hindrance to their daily routine (Post and Kagan, 2007).

For some users some sort of motivational antecedents such as (organisation type, job role, job satisfaction, and organisational commitment) are needed for them in order to comply with appropriate practices of information security (Stanton et al., 2004). Other research such as (Beautement et al., 2008; Chan et al., 2005; Mohamed and Ahmad, 2012) suggests that users will perform expected information security behaviour better if they expect to receive some form of rewards. On the other hand studies by (Siponen et al., 2010; Vance et al., 2012) indicated otherwise. The negative impact of rewards on information security behaviour may be the result of the failure of the users to perceived the benefits of the rewards when weighed against the effort required for them to learn and carry out the countermeasures (Beautement et al., 2008).

Although there are a significant number of studies and efforts to make sure that users comply with their information security commitments, many organisations still find it a major challenge. For this reason, further understanding of the factors that help in forming the belief and behaviour towards information security is essential in order to identify which

factors can be used to influence changes to improve information security intentions of stakeholders and subsequently will improve their compliant behaviours.

1.4 Broad research objectives

The literature review suggests that human aspects are more important causes of failure in information security, both active: intention to break information security, and passive: failure to comply with the countermeasures that are available. This PhD study is focusing primarily on the users' failure to comply because many prior studies (Guo, 2013; Rhee et al., 2009) have claimed that users' failures to comply are the most common reason for information security breaches.

Following are broad objectives of the research that will act as stepping stones to help pave the way to achieving a richer understanding of the phenomena of interest. Generally, the *first broad objective* of this research is to make sense of users' (stakeholders) intentions and behaviours, with regard to information security countermeasures, through their 'perceptions of information value'. The big questions are whether stakeholders value the information they are handling; how are these perceptions created; and what unit of measure is used to value the information.

The *second broad objective* of the research is to explore whether there is any relationship between the information value, as perceived by the stakeholders, and their resultant behaviours towards the protection of the information. Are there any changes to how they would protect the information in terms of their attitude and behaviour towards the information security countermeasures? This will include the study of stakeholders' compliance behaviours and their underlying assumptions. In so doing, this objective will seek to highlight any key differences and commonalities in stakeholders' information security compliance behaviours.

The *third broad objective* is to explore and understand how attitudes towards the 'utility' of the information are being derived. The utilities might be based on several factors that may be categorised and their influence on how the stakeholders intend to behave towards the protection of the information could be understood. Therefore it is an interest of this

research to explore, identify and understand the factors that the stakeholders use to base their valuation of information on.

It is also an interest to investigate whether different users or stakeholders have different views on the issues of information value and the issues of information security. It is expected that there are gaps between these two views and are having some impact of the effectiveness of information security.

A detailed discussion of the specific research objectives arising from the broad objectives above, and based on a review of existing literature, will be presented in Chapter 3.

1.5. Overall Research Approach

The following key stages represent the overall approach adopted within this research study:

- A review of the extensive literature pertaining to creation of perceptions of information value. In addition, reviewing the existing body of knowledge associated with organisations' efforts to meet regulatory requirements, with further concentration on the utility expected on information to ensure efficiency and effectiveness of compliance;
- The identification of key gaps arising from the review of the literature from which the research objectives have been derived, and the conceptual framework has been formulated;
- The establishment and justification of the overarching research strategy, from which the specific research and data collection strategies have been derived;
- The conduct of the data collection exercise, which entailed pilot interviews, followed by face to face interview sessions, focus groups sessions as well as workshops conducted in several phases with a wide variety of public sector informants.
- The detailed analysis of the interview, focus group, and workshop data, as well as a review of all the relevant documentation on information security, collected during the interviews.
- The Presentation of the outcomes of the analysis and the contributions to the existing body of knowledge, as well as the introduction of an alternative approach to view the research perspectives through a revised framework.

1.6 Thesis Structure

This section will present the structure of the thesis. Figure 1.0 below depicts the thesis structure and the brief explanation on what each chapter presents follows.

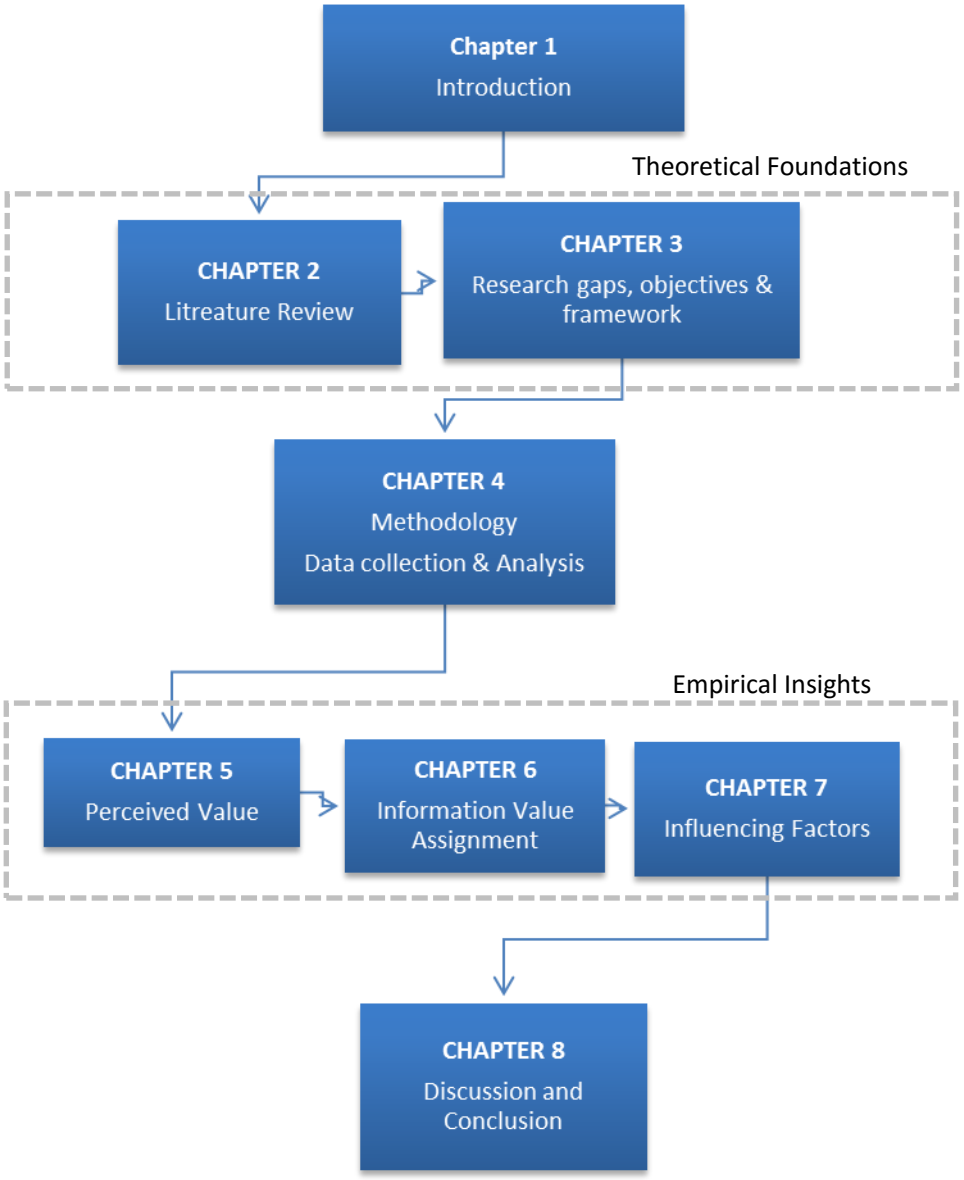


Figure 1.0 The thesis structure

Chapter 1 - *outlines the contextual background of the research*. The chapter begins by presenting the driving factors and the initial interest of the research. This includes a detailed rationale underlying the research and its position in the real world. This chapter will also provide a conceptual map on how this thesis is structured.

Chapter 2 - *discusses the findings of the review of the literature* on subjects that are significant to information security, information security behaviours and perception of value on objects and services. This chapter will also present the formulation of a conceptual model that ultimately guided the conduct of the research.

Chapter 3 - *outline and discusses the gaps* found from the literature review and highlights the objectives of the researchers. This chapter will also discuss in detail the interpretive framework that will guide the studies planned for this research.

Chapter 4 - *discusses the general methods and approaches* taken by the researcher on the methodological aspects of this research. Pros and cons of various techniques, methods and approaches are also presented. This chapter will proceed to present the data collecting activities.

Chapter 5 – *presents first research objectives key findings* as well as present the findings in relation to each of the sub-objectives developed under research objective one. Based upon this analysis, a revised version of the interpretive model is introduced, at the end of this chapter, and its significance to the research is explained and justified.

Chapter 6 - This chapter starts by revisiting and validating the revised view of the information value assignment processes as portrayed in the conceptual model [presented in chapter 5]. Having revisited the information value assignment process, the bulk of this chapter will then focus on addressing Research Objective 2.

Chapter 7 – *presents the key findings relating to the third research objectives***.** The focus will be on the various factors that were found to have a significant influence on stakeholders' intentions and behaviours.

Chapter 8 – *final discussion and concluding chapter* which presents the discussions on the general findings of the research but more importantly it will discuss the key findings of the research according to the objectives of the research. This chapter will also outline the theoretical contributions that this research makes as well as outlining some recommendations. Possible further works will also be discussed.

2. Literature Review

2.1 Introduction

This chapter presents a detailed review of the existing body of literature that will form the theoretical foundation for this study. A review of the literature relevant to the study will ensure that the research is firmly rooted in the knowledge and insights already made available by other researchers. The knowledge on various issues of information, information security and the behaviour of the stakeholders of Information is important to frame and locate the focus of the research. Therefore, the following sections will present all the relevant literature that builds the fundamental understanding of the issues of the research.

2.2 The concept of information and information security

There seems to be no consensus on what 'information' is, or even what its essential features are. Indeed, it has been suggested that no single thing is meant by 'information' in the sense that it is used differently by people in different contexts (Mathiesen, 2004). Orna (2004) describes information as what human beings transform their knowledge into when they want to communicate it to other people. Smith (2001) suggest that information is documented “know-what” or explicit knowledge that is described in formal language, print or electronic media, often based on established work processes. On the contrary, Davenport and Prusak (2000) state that information is merely a message that is meant to change the way the receiver perceives something, to have an impact on his judgement and behaviour. What is delivered through structured media such as books and documents and person-to-person contacts ranging from conversations to apprenticeships is knowledge. Knowledge is sensed to be broader, deeper, and richer than information (Davenport and Prusak, 2000). Due to the subjective nature of the process of defining information, and the broad context in which information can be assigned value, it is hypothesised that the assignment of protection levels and the need for security also varies. Therefore, in the context of this research it

seems to be sensible to adopt the definition of information as the one described by Orna (2004).

Information has little value until it is given meaning or used on the job, such as raising levels of competence (Pascarella, 1997). McCain (2004) states that the meaning of information depends on how it is interpreted, understood and used. It all depends on the utility the information provided. Ackoff (1989) describes information as the collection of raw data that is only useful when given meaning by the user in a way of relational connection. Similar to Smith's (2001) suggestion that information is data that has relevance, purpose and context but for information to be useful or to possess any real value or utility, it has to be assigned some meaning. Since the value of information depends on the context of its usage and the benefits it brings to the use, this resulted in several perspectives towards the importance of information.

2.3 The importance of information.

Information is seen as critical as it can support decision-making and control processes (Mowshowitz, 1992). Having the right information will help in clarifying a (Shannon, 1949). Information is a key asset to Government and its correct handling is vital to the safe and effective delivery of public services. Departments and Agencies need to be confident that their information assets are safely and securely stored, processed, transmitted and destroyed, whether managed within the organisation or by delivery partners and suppliers. Equally, Government has a legal obligation and duty to safeguard personal data entrusted to it by citizens and businesses. In striking the right balance between enabling public services and sharing and protecting data, organisations must assess and manage the risks to the services they provide and to the Confidentiality, Integrity and Availability (C, I & A) of the information assets they are formally responsible for (Home Civil Service, 2012). The importance of information may be seen from two different perspectives i.e. the value of the information and how the information is being protected and secured. The following section will discuss information from these two perspectives.

2.3.1 Information Value

Orna (2004) highlights that information in the form of the 'information product' could represent the organisation's values and knowledge, which can act as the agent of transformation, diffusion and organisational learning, and can be a valuable repository for organisational knowledge.

This signifies that the more the information can contribute a positive outcome to the organisation the higher the value is placed on the information and, therefore, might place a tighter protection on it. The importance of information to the life of an organisation has brought about its commodification. According to Mowshowitz (1992) commodification of information is the process of turning information into a commodity, in the sense that it has a market value and it is appropriable. Since information is much needed (appropriable) and people or organisations are willing to pay for information (market value), information is considered as a commodity. This value according to Mowshowitz (1992) is derived from its capacity to support decisions or control processes by the furnishing information. However, this capacity is only partly dependent on the specific information (ability to decide or control) furnished by the commodity. The concept of commodity includes the notion of selling and buying and the concept of possession. Once information is bought, it becomes one's personal information or part of the organisation's assets. Similarly to other commodities, information as a commodity will need to be protected from theft and unauthorised access and use by other people who are not the intended users. The appropriate level of protection in this context is subjective to the value assigned to the information based on the capability of the information to contribute fully and productively to achieving the organisation's goals. As a result, this may yield a different perceived level of security deemed necessary to protect the same piece of information.

Globalisation forces businesses and individuals to reach beyond their local domains for richer information to assist in their decision-making and processes. According to (Leidner, 2010) the increase of globalisation has brought changes to information requirements. The need for information such as information about suppliers, markets,

and consumers as well as information about distribution, logistics, and operations has grown support growing business needs.

This need for organisations to acquire more and better information has been fuelled by the Internet; diminishing physical boundaries, heightening information sharing and, simplifies accessing to information. At the same time, the drive to acquire and utilise more information has brought new risks, particularly in terms of information security and privacy. Globalisation has also introduced new government regulations, requiring the organisation to protect data. This has increased awareness of the need for effective corporate governance of information security (Kayworth and Whitten, 2010). The competition in the global information economy is also contributing to the rising value of organisations' proprietary information (Wiant, 2005) and it is important that this proprietary information not is available to the general public and is protected.

There are three different perspectives towards the importance of information: the individual perspective, the organisational perspective and the global perspective. These three perspectives differ regarding the use, benefit and significance of information, the type of information used and how much security are deemed necessary to protect the information. Bélanger & Crossler (2011) introduced the multilevel concept of information privacy and security forming several levels of perspective. These levels are outlined as individual, group, organisations, businesses or societies. However, due to the similarity of the information handled by groups, organisations, business or societies these perspectives can be simplified into two main perspectives: individual perspective and organisational perspective. Furthermore, Milberg et al. (1995) suggest another level of perspective, which is the global perspective. This perspective arises from the globalisation of information systems (IS) and organisations entering into increasingly competitive international markets.

From the individual perspective, information is valued due to its ability to support daily decision-making and control processes, such as the management of personal finance and health. Information has become very significant in peoples' professional and personal lives to be able to thrive and progress in society and to fulfil the requirements

of studies or work (Tahir et al., 2008). The dependency on information has changed the way people live their life; many people depend on the Internet as the provider of their much-needed information (Robinson, 2013). Activities such as banking, shopping and even communication between friends are increasingly done online rather than through traditional means. These activities provide opportunities for cyber criminals to attack and compromise information. Cybercriminals operate globally taking advantage of the non-standard regulation of information security laws by different countries.

Apart from acquired information (Information that comes into their possession) individuals also generate other information, which could be used to identify them. This information is defined as individual personal or private information in the Data Information Act (1998). The Data information Act of 1998 is a United Kingdom Act of Parliament, which defines UK law on the processing of data on identifiable living people. It is the main piece of legislation that governs the protection of personal data in the UK. The existence of such law and regulation signifies that the need to protect and secure information is paramount.

2.3.2 Protecting and Securing Information

According to Milberg et al. (1995) it is of great interest to the majority of individuals to have the ability to have control over their personal information thus maintaining their personal information privacy. Personal information privacy, is defined as "the ability of the individual to personally control information about oneself" (Stone et al., 1983) particularly, the ability to determine for themselves when, how, and to what extent information about them is communicated to others (Westin, 1967). Additionally, Schwartz (2004) extends the definition of personal information privacy to include the concern for how one's personal information is being used, transferred and generated.

Technological developments such as the use of cookies to identify visitors and document their usage on the Internet and the introduction of wireless communication devices that provide organisations with the ability to locate individual users by time and place through mobile technology, brings many positive features to users but at the same time raises the privacy alarm (Westin, 2003). Changes in the ways information is

generated, accessed and processed, for example, the ability to perform government processes online through the provision of e-government services, the use of cloud storage offered by numerous organisations and effectiveness platforms for communication provided by various social networks have changed the way people view and treat information security. Westin (2003) believes that these changes lead to fears about privacy invasions in the social and political world and also a potential threat to privacy by the government and businesses. Due to this consumers began to exercise individual privacy assertiveness by refusing to give information if they think it was too personal or not needed. Incidents such as of the September 2001 terrorist attack on the US has increased the focus on security as a whole, but there is a general sense that privacy has become a less important issue (Swire and Steinfeld, 2002). People's expectations of the privacy rights of foreign nationals and U.S. citizens in the United States post-September 2001 have been reduced (Council National Research, 2007) this is due to the passing of the "USA PATRIOT Act 2001" giving law enforcement agencies sweeping search and surveillance powers over foreign nationals and US citizens. In 2003 the Information Awareness Office (IAO) set up under the 'USA PATRIOT Act 2001' initiated the Terrorist Information Awareness program with the aim of developing a technology that would enable it to collect and process massive amounts of information about every individual in the United States, and trace patterns of behaviour that could help predict terrorist activities. The information the IAO would gather includes Internet activity, credit card purchase histories, airline ticket purchases, car rentals, medical records, educational transcripts, driver's licences, utility bills, tax returns, and other available data. Critics of the IAO believe it goes too far in the sacrifice of civil liberties and privacy, putting in place an infrastructure prone to abuse. Sometimes security and privacy are seen as opposing each other. That is, to achieve greater security means increases in surveillance, information gathering, and forced information sharing thus raising privacy risks. Individuals are becoming more concerned about the amount of control they have over access to their personal information privacy due to this advancement in technology and process Nehf (2012) and the lack of regulation and enforcement of law and legislation add up to the concerns (Prins, 2006).

Harris and Westin (1995) categorised how people (consumer) deal with privacy into three perspectives: the '*fundamentalists*', the '*unconcerned*' and the '*pragmatists*'. The fundamentalists rejected consumer benefit or societal-protection claims for data uses and sought legal-regulatory privacy measures while the privacy unconcerned were generally ready to supply their personal information to business and government and rejected what was seen as too much privacy fuss; and between the two positions, the privacy pragmatists examined the benefits to them or society of the data collection and use, wanted to know the privacy risks and how organisations proposed to control those, and then decided whether to trust the organization or seek legal oversight. Ackerman et. Al (1999) in their study of users concerns and attitude towards e-commerce privacy found out similar clustering of respondents. They classified three main clusters; respondents as privacy fundamentalists, the respondent as a member of the pragmatic majority and marginally concern respondents. According to Harris and Westin (1995), the consumer policy struggle of the 1990s was (and remains today) a battle for the mind and hearts of the privacy pragmatists. This statement and the three categories of privacy view strengthened by recent studies such as those by Malheiros et al (2011), Grossklags et al., (2007); and Prins (2006) suggesting that people are willing to disclose some information in return for rewards and benefits, while the study by Christofides et al. (2009) states that people have little concern regarding their information security and personal privacy. Despite these findings, studies by Swire & Steinfeld (2002); Christofides et al.,(2009); Tsai et al. (2010) suggest that people are also taking a cautious approach to information disclosure. These studies indicate that there exist multiple perceptions of the value of information and are subjective to the benefits and the risks relating to the information deemed by the owner of the information. It is realised that a proper standard to evaluate information and value associated with it is non-existent.

The other perspective of information security is from the organisational perspective. Oppenheim et al. (2002) argue that from the organisational perspective, information should be viewed and managed as an asset that can help to enhance the effectiveness of the organisations' communication and decision-making. Organisations can either be

in the private sector or the public sector. The information allows organisations in the private sector to thrive and provide them with distinct advantages in the ever competing economic environments. For example, having access to information such as customers' buying patterns and preferences will provide them with a leading edge over their competitors. Easley & O'hara (2004) suggest that a well-informed investor would have a better prediction of the cost of capital than an ill-informed investor. While for the government's organisations. For organisations in the public sector better use of information can improve public services such as the provision of better infrastructure and services for citizens (Woodhouse, 2007). Better use of information ensures that people get all the services to which they are entitled, or allow services to be personalised (Cabinet Office, 2008) which, helps to protect the public and to fight crime including fraud. Furthermore, having access to information such as citizens' employment information, personal information, medical history, criminal records, education and immigration information can help in providing more efficient and improved processes, services and treatments. As more and more organisations see information security as an integral part of their business processes and the dependency on information increases, the more they value information as an important asset (Davenport and Prusak, 2000; Orna, 2004).

The different information perspectives have meant differences in perceived levels of protection needed. For individuals, they desire that their information is used only for what is necessary to complete a process and expect to be able to have control over their information. Clearly, there is a mixed view of how much each values their personal information, and in return this might suggest how much security is enough to protect their information or is worth protecting at all. On the contrary, organisations see the opportunity to use information as an advantage over their competitors. The value of information as a commodity provides an estimation of profit opportunities and the ability of organisations to stay ahead of their competitors. Therefore, it is important for businesses to protect such information to prevent it from being widely known which would decrease its value. Again the varying values assigned to a piece of information

might signify or translate to how much protection is deemed sufficient to secure the organisations' information assets.

2.4 The Evolution of Information Security

The main aims of data securing activity are to achieve and maintain various security goals by eliminating, avoiding or minimising threats (McIlwraith, 2006). Table 2.1 ((Complied from (Alnatheer and Nelson, 2009; Cherdantseva and Hilton, 2012; isaca, 2009; Nehf, 2012; Raiu, 2012)) lists several common security goals, which should be a key feature of current information security protocols, the threats faced by each security goal, the aims to be achieved for each security goal and common measures or tools that are used to achieved and maintain them.

Table 2.1 *Security goals, threats, aims and measures*

Security Goals	Threats	Aims	Techniques/ measures
Confidentiality	Unauthorised access to data Interruption, malicious activities Data/information stealing	Only authorised parties can view information and execute processes Limiting entry to authorised users	Encryption Cryptography Firewalls Passwords Biometric Devices
Integrity	Unauthorised modification	Only authorised parties can modify data, information and code in an authorised way	Hashing Digital Signature Encryption Message authentication codes Message digest
Availability	Denial of Service (DoS) Distributed Denial of Service (DDoS)	Information is accessible when required	Disaster recovery Business continuity Redundancy, failovers, and Clustering of information
Authenticity	Fake or fabricated information Interception of information and modification	Origin verification to establish authority for truth and correctness (Genuine)	Digital signatures Challenge response Passwords Biometric devices
Non-repudiation	Interception of information and modification Denial of action	Proof of origin, receipt and contents (sender cannot falsely deny sending or receiving the message)	Bidirectional hashing Public key encryption Digital signatures Transaction certificates Timestamp Confirmation services
Utility	If data is not in a useful state or form, it is basically useless	Usefulness of data / information	
Possession/ Control	Access to information when device or storage is stolen	Access to data and information on device is strictly for the possessor of the data or information only	Public Key Encryption Violation control Limitation on information transferred or acquired

The concern for information security began in the military and the government environment in the 1970s with the aim of protecting classified information. The major approach towards information security was very much defence-focused with the emphasis on the confidentiality of data and information. This defence-focused approach is done by restricting access to information technology devices. Back then when computers were standalone and software was unique to each computer, security was mainly focused towards the protection of the computers rather than the information. The early years also saw the beginning of the recognition of information as a key asset by many organisations.

The 1980s brought changes to the way computers were used; computers were joined to form networks. Networked computers introduced the concept of a centralised database providing remote access to stored information. This function introduced a new vulnerability to information security; unauthorised modification became the new threat and a new goal of information security included ensuring the integrity of the information communicated (Clark and Wilson, 1987).

By the 1990s a commercialised international network emerges as a result of the merger of many previously independent and isolated networks; this resulted in its popularisation and incorporation into virtually every aspect of modern human life (Groups Miniwatts Marketing, 2012). The growing size of the network provided simplification of access to information through remote access; information could be easily shared among connected computers from different networks, and more and more services relied on the availability of the networked connections. These advantages also paved the way for a new threat to the security of information. The 1990s saw the first worm virus attack that aimed to disable the networking by denying services, and this attack came to be known as the Denial of Service attack. This threat introduced the information security concept of availability and the focus of Information Security now includes ensuring that access to information is possible at the desired time and moment. The focus or goals of information security have changed over time and most of the time

it is according to the current needs and requirements. Over the three decades of evolution; confidentiality, integrity and availability have become information security's main attributes (Cherdantseva and Hilton, 2012) and these concepts of information security are collectively known as the 'CIA Triads'.

2.4.1 Models and Evolution of Information Security

However, in recent years, with changes in the way information is handled, stored and communicated the threats to the security of information have also increased(IBM Security Services, 2015). Inevitably, the medium and needs for securing information have also augmented. Information on transit can be intercepted, modified, or new information can be fabricated giving rise to a new form of threats and vulnerability. The authenticity of information becomes very important, as integrity alone is not sufficient to ensure that the information truly came from the intended sender. An effective information exchange requires that the information received by the receiver was not compromised and it is also important that the sender does not deny the validity of the information and refuse to be associated with the information exchange. This denial of association and responsibility for the validity of the information is known as non-repudiation (Fielden, 2010; Wilson et al., 2012).

Authenticity and non-repudiation are two additional security goals introduced by another information security model that evolves from the definitions and concepts of Information Security defined by the legendary CIA triad. This model is known as the 'five pillars' model of information assurance (IA), which is seen not only to achieve the pre-defined security goals but the successful operation and the overall protection of information. The 'five pillars of IA' is defined by the U.S. Department of Defence within the National Information Assurance Glossary, Committee on National Security Systems Instruction CNSSI-4009. The glossary defines Information Assurance as "Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation". The UK cabinet office 2007 shared the same definition of IA as "the confidence that information systems will

protect the information they carry and will function as they need to, when they need to, under the control of legitimate users". Boyce and Jennings (2002) claims that the five pillars of IA involve protecting the rights of people and organisations. McKnight (2002) suggests that IA extends beyond the technical domain; in a broad sense IA incorporates the product, procedures, and policies that allow the timely transfer of information in an accurate and secure way among involved parties. Despite the claims that IA covers all the elements involved in information security, it does not explicitly mention standards and guidelines that relate to the management of the human element, in the information security process. It only addresses information security from the technological perspective and fails to take into consideration the organisational, legal and human perspectives. Cherdantseva and Hilton (2012) argue that even the new Five Pillars of IA still not adequately reflect the complexity and scope of the information security disciplines in full. The following figure illustrates the five pillars of IA.

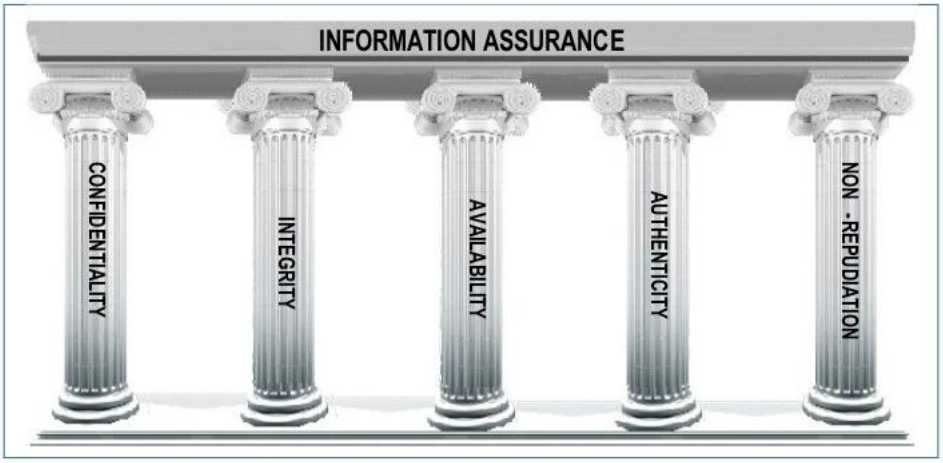


Figure 2.0 ***Five pillars of Information Assurance***

In 2002, Donn Parker proposed an alternative model for the classic CIA triad that he called the six atomic elements of information. This model is also known as the 'Parkerian Hexad" The elements are confidentiality, possession, integrity, authenticity, availability, and utility. Authenticity, utility and possession or controls are three new security goals in the new model. According to Parker, the CIA triads model was very technology driven and does not focus enough on the human element of information

security. His new model aims to change how information security is understood and implemented and to fill in the gaps of the CIA triads model in improving the security of current information assets. It is in the interests of Parker's model to address the possible threats from the weakness of human, for example, ensuring the authenticity of information handled, ensuring control over the possession of information and to ensure the usability of the information.

The security goals introduced by the three models (CIA triads, Parkerian Hexad and IA) in a way defined that if an acceptable level of security is to be reached the underlying goals must be achieved or maintained. Information must be confidential, not known to unintended persons; the information needs to be correct or consistent with the intended state of information. Breach of integrity from unauthorised modification of data, whether deliberate or accidental should be avoided. Information needs to be readily available, i.e. it needs to be accessed at any time thus protecting against hardware failures and distributed denial of service attacks and maintaining network health and functionality is critical. All the three goals mentioned in the CIA triads model along with possession and control mentioned in the Parkerian Hexad model focus on the protection of information. These additional goals are not necessary characteristics of information or system; instead, they are how procedures and methods to protect the confidentiality and the assurance of the information integrity and authenticity is characterised. The following table denotes the different models and goals laid down by each.

Table 2.2 *Different security goals set by the three information security models*

CIA Triads	**Information Assurance (IA)** **Five Pillars model**	**Parkerian Hexad**
Confidentiality	Confidentiality	Confidentiality
Integrity	Integrity	Integrity

Availability	Availability	Availability
	Authenticity	Authenticity
	Non-repudiation	Utility
		Possession

Although the Parkerian Hexad Model claims to include the human element of information security most of the measures and tools used to achieve these goals, for example, digital signatures, challenge-response passwords, bidirectional hashing, public key encryption, transaction certificates and time stamp are predominantly technological (Cherdantseva and Hilton, 2012). Despite the shift of focus from information protection to include the overall protection of the systems stated by the Five Pillars Model, it does not define the importance of the human elements of the information security. It does not explain how humans can and may contribute to the success and efficiency of information security. How the goals outlined by the various models are to be achieved is left to the individual or organisation to translate and find effective ways in which to attain them. These models clearly indicate what threats can arise from human discrepancies and weaknesses. Cherdantseva (2011) and Herath & Rao (2009) believe dependency on technology alone cannot guarantee security. Studies by Mcconnell & Hamilton (2002), (Notoatmodjo (2007), Bansal et al. (2010) and Liginlal et al. (2009) suggest that the main contributor to information security failures is the poor security behaviours of users instead of poor technical security solution.

2.4.2 A Socio-technical Approach

Despite the dependency on technology to maintain information security, there has, however, been a shift towards a holistic approach. This approach, a socio-technical approach, includes not only technology but other elements such as people, processes, and organisation design and strategy as well. The Socio-technical approach is about

harnessing the people's strengths and technical aspects of organisational structure and processes to achieve joint optimisation. Socio- technical approaches emphasise achieving excellence in both the technical performance and the quality of people's work, which was introduced by Eric Trist and Fred Emery, consultants at the Tavistock Institute in London in the 1960s. Initially, information security is seen as a three-way model comprising people, processes and technology (Dhillon and Backhouse, 2001) but the growth in complexity of information security saw that other elements such as organisation design and strategy was thought to be necessary (isaca, 2009). Looking at information security in its components (people, process, technology) has not proven to be an effective method to manage a security programme (Cherdantseva, 2011). A holistic approach that examines the system as a complete functioning unit is necessary. For this ISACA, a worldwide association of IS professionals dedicated to the audit, control, and security of information systems IS (formerly known as information systems audit and control associations) came up with its information security model called the 'business model for information security (BMIS model)'. The BMIS model was introduced as a holistic and business-oriented approach to managing information security that aims to assist security professionals to address the complexity of security while encouraging a balance between protection and the business. The model highlights the importance of the human contribution to achieve an appropriate level of information security. Humans as the information security user must ensure the balance between all elements in the system (Anderson, 2003). Figure 2.1 shows the difference between the CIA Triads approach, which focuses more on achieving information security goals and the holistic approach adopted by the BMIS model.

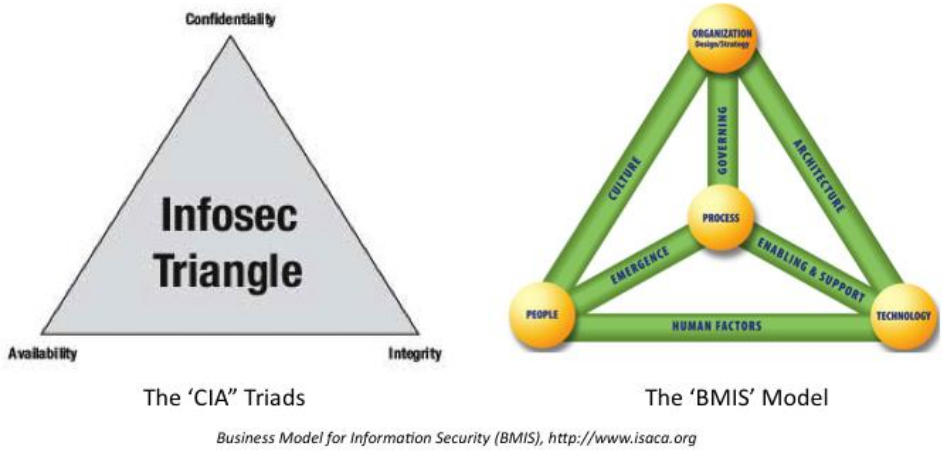


Figure 2.1 *The CIA Triads vs. the BMIS Model*

Despite the realisation that major weaknesses in properly securing information assets involves individual user within an organisation, actual security research is still focused more on technical issues (Crossler et al., 2013). To reduce the risk of systems' vulnerability from attackers and to guide users to practice appropriate information security procedures, organisations often rely on technology-based solutions (Ernst & Young 2008; PricewaterhouseCoopers 2008). The technology aspect of information security is a well-developed area in which much work and research have been done. Technological approaches to information security can be organised into proactive and reactive approaches. Proactive approaches are initiating preventative measures to secure data or resources before a security breach can occur while reactive approaches initiate curing measures to secure data or resources as soon as a security breach is detected (Venter and Eloff, 2003).

On the proactive approaches, several active research areas include improvement of cryptography technology, digital signatures, digital certificates, the use of Virtual Private Network (VPN) and vulnerability scanners. Companies such as Microsoft and Java are improving their security software development kits (SDKs) assisting in the development of web-based authentication programmes. Anti-virus technology companies continually follow and study virus developer approaches and devise methods to overcome threats created by them. Research on improving antivirus scanners involves developing new

methodologies to detect virus format and patterns (Rad et al., 2011). Similarly, there is a substantial body of research on reactive approaches to improving information security. Research in this area includes: new generation firewalls (Thomason, 2012) with deep packet inspection ability; new encoding techniques and sensory methods for improving intrusion detection; intrusion prevention systems and mechanisms (Hansen et al. 2007; Ayuso et al. 2012); improvement of existing passwords mechanisms (Weirich & Sasse 2001); the development of new techniques for secure password usage (Forget et al., 2008a) (Sasse et al. 2001); the development of new technology to support advanced passwords (Forget et al., 2008b; Brostoff & Sasse, 2003) and biometrics technology. Various new methods have also been identified to help in developing new anti-phishing techniques to combat the ever-rising threats on the web(Thiyagarajan et al., 2010). Phishing is a form of deception in which an attacker attempts to fraudulently acquire sensitive information from a victim by impersonating a trustworthy entity (Jagatic et al., 2007). Despite all the development in the technical aspects of information security, it is acknowledged that technology and process alone do not solve the problems (Kim et al., 2007). Schulz (2005) stated that Information security is not only a technical problem but is also a 'people' problem.

2.4.3 Information security, are humans the problem?

Despite, the advancements in technology, the availability of good practice guidelines and policies as well as proper design and implementation of the organisational strategy, it still requires people to use the technology, observe outlined good practices and adopt the organisational policies and strategies (Doherty and Fulford, 2005; Doherty et al., 2009). Consequently, information breaches are still, all too frequently, experienced (Doherty and Fulford, 205). This leads to the indication that human behaviour is a key area for information security and contributes significantly to the effectiveness of information security countermeasures (Kral, 2001). Siponen et al. (2007) and Pahnila et al. (2007a) suggest that most information security incidents are caused by careless employees who do not comply with organisational security procedures or policies thus placing the organisations' assets and business in danger (Stanton et al., 2005). Similarly,

a study by Kraemer et al (2009) agrees with Siponen et al. (2007) and Pahnila et al. (2007a) suggesting that human and organisational factors play a significant role in the development of CIS vulnerabilities and are not the sole result of a technological problem or programming mistake. The relation of vulnerabilities with human behaviour led to researchers such as Muniandy and Muniandy (2012), Eric Savitz (2011), Bulgurcu et al. (2010), Notoatmodjo (2007), Harrison(2005), Sasse et al. (2001) to postulate that ' The human is the weakest link' in information security. The same issue is augmented by PriceWaterhouseCoopers in their current 2012 survey. The survey states that most of the reported information security breaches and incidents are human related: fraud and theft using computers, physical theft, staff misusing facilities, infringement of laws and regulations, internal and external attacks and careless action by employees.

It is due to this realisation that much research has been dedicated to finding solutions on how to improve human compliance towards information security policies. Some of the areas that are being studied are: human decision making when faced with information security, the determinants or influencer of human intention to behave, and how intention to behave can be used to predict the choice of actual behaviour.

2.4.4 Compliance with information security

Pahnila et al. (2007b) and Bersz (2004) suggest that to improve employees' compliance with information security policies and guidelines, employees need to be provided with appropriate awareness, education and training (AET). D'Arcy et al. (2008) found out that employees' awareness of security procedures, security education, training, and awareness (SETA) programmes, and computer monitoring may have a deterrent effect on IS misuse. However, despite significant investments in AET, many organisations still experience security breaches, initiated by insiders (Verizon, 2012; Richardson, 2008). Insider breaches include non-compliant behaviours (whether intentional or not) by staff, and usually results in financial losses (PWC, 2012). Some organisations have even seen their reputation ruined (Bulgurcu et al., 2010). These apparent weaknesses posed by the human elements of information security have spurred studies to understand how

human behaviour is significant in the improvement of information security compliance. As detailed in the following section, researchers have studied the factors that may influence intention to behave based on variables suggested by various theoretical models.

2.5 Modelling human behaviour

This section presents the findings on the review of existing literature on various model or theories that are commonly used to study human behaviours towards several specific issues. It is believed that theories and models may help explain behaviour, as well as suggest how to develop more effective ways to influence and change behaviour (Glanz and Bishop, 2010). The understanding of these theories contributes to the construction of the fundamental framework, which underpins this research. Amongst the vast selection of theories that explain socio-technical behaviours, a small group of theories were chosen as a focal point for this study, because they were very much about people's behavioural formation and intention in the context of IT. Therefore, they are the most relevant to the research context. However there is one group of theories such as Theory of Planned Behaviour (TPB), Social Cognitive Theory (SCT), Protection Motivation Theory (PMT) and General Deterrence Theory (GDT) which have been chosen as the point of departure for this particular study because they have a very explicit focus on behavioural intention. According to Lebek et al. (2013) and Siponen (2010) there are four dominant applied behavioural theories that are commonly used in the context of Information Technology. Additionally, another behavioural theory that was looked at which is widely used in the human health area is the Health Belief Model (HBM). The HBM helps in predicting human action towards medical processes and procedures. The following paragraphs briefly explain these theories, in general, and critically appraises their significance to this research study. The remaining theories from the initial small group chosen for this study are presented in Appendix F.

TPB is an extension of the theory of reasoned action (Ajzen and Fishbein 1980; Fishbein and Ajzen 1975) and explains an individual's intention to perform a given behaviour. The theory postulates that behaviour can be explained by behavioural beliefs, normative beliefs, and self-efficacy as antecedents of attitudes, subjective norms, and perceived behavioural control, respectively.

SCT explains how people acquire and maintain certain behavioural patterns while also providing the basis for intervention strategies (Bandura, 1997). According to the social cognitive theory evaluating behavioural change depends on the following factors: environment, people and behaviour. People do not learn new behaviours solely by trying them and either succeeding or failing, but rather, the survival of humanity is dependent upon the replication of the actions of others. Depending on whether people are rewarded or punished for their behaviour and the outcome of the behaviour, that behaviour may be either be rejected or imitated.

PMT was originally proposed by (Rogers, 1975) to provide conceptual clarity of fear appeals. A fear appeal is a perceived condition in which, a user on the threat if they do not exercise some action on certain things. For example, if you don't "buy or use" some product or services particular dreadful consequences will be experienced. Roger (1983) extends the theory to a more general theory of persuasion with the emphasis on the cognitive processes promoting behavioural change. Protection motivation is the result of the threat appraisal and the coping appraisal. Based on human health environments, threat appraisal is the estimation of the chance of contracting a disease (vulnerability) and estimates of the seriousness of a disease (severity). A coping appraisal consists of response efficacy and self-efficacy. Coping appraisal includes response efficacy, the individual's expectancy that carrying out recommendations can remove the threat and self-efficacy, which is the belief in the individual's ability to execute the recommended courses of action successfully. The Protection Motivation Theory proposes that we protect ourselves based on four factors: the perceived severity of a threatening event, the perceived probability of the occurrence, or vulnerability, the efficacy of the recommended preventive behaviour, and the perceived self-efficacy.

GDT is adapted from criminal justice research. It is based on rational decision-making. GDT states that perceived severity, the certainty of sanctions or punishment influence the decision to engage in crime by balancing the cost and benefits (Straub, 1990).

HBM is a psychological model that attempts to explain and predict health behaviours and is mainly used in the healthcare research but has recently been adapted to studies

on information security compliance. This perspective is applicable because security practices can be seen as preventive behaviour to avert security incidents (Ng et al., 2009). The model suggests that an individual's behaviour is determined by the threat perception and evaluation of the behaviour to resolve the threat. This model focused on the attitudes and beliefs of individuals. It was first developed in the 1950s by Hochbaum, Rosenstock and Kegelsin response to a failed free health programme given by the U.S public health services. The Health Belief model postulates that a person will take a health-related action if he feels that a negative health condition can be avoided, or has a positive expectation that by taking a recommended action will avoid that negative health condition and he believes that the recommended action is accomplishable. The constructs that outline this model includes: individual perceptions of his chances of getting a condition and how serious are the condition and what are its consequences, these are perceived susceptibility and perceived severity respectively. Perceived benefits, the belief in the efficacy of the advised action to reduce risk or seriousness of impact, perceived barriers, the belief of tangible and psychological costs of the advised action, cues to action, strategies to activate the readiness to take the action and self-efficacy are the other constructs that are used by this model to predict human behaviour.

One point, which is common amongst all the theories and models, mentioned above, is the users' perception and its relation to the users' resultant behaviours. Perception is described as the 'act or faculty of perceiving, or apprehending by means of the senses or the mind; cognition and understanding' (Oxford Dictionary, 2015). The various models and theories suggest that user' perceptions on certain issues or variables may have an influence on the next action they will undertake. Although the theories and models suggest the significant of users' perceptions to their choice of behaviours, these insights are mainly quoted from findings on general issues and behaviours, and they are not specific to information security and information security behaviour. Therefore, it is important to explore the validity of these theories through the constructs and

determinants used in various application in similar context, specifically within the issues of information security.

2.5.1 Constructs and determinants of Information Security Behaviors

Many studies have extracted, adapted and tested the various constructs; determinants and antecedents suggested by various significant theories believed to have had an influence on human intention to behave and predictions of the actual behaviour. Table 2.3 and Table 2.4 lists out the various constructs, determinants and antecedents studied by various researchers in light of the theories mentioned earlier. A red star in the rows of the respective constructs shows that no significant impact was found in the study/studies they were used in, while the black star shows a discovery of positive impact.

Most of these studies, explore the impact of different users' perceptions, in the form of a variety of constructs, determinants and antecedents, might ultimately influence their information security behaviour. Studies by Pahnila et al. (2007a), Siponen et al. (2006), Siponen et al. (2007) Siponen et al. (2010), Herath and Rao (2009), and Ifinedo (2012) found that the individual's perception of social normative pressures, or relevant others' beliefs that he or she should or should not perform such behaviour that is also known as normative beliefs have a positive impact on the individual's intention to behave. This strongly suggests that the perceptions of others are important the user in how they determine the behaviour they should adopt. The same studies also found out that the individual's perception of their ability to manage and cope with the situation faced (coping appraisal) also has the same impact on the individual's intention to behave. Chan et al. (2005) study found out that self-efficacy coupled with the positive change in employees' perception of the current organisational information security climate (state) had a positive impact on employee's compliant behaviour. Bulgurcu et al. (2010) posit that an employee's attitude is influenced by the benefit of compliance, the cost of compliance, and cost of non-compliance, which are beliefs about the overall assessment of consequences of compliance or noncompliance. This study suggests that the user'

gauged importance of the information, to him or her, plays an important role in developing their perceptions towards the information.

The above notion is strongly supported by the study of Beautement et al, (2008). Beautement et al's study suggests that users' intention to behave, in the context of of information security, is largely influenced by the actual and anticipated costs and benefits, and that there exists a threshold after which the user perceives too much anticipated cost over benefit, resulting in a circumventing security procedures.

Other researchers have studied various ways for improving information security compliance; Albrechtsen (2007) has worked on *involving users in information security design*, Chen et al. (1992) and Furnell et al. (2002) used *e-learning and interactive computer-based learning* to improve awareness, while, Cox et al., (2001), Hansche (2001) and ENISA(2006) suggest that by *improving communication of risk and better communication* and discussion on information security amongst employee will help improve behaviour towards information security, this is supported by (Bulgurcu et al., 2010) stating that the *features of Information Security procedures* may also influence user behaviour towards complying with such procedures. The findings mentioned above also suggest that, by empowering users, they will develop the sense of belonging and recognise the appreciation of their contributions and involvements. It is through these recognitions they are postulated to consider the importance of the information thus appreciate the security and protection of that specific information.

Furthermore, Siponen & Vance (2010) and Ifinedo (2012) found out that *deterrence* methods are effective in influencing employee compliance behaviour. Other authors like Power (2007), Power & Forte (2006), and ENISA (2010) suggest that to have an effective improvement in information security, the *organisations' culture needs* to be changed to deliver a more holistic view of information security. The studies mentioned above suggest that culture, especially organisational culture plays an important role in the issues of information security. This notion warrants an investigation into whether culture, both from the national and organisational level would have influence over information security decisions.

Additionally, other researchers have looked into other factors such as *persuasive technology* to influence users to choose more appropriate behaviour when faced with information security issues Yeo (2009). Other factors, including *elements of human characteristics and traits,* have been studied to understand the act of compliance phenomena (Shropshire et al., 2006). Shropshire et al. (2006) postulate that human conscientiousness described as 'socially prescribed impulse control that facilitates task and goal oriented behaviour, such as thinking before acting, delaying gratification, following norms and rules, and planning, organizing, and prioritising tasks' and agreeableness, friendliness pro-social and communal orientation towards others that include traits such as altruism, tender-mindedness, trust and modesty are positively related to Information Security compliant behaviour.

In another study, Aytes and Conolly (2003) assume that risky computing behaviour is the result of *individual choices,* and argue that conscious thought about the consequences may play some role in guiding risky behaviour. The model proposed by (Aytes and Conolly, 2003) postulates that the antecedents of a user's choice are the *user's perceptions* of several factors such as availability and usability of safe practices, the *probability of negative consequences, the significance of negative consequences*, ease of recovery, and *beliefs regarding peer behaviour*. The user's perceptions of these factors are formed based on the knowledge of the user on the factors constructed from various information sources such as training attended, news and media, through communication with peers and friends, policies and procedures as well as personal experience.

Li & Chen (2011), in their study to explain disclosure privacy behaviour on social network sites, combine TPB with privacy calculus theory. Privacy calculus theory posits that for a user to consider using an information security countermeasure, the benefit perceived by the user must exceed the risk to guarantee the motive of self-disclosure. This finding application to the use of information security countermeasure may also be relevant; that is if the user perceives the value of information they are handling as high they might see the need for the protection of the information as much higher.

Table 2.3 *constructs, determinants and antecedents of information security behaviours studied*

Research	John Adam Risk (1995)	Weirich (Avialable Behaviour)	Thaler and unstein (Nudges)	Fishbein & Ajzen (TRA/TPB)	Kankanhalli et al. (2003)	Stanton et. al. (2005)	Chan, Woon & Kankanhalli (2005)	Kraemer et. al. (2006)	Siponen et. al. (2006)	Pahnila et. al. (2007)	Siponen et. al. (2007)	D'Arcy & Hovav (2007)	Albrechtsen (2007)	Kraemer and Carayon (2007)	Beautment, Sasse and Wonham (2008)	Beautement et. al. (2008)	Herath & Rao (2009a)	Herath & Rao (2009b)	Ng, Kankanhalli & Xu (2009)	Myyry et al. (2009)	Jhonston & Warkentin (2010)	Li, Zhang & Sarathy (2010)	Siponen, Pahnila & Mahmood (2010)	Siponen, Vance &Willison (2010)	Vance et. al. (2010)	Belgurcu, Hassan & Benbasat (2010)	Guo et. al. (2011)	Ifinedo (2012)	Mohamed & Ahmad (2012)	Li & Chen (2010)	D'Arcy et. al (2009)	Kankanhalli et. al (2009)	Williams (2012)	Pahnila et al (2007)	Clark and Wilson (1987)	Cox et al (2001)	Hansche (2001)	ENISA (2006)	Ng et. al (2009)	Karjalainen (2011)	Albrechtsen and Hovden (2009)	Peltie (2005)	Doherty and Fulford (2006)	Kayworth and Whitten (2010)	Padayachee (2012)
Variables	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**	**32**	**33**	**34**	**35**	**36**	**37**	**38**	**39**	**40**	**41**	**42**	**43**	**44**	**45**
Threats																																												
Percieved Severity									*	*	*						*	*	*		*							*	*														
Percieved Probability (Vulnerability)	*	*														*	*						*		*	*	*	*														
Percieved Susceptibility										*									*								*		*													
Security Visibility							*		*			*											*																				
Detection probability																	*					*																				
Coping Apprisal																																											
Self efficacy							*		*		*						*	*	*		*				*	*		*	*													
Response Efficacy									*		*						*	*			*		*		*				*													
Sanction/Detterence																																											
Percieved Severity/ Deterrent Severity																														*	*	*											
Percieved Certainty/ Deterrent efforts																														*	*	*											
Formal Sanction		*									*					*				*			*	*		*	*														
Shaming																								*																			
Benefits																																											
Percieved/Anticipated Benefits	*	*	*	*												*		*	*			*	*				*															
Actual Benefits															*	*																											
Normative beliefs									*	*													*			*	*																

* non significant * Positively significant GDT - General Deterrent Theory SCT - Social Cognitive Theory PMT - Protection Motivation Theory

TPB - Theory of planned behaviour HBM - Health Belief Model

Table 2.4 *constructs, determinants and antecedents of information security behaviours studied (continued)*

Research	John Adam Risk (1995)	Weirich (Avialable Behaviour)	Thaler and unstein (Nudges)	Fishbein & Ajzen (TRA/TPB)	Kankanhalli et al. (2003)	Stanton et. al. (2005)	Chan, Woon & Kankanhalli (2005)	Kraemer et. al. (2006)	Siponen et. al. (2006)	Pahnila et. al. (2007)	Siponen et. al. (2007)	D'Arcy & Hovav (2007)	Albrechtsen (2007)	Kraemer and Carayon (2007)	Beautment, Sasse and Wonham (2008)	Beautement et. al. (2008)	Herath & Rao (2009a)	Herath & Rao (2009b)	Ng, Kankanhalli & Xu (2009)	Myyry et al. (2009)	Jhonston & Warkentin (2010)	Li, Zhang & Sarathy (2010)	Siponen, Pahnila & Mahmood (2010)	Siponen, Vance &Willison (2010)	Vance et. al. (2010)	Belgurcu, Hassan & Benbasat (2010)	Guo et. al. (2011)	Ifinedo (2012)	Mohamed & Ahmad (2012)	Li & Chen (2010)	D'Arcy et. al (2009)	Kankanhalli et. al (2009)	Williams (2012)	Pahnila et al (2007)	Clark and Wilson (1987)	Cox et al (2001)	Hansche (2001)	ENISA (2006)	Ng et. al (2009)	Karjalainen (2011)	Albrechtsen and Hovden (2009)	Peltie (2005)	Doherty and Fulford (2006)	Kayworth and Whitten (2010)	Padayachee (2012)
Variables	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**	**32**	**33**	**34**	**35**	**36**	**37**	**38**	**39**	**40**	**41**	**42**	**43**	**44**	**45**
Percieved Barriers																																													
High Workload								*					*	*																															
Precieved Costs	*	*	*	*												*							*																					
Response Costs																	*								*			*																
Public Image		*		*			*									*							*																					
Awareness, Eduction & Training (AET)																																												
Better knowledge of information security																																									*	*			
Sufficient awareness of AET						*	*					*			*																			*							*	*	*		
Organisation																																													
Organisation Culture/Climate							*								*																														*
Perceived Risks																																													
Percieved security riisk																												*								*	*	*					*		
Rewards																																													
Tangible							*									*							*		*				*				*	*									
Intangable (work appreciation, praise from peers)		*	*	*			*				*					*	*	*			*	*	*					*															
Personal accomplishment							*																																						
Rewards from non-compliance	*														*																														

* non significant * Positively significant GDT - General Deterrent Theory SCT - Social Cognitive Theory PMT - Protection Motivation Theory

TPB - Theory of planned behaviour HBM - Health Belief Model

In another study, Liang and Xue (2009) suggest that technology acceptance theories while providing valuable insights on how humans intend to behave, do not provide insight into users' IT threat avoidance behaviour. Liang and Xue postulate a theory of technology threat avoidance theory (TTAT). Liang and Xue's TTAT posits that when users perceive a threat, they will comply with the countermeasures provided when they believe that the threat is avoidable by adopting such countermeasures; otherwise if they believe that the threat cannot be fully avoided by the information security countermeasures, they would resort to emotion-focused coping. Emotion-focused coping is adjusting one's desires or the importance of desires so that negative emotions related to threat (e.g., fear and stress) are mitigated. It includes various modes such as religious faith (beliefs in God's will to remove danger), fatalism (acceptance of a dangerous situation), denial (denial of the presence of danger), and helplessness (internalisation of blame or resignation for not being able to control the danger) (Lazarus and Folkman, 1984). This process of perception of threat relates to the extent to which the users value the information and how well they think the countermeasures can prevent them from experiencing the consequences of the threat. Liang and Xue (2009) further suggest that IT users need to be educated about not only the likelihood of being attacked by malicious IT but also the negative outcomes once they become victims.

The studies mentioned above suggest that a user carries out some analysis, weighing up the pros and cons before deciding on how they will react and behave towards that certain action. The construct of this process is known as perceived value (Rajh, 2012). In the marketing and e-commerce field, perceived value is seen as an important determinant of consumer shopping behaviour (Eggert and Ulaga, 2002) in which, the higher the value assigned by consumers on certain products greatly determines the likelihood of a purchase. Similar constructs; such as perceived risks, perceived benefits, perceived costs, perceived susceptibility, perceived severity and perceived barriers from various behavioural theories have been studied for their influence on humans to perform the appropriate behaviour towards information security behaviour but no study have explored the potential of perceived value.

The idea of treating information as a commodity leads to the notion that a matrix of measure of values can be assigned to information and it is realised that these values are subjective to different individuals, groups and organisations about the fulfilment of their needs of the information. People's belief in outcome and judgement relies heavily on their perceptions of the likely outcome of a particular action or behaviour (Adams J, 1999). Therefore, there is an opportunity to explore the ability of 'perceived value' as a construct to building the beliefs of end users that outcomes of secured behaviours are beneficial.

2.5.2 The Human Behavior towards Information Security

Reliance on employees to behave sensibly is the last defence an organisation may have and it could prove to be the most important one. No matter how good an organisation's security policies and standards, security documentation simply cannot spell out unambiguously how staff should act in each situation they might encounter (Leach, 2003). It is understood that compliance behaviour is a complex matter, "compliance may vary from a truly accepted security culture at one extreme through to active disobedience at the other" (Furnell and Rajendran, 2012). To improve on human compliance, it is inevitable to study and understand how compliance works and the understanding of factors that may influence and affect compliance is inevitable. Understanding of the factors that motivate undesirable behaviours by employees is still considered very limited (Guo et al., 2011).

Tackling the compliance behaviour involves a decision action procedure that a person has to go through. Thaler & Sunstein (2008) describe a 'human thinking system', which is driven by either human gut feeling or human reasoning. A decision resulting from human reasoning is an outcome of a careful process of weighing the pros of cons of various factors that may include acceptable grounds and rules, experience and knowledge on the matter. Leach (2003) highlights that the influencing factors that can affect users' behaviour can be categorized into two main groups, the factors that may influence users' understanding of what behaviours the organisation expects of them and the second group are factors that may influence the users' personal willingness to constrain their behaviour to stay within accepted and approved normality. Leach (2003) further categorises the factors that may influence user understanding of what behaviours are expected of users into the following:

the body of knowledge (values, policies, standards, procedures, etc.), peer behaviour, user's security common sense and decision-making skills. On the other hand, user's willingness to constrain their behaviour to stay within accepted norms is further categorised into the user's personal values and standards of conduct, user is psychological contact with their employer and the users' perceived effort required for adopting the compliance behaviour. Human behaviour changes over time, and according to the situation, and it also changes according to self-assessment of the situation and the requirements of the environment.

There are many factors or issues that influence and can determine how behaving user might behave. Behaviour is closely related to attitude towards an object or subject although not necessarily all the time. Fishbein and Ajzen (2011) define attitude as a tendency to respond with some degree of favorableness or unfavourableness to a psychological object. A common example is the liking or disliking of a particular habit such as the habit of smoking; for example, people who despise smoking have a very high probability of being a non-smoker, but people who do not despise the action of smoking are not necessarily smokers. Users' attitudes towards security compliance are mainly based on what they learn from other people's experience (mostly acquired from incident(s) happening around them and what is reported) and users' attitudes are also shaped by the organisation's culture. This perspective of users' attitude based on "Community Practices" in which users bounded together as a community sharing the same services; for example, an organisation Intranet and network facilities. People in such communities learn from and with each other's day-to-day experiences. A company culture and custom directly influences their employees' behaviour. The behaviour is demonstrated by senior management and peers in the way they share personal experiences and advise each other on how to behave in a specific situation (Wenger, 2009). The drawback of this practice is that new users may copy everything from the community including bad behaviours and attitudes, assuming they are the most appropriate approaches, as they've been practised by the community. In an organisation, the body of knowledge made available to the employee on how the organisation perceived information security would greatly influence how they behave. The employees' understanding of which behaviours are expected of them is formed from: what they are told

(Company's security values and principles), what they see being practised by others around them and their experience built from decisions they have made in the past (Leach, 2003).

Motivation involves working to raise the probability that people will make choices or decisions that are positive. Dirk Weirich (2005) suggests that employee behaviour change is highly motivated or influenced by the individual's economic reasoning in performing the behaviour. Employees weigh the importance of behaviour by its primary and secondary cost, social cost and image cost. The primary cost for an employee that uses a strong password is to memorise the password and by assigning passwords to each password protected computing resources will add up to the primary costs. To choose a weaker password will result in the employee being denied access to his computing resources thus incurring him a secondary cost. The impact of their behaviour on their social relationship is also seen as a cost to an employee; it is measured with how well their behaviour is being accepted by their peers and friends. An employee might share his password just to avoid being labelled as not trusting. Employees also measure the benefits that they acquire from performing certain positive behaviours. Such benefits are social benefits and image benefits. Employees are keen on performing behaviours that can improve their social relationships and popularity among colleagues whether the behaviour complies with the organisation policy, or not (Weirich, 2005). Image benefits also contributes to employees' cost-benefit evaluation. If the behaviour reaffirms or improves one's self-image or their public image its tendency to be adopted is high.

Beautement et al. (2008) extended Weirich's (2005) availability model, to study the additional costs perceived by employees. Among the additional costs are increased the physical load, increased cognitive load, embarrassment, missed the opportunity and the hassle factors. Humans are also frequently influenced or nudged by other humans (Thaler and Sunstein, 2008). According to Thaler and Sunstein (2008) social influences may have great effects in changing human behaviours, and it comes in two basic categories, peer pressure and information conveyed by other people's actions or answers. This view is supported by Fishbein and Ajzen (2011), in their theory of planned behaviour. This belief will lead to a perceived social pressure to engage in the behaviour. In this context, peers' and superiors' behaviour may affect or influence one's behaviour. In the end people adopt the

behaviour, which they deem to be acceptable to the people surrounding them and acceptable code of practice by his community. Thaler and Sunstein (2009) describe this as "following the herd". Dirk Weirich and Martina Angela Sasse (2001) reported that most individuals try to "fit in" rather than going against the community; this behaviour is strongly influenced by behavioural norms or what is expected of them. These findings might apply to how users assign a value to information and information protection. There is a possibility that a user might place the same value to an information asset similar to the value they believe others (users or their peers or superiors) perceived for that same information asset just to be seen belonging to the community.

2.5.3 Information Security Behaviour taxonomy

Stanton et al. (2004) define a taxonomy of security behaviours that comprise malicious behaviour, good behaviour and neutral behaviours. *Malicious behaviours* come with intentions to do harm to the organisations. Employees with malicious intentions or behaviour are described as "insider's threat". Most current AET frameworks and models target behaviours with the malicious intention or malicious behaviour as most research focuses on studying these internal threats. *Beneficial behaviour* comes with good intentions to protect and preserve the organisation's IT and resources. Such behaviour is seen as the ideal behaviour and organisations strive to instil these forms of behaviour in their employees. The behaviours that are paid less attention to are the *neutral behaviours*; these are behaviours with no intentions to do any harm, but which have detrimental effects on the organisation's security. Non-malicious behaviour is further divided into two categories; dangerous tinkering and naïve mistakes.

Both categories of non-malicious behaviour do not have any clear intention to harm the organisation's information technology and system. Examples of these behaviours are if an employee configures a wireless gateway that inadvertently allows an outsider wireless access to the company's network or a user choosing a weak password such as "password". These behaviours violate policies, but rather than malicious intent, they emerge from a failure to understand the consequence of behaviour for the organisation. These behaviours are termed non-malicious, yet non-complying, behaviours. Non-malicious behaviour can be

a result of failure to understand the risks involved, or employees are aware of the risk, but choose compromising behaviour because they perceive the effort involved with compliance as too high.

Alfawaz et al. (2010) define four modes of individual security behaviours, the: Knowing-Doing mode, Knowing-Not doing mode, Not knowing-Doing mode and Not knowing-Not doing mode [see figure 2.2]. Alfawaz's Knowing-Not doing mode is a situation where an individual has the required knowledge and skills, but decides not to adopt the right behaviour. This behaviour may violate the norm of expected behaviour and may compromise security; examples of this behaviour are users using shortcuts to accomplishing risky task and users ignoring related procedures and rules. Guo et al. (2011) describe a similar behaviour as non-malicious security violations. Crossler et al., (2013) divided inappropriate information security behaviour into two categories i.e. intentional behaviour also known as deviant behaviour including behaviour such as sabotage, stealing and industrial or political espionage and unintentional behaviour also known as misbehaviour that includes employees selecting simple passwords and visiting inappropriate websites.

Stanton et al. (2004) describe non-malicious behaviours as behaviour that has no intent to cause any detrimental outcomes contrary to Guo et al. (2011), who categorised intentional behaviour as non-malicious behaviour in the context, which implies that end users make "conscious decisions' to follow a course of action. Information security awareness programmes are an important approach towards educating users to prevent security incidents. It is critical that people understand their role in protecting information and information assets (Russell, 2002). Once a person undergoes security information AET, his ill understanding of the consequences of non-compliance behaviour is hopefully eliminated. He is then expected to take the compliant standing (Knowing-doing mode). Otherwise he is taking the Knowing-Not-Doing mode as described by (Alfawaz et al., 2010). This view is significant to the 20-60-20 theory of people segmentation.

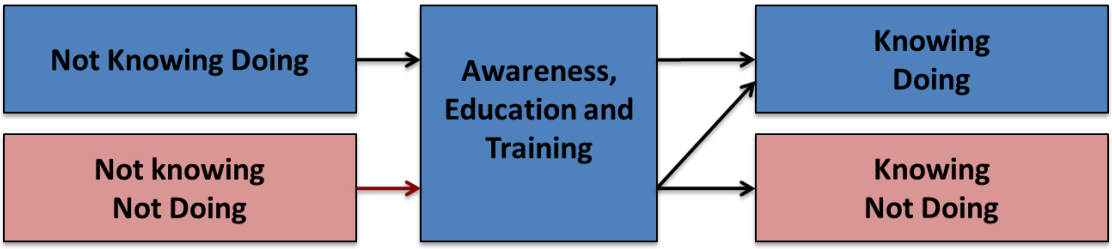


Figure 2.2 Individual security behaviours, (Alfawaz et al., 2010)

The theory is widely applied in the field of leadership and time management despite lacking empirical evidence (Strand, 2013). The 20-60-20-theory postulate that the top 20% of the population are already ready and on board with the desired situation; in the context of information security this is the '*not-knowing-doing*' groups of people, although not knowing what is expected of them and what are the consequences of their behaviour, but their behaviours are in line with the policy. 60% of the people can be influenced one way or the other to follow certain rules and regulations. These are the group of '*not-knowing-not-doing*' people, which with appropriate AET programmes will transform into '*knowing-doing*' people. The remaining 20% of people, the lower percentile or the negative 20% are the hardest people expected to have a compliance standing. Although, in the leadership and management area, this group of people are considered 'a waste of time' and should be left alone; in the context of information security, these are the people who if not addressed will become the highest vulnerability and invite threats to the organisation.

Two things can be derived from these concepts of behaviour: firstly, AET programmes are mostly effective to motivate 80% of the people on information security issues; and secondly, traditional AET will not work for the negative 20% of the population. In this context, an additional approach should be studied to compliment and enhance existing efforts to improve compliance with information security countermeasures.

2.6 Concluding Remarks

This chapter has a sought to outline the fundamental thinking into the key issues underlying this research. One of the earliest points established in this chapter is the range of different perspectives through which this study could investigate the issue of information and its security. There are two different sets of stakeholders i.e. as an individual and as a group or organisation. This individual or group setting is further subdivided into a group that has information technology or information security knowledge, a group that comes from the management level and the group that consist of day to day users of information. The management level stakeholders and the stakeholders with IT/IS background are also considered to be the owners of the information, as they will ultimately be responsible for the consequences of any breaches of information occurs. It is the perspectives of these stakeholders that is the primary focus of this research. The reason for this interest is that it is these different stakeholders are the ones that make up a public organisation and these are the people who deal with information and its security.

Another point that was established from the literature review is wide variety of existing theories that have sought to explain the 'how and why' of information security behaviours. The research seeks to find alternatives, and hopefully more effective, ways to explain the reasons behind information security behaviour.

The theoretical framework will guide the development of the research. The translation of the understanding made at this stage into the investigation framework will be discussed in the next chapter, chapter 3.

3. Research Gaps, Objectives and Framework

3.1 Introduction

This chapter presents a summary and critique of the literature, from which the research gaps, to be explored, in this study are derived. Furthermore, this chapter also introduces the research objectives and the conceptual research framework that are deemed suitable to explore effectively the identified areas of interest. The research objectives and the conceptual research framework are the foundations that support the attempt to explore and address the research gaps identified in the literature. More importantly, they will help in the process of attaining the specific knowledge through which this study's contributions to the extant literature will be realized.

This chapter is divided into four sections; first, the chapter will present the identified gaps from based upon an analysis and critique of the existing literature. Then the discussion will move to the objectives of the research, which are important as they act as both the foundation and the direction finder for this research study. Next, the discussion will touch on the existing theories that shape the development of the research framework. In so doing, this will provide an additional rationale for the research, from which the study's conceptual framework is derived. The last section will present the research interpretive model that guides the studies made in the research, after which some brief concluding remarks are presented.

3.2 Critique of the literature and presentation of research gaps.

From the literature on human behaviour towards information security and information security countermeasures, it can be concluded that there are indeed some significant research gaps that warrant empirical exploration. The research gaps identified are critiqued and described below.

Firstly, the human dimension of information security management is highly dependent upon its successful management, but the precise nature of this relationship is extremely complex and opaque. Overall, it is evident that our understanding of users' compliance behaviour

towards information security countermeasures is partial, as most existing research has been based upon the quantitative, closed-ended questionnaire based survey approach. Therefore, to appreciate users' perspectives and representations of information security compliance behaviour, a detailed qualitative approach to study the phenomenon is important. It is necessary to have a comprehensive and in-depth understanding of the human behaviour elements of information security. A potentially productive way to achieve this would be to explore representations of users' perspectives of the phenomena by different level of users or stakeholders.

Secondly, there have been no previous studies that look into the *process of value assignment* by the wide variety of stakeholders affected by information security protocols. Similarly, there are also no studies that explore the relationship between the stakeholders' value assignment process and their ultimate information security behaviours. It is appreciated from the literature that different stakeholders hold different perspectives on information security. It is believed that these notions are derived from how the stakeholders' value the information they are handling. This valuation includes their understanding and definition of information security, its importance to them individually as well as to others, what they think entail appropriate information security and many other aspects. Therefore, these different views and perceptions may generate different perspectives towards information security and its compliance. In the business and marketing fields, a '*customer value'* from the viewpoint of a customer is what they "get" (benefits) in return to what they have to "give up" (costs sacrifices) (Zeithaml 1988). The customer value is the foundation for customer satisfaction and loyalty (Woodall, 2003) and has become the main key to success via differential positioning (Cooper 2001). Other researchers such as Rajh (2012), Eggert and Ulaga (2002), Sanchez-fernandez and Iniesta-Bonillo (2007) refers to the customer value as '*perceived value*' by the customer.

As evidenced in the literature, there is a strong notion that information is treated more and more as a commodity and with this arises the concept of *creating a matrix of measures for values that could be assigned to information*. It is fully realised that the issue of value is emphasised as a subjective matter and therefore it is important to correctly conceptualise it. Thaler (1985) pioneered the work on value function that based the concept in both

cognitive psychology and economic theories, however, recent studies in the same field have initiated the concept 'value' as a complex phenomenon and consists of several dimensions (Babin & Attaway 2000; Morris B. Holbrook 1994; Sweeney & Soutar 2001). Holbrook (1994, 1996) pointed out that apart from the simplistic understanding that users only want in return for what they have paid for or laboured for, there are more dimensions that can affect users' value on the object or commodity they are consuming (Gallarza et al., 2011; Sánchez et al., 2008). Holbrook (1994) developed an approach that captures diverse aspects of value creation, which includes economic, social, hedonic and altruistic dimensions.

An assumption developed around this research is that *the more an object is valued; the more willing, its owner will be to protect their object*. With regard to the possible value arising from the commodification and appreciation of information, it is envisaged that the 'perceived value' of information will have a mediating role in encouraging compliance towards its protection. In this context, there have not been any previous studies that explicitly explore and study the process of 'value assignment'. Moreover, there is no evidence in the literature that any study has been conducted to understand stakeholders' perspectives of information and information protection evaluation. In this regard, Holbrook's value dimensions will be used as the basis to explore the value dimensions used within the context of information security compliance behaviour. The justification for the selection of suitable dimensions from Holbrook's value is presented in Section 3.4 in this chapter.

Furthermore, the review of existing literature has also revealed that the insight into the relation of user's 'perceived value' with information security or protection compliance has yet to be sufficiently investigated. Herath and Rao (2009) in their study, describe the term 'perceived value' as the contribution (intrinsic incentive) to the organisational security policy compliance. Therefore, this research will adopt a similar definition of **perceived value**, namely: ' *a stakeholder's opinion of the value of the information he or she is handling (using, storing or communicating). It may have nothing to do with the price but more about what the information means to him or her usually in the form of intrinsic or/and extrinsic satisfactions. This value is susceptible to intrinsic or extrinsic factors that may influence the stakeholders' information appreciation (perception) that may determine their willingness to*

protect the information'. Consequently, the ***'perceived value'*** of information or the '***perceptions of information value'*** is postulated to be able to motive stakeholders to exercise appropriate security behaviours. It is expected that the 'perceptions of information value' (PIV) will provide the stakeholders' satisfaction in terms of feeling the contribution from one's actions. If the employees believe that their actions can contribute to greater good, such as organisational betterment, it is likely to induce a positive impact on their decision to carry out such actions.

The evidence from the field of marketing and health suggest that perceived value or customer value can be manipulated to influence the the customers' loyalty and patient compliance, respectively. In this regard, a study enhancing the understanding of how 'perceptions of information value' can contribute to information security compliance behaviour would indeed be an interesting area that is worth further exploration.

Moreover, it is also postulated that the perceptions of information value conceived through the process of valuation and assignment of value on information by the stakeholders are prone to influences from several factors. These factors might form the basis on which the valuation is made. Indirectly, how these factors influence the stakeholders' decision making will help to determine how much the stakeholders value the information. Subsequently, it also postulated that these factors could also assist stakeholders in determining the level of protection for the security of the information and as a result better compliance behaviour may be adopted. Although factors of influence information security issues can be found in the literature but the common approach for studying these factors was based on inductive approach. This research will study these factors based on a hybrid approach of inductive and deductive (further discussion in chapter 4), which will provide a fresh insight on the factors based on the perspectives of the stakeholders

To summarise, there are three gaps that have been identified and discussed above, which have been summarised in Table 3.1.

Table 3.1 Gaps identified from the review of existing literature

Gaps Identified
1. The extent to which stakeholders develop a clear perception of the information they handle, and the processes by which value is assigned, in the context of information security.
2. The relationship between 'perceptions of information value' and resultant stakeholders' information security compliance behaviours.
3. The identification and understanding of factors that may motivate or influence the stakeholders 'perceptions of information value'.

In general, it is believed that developing a richer understanding the process of information value appreciation and assignment will potentially contribute to an improvement in information security compliance. To explore and fill the understanding of the gaps mentioned above, several research objectives have been developed to answer questions that arise from the gaps identified. There are three research objectives developed corresponding to the three gaps, each of which will be discussed in the next section.

3.3 Research Objectives

This section will present and review the specific research objectives that were ultimately derived, to guide the conduct of this research study. More specifically, there are three research objectives that have been identified to address the research gaps mentioned in the previous section effectively. The research objectives are designed to provide systematic guidance in addressing these research gaps.

The basis of the objectives is to look into the perceptions of different stakeholder groups (individual/user and owner/management) about the information security issues as mentioned in the previous section. To appreciate the process of compliance decisions made by these stakeholder groups, it is important:

i To interpret and construct the meaning of 'perception of information value' from the perspective of different groups of stakeholders;

ii To distinguish between and categorise the variations of views and beliefs towards the value of the information they are handling.

iii To explore the relationship between the stakeholders' information perceived value and their protection level rating.

In particular, it is important to frame the process of assigning a value to information and how the protection of the information is being justified. For the objectives to be valid, the following assumptions have been applied to this study:

Assumption 1*: The intention to exercise appropriate behaviour is influenced by the variation of perspectives of stakeholders on their 'perceptions of information value' of the information they are handling.*

Assumption 2*: The Value placed on information assets is dependent on the personal assumptions on several influencing factors (for example importance of information, and the sensitivity of the information)).*

Assumption 3*: The higher the value placed on the information assets (by the stakeholder), the higher will be the need to protect it, and the more willing the stakeholders will be to comply with security measures.*

Assumption 4: *The behaviours enacted by stakeholders will have an impact on the value of the information.*

Assumption 5: *Organisational and national culture have a significant impact on how the stakeholders' approach the process of assigning value.*

The research objectives are designed to explore the possible influencing constructs or dimensions that may be experienced or used by users in their decision-making procedures in the context of complying with information security countermeasures.

3.3.1 Research Objective One (RO1) – 'Perceptions of Information Value.'

The first research objective relates to the key construct 'Perceptions of Information Value', as defined in chapter two. More specifically, the first research objective focuses on the need to explore the notion of 'Perceptions of Information Value' in the context of information security. Therefore, the first research objective is:

To understand the extent to which stakeholders develop clear 'perceptions of information value', and the processes by which they assign value to the information that they handle.

The major interest of this objective is to understand how individual, and organisation information security behaviour is formed based on how much they perceived the value of their information is. In this regard, the goal is to understand the overall approaches and the mechanism by which individual and organisation (public) look into 'value creation' towards information and its protection (information security).

As discussed in the previous section, there is little existing literature that explicitly addresses information security compliance from the perspective of users or stakeholders' perception of the value of the information they are handling. The closest literature in this regard is from the studies by Aytes and Conolly (2003) and Shropshire et al. (2006). Both of these studies touch on the human perception on why they should exercise appropriate information security due to perceived consequences faced if they fail to exercise adequate information security. It is realised that if the user can associate the information, they are handling with an appropriate value (that is dear to them), the willingness to comply with information security countermeasures would be expectedly higher. Furthermore, how the perceptions

of these two dimensions relate to how stakeholders choose to behave was never explored. It is believed that the stakeholders "perceived value" may be either self-constructed or it may be borrowed or copied from other stakeholders' valuation. Ultimately, it is envisaged that a stakeholder's willingness to comply with the security procedures, designed, to protect the information, may heavily depend on how valuable they perceive the information to be.

To explore this first objective, the study needs to understand the structure of the Brunei Darussalam public organisations, particularly to understand the significance of different stakeholders' contributions in the context of maintaining appropriate information security. This means exploring how stakeholders' appreciate the information they are handling and how they work around information security issues will provide a comprehensive understanding of how information security is practised in the Brunei Darussalam's public organisations. This will include exploring how different stakeholders classify their information and what are their perceptions of the importance and sensitivity of the information they are handling. Furthermore, the first research objective will also explore the common values used in appreciating the information. In general, the first objective is to explore whether the term 'Perceived Value" exists in the information security environment and if it does exist, the next task is to explore how the Information Perceived Value can contribute to the betterment of the security of information.

3.3.2 Research Objective Two (RO2) – Value assigning process

The main interest of the second research objective is to understand how stakeholders form or develop their information 'perceived value'. It is assumed that this involves a complex process of decision-making and value assignment. Therefore, RO2 will explore processes of decision-making that leads to value assigning to information (construction of Information Perceived Value) and how such processes interrelate and support each other.

It is postulated that the information security behaviours displayed by stakeholders result from multiple phases of complex decision-making processes. Furthermore, because there are different categories of stakeholders, therefore there are also different types of the decision-making process. It is also believed that these processes are related and in support of each other.

Therefore, the second research objective of this research is:-

> ***To explore and understand the relationship between stakeholders' 'perceptions of 'information value' and their resultant 'information security behaviours'.***

This second objective will explore the extent to which decisions on the Information Security Behaviour of stakeholders are prone to be influenced by their own 'perceptions of information value'. The second research objective will also look into how other's (stakeholders) perception of the value of the information they are handling might affect their information security behavioural decision.

3.3.3 Research Objective Three (RO3) – Factors influencing Information Security Behaviour

The decision-making process is usually in the presence of multiple criteria (Hwang and Yoon, 1981). These criterions are factors that may influence the outcome of the decision making. For example in choosing what car to buy factors such as price, gas mileage, safety, comfort, status and many others need to be addressed. The evaluation of the factors helps derives the value of the car to the buyer. In another word, the value of the car is prone to the influence of the factors mentioned earlier. Similarly, in the context of conceiving the

'perceived value' of the information they are handling, surely there are many factors that may influence the value. Hence, it is important to explore what are the supporting and opposing factors that may influence the outcome of the value assigning process. Subsequently, supporting factors may be manipulated to conceive compliance behaviour and opposing factors may be eliminated to reduce non-compliance attitudes. Consequently, the third objective has been specified as follows:

> ***To understand the factors that influence the stakeholders' 'perceptions of information value', which in turn effect their resultant 'information security behaviours.'***

Existing knowledge in the literature on factors that influence information security behaviours fall into the category of 'forced' interventions. For example, the provision of penalties to deter inappropriate behaviours, the allocation of rewards for exemplary behaviour, and the setup of a conducive environment to encourage a better information security compliance culture. What clearly arise from these examples is that all initiatives are forced and reactions are more non-voluntary than self-realisations. What is postulated for an effective and efficient information security culture is that the stakeholders pose a self-conscientiousness personality trait. From another perspective, all the decisions made by the stakeholders on their information security behaviour must be influenced and encouraged according to their inner sense of what is right, built on the sound principle of an understanding of the issues. In this regard, with or without the existence of rewards or penalties, despite less training and in conducive environments, the stakeholders still choose or adopt an acceptable level of information security compliance behaviours.

In order to achieve this third objective, it is important to explore various factors that are considered by the stakeholders to have significant impact on the information value assigning process. Upon learning and understanding these factors, it may be possible to link their significance as an "influencer" to the stakeholders' beliefs, attitude and behaviour. The findings of such nature would be priceless insights into how stakeholders' value their information and its protection. These insights then might be used as guidelines for developing better awareness, education and training to encourage better compliance with information security countermeasures. The factors under investigation will not only come

from the deduction made on the stakeholders'' interviews but will also come from the literature. The pre-conceived factors that are going to be explored in this research will be more fully discussed under the framework development section (section 3.5) of this chapter.

Although this research has an exploratory nature, it must be noted that the research is also largely guided by some orienting ideas from various existing theories that explain human behaviours in terms of adaptation to certain situations. As pointed out by Miles and Huberman (1994: p. 17) "*any researcher, no matter how unstructured or inductive, comes to fieldwork with some orienting ideas*

In recognition that this study is going to be a large wide ranging study and with a lot of ground to cover. Therefore, in order to ensure focus and high level of granularity it is essential to decompose the three substantive objectives mentioned above into several sub-objectives. These sub objectives are questions that help to define and achieve the main objectives so that through exploration of the issue can be done. The sub objectives will lead to a clear discovery or outcome that will correspond to the substantial objectives. In the context of this study RO1 has been decomposed into the following sub-objectives: -

i To explore whether 'perceptions of information value' vary from the perspective of different groups of stakeholders,

ii To understand the overall approaches by which stakeholders assign value to information, particular in relation to its protection and security.

One of the gaps, identified in the literature (Table 3.1) is the lack of studies on the mediating influence of stakeholders' perceptions of information value on their intention to behave towards information security countermeasures. These intentions may in turn influence and form their actual behaviour. Therefore, the second research objective RO2 has been decomposed into the following sub-objectives:

i To explore whether there is relationship between stakeholders' *'perceptions of 'information value'* and their resultant 'information security behaviours and the extent to which this is mediated through 'intention to comply';

ii To explore and understand how a stakeholders' *'perceptions of 'information value' is affected* by other stakeholders' existing information security behaviours.

iii To explore and understand how a stakeholder' 'perceptions of information value' is affected by the results of their own 'information security behaviours.

The next envisaged plausible relationship in the framework is the possible form of influence from various factors deems to be important by the stakeholders. The research will explore various factors that are thought to have significant influence to the process of Information Value assignment by the stakeholders. Section 3.4.5 presented the various dimensions of factors that are postulated to have significant impact on the stakeholders' information value assignment processes. The dimensions mentioned was also explored during a pilot study in which the result supports the need for exploration of the dimensions. It is expected that, on further exploration of these dimensions some of the factors may be proven to have little or no significant at all. Additionally, it is also expected that other factors may come up showing better influence on the information Value assignment during the interviews. Therefore, the exploration of the impacts of the identified dimensions of factors as well as exploration of new factors is the third objective of this research (RO3), and it has been decomposed into the following sub-objectives:

i To understand the factors that influence the stakeholders' perceptions of information value from an individual perspective.

ii To understand the factors that influence the stakeholders' perceptions of information value from the perspective of a work-group.

3.4 Framework Development

This section of the chapter will describe the development of the framework that has been developed to guide the research. The objective of this section is to clarify the key constructs and relationships that are to be the primary focus for this research. The section will start with an explanation of the emergence of interest in the concept of 'perceived value', in other fields of academic study, followed by a brief explanation on the topology of value from the perspective of the consumer, which is the basis of this research. Next the rationale behind the potential use of perceived value in the field of information security compliance behaviour is justified and lastly, this section will present the reasons behind the choice of dimensions used in the investigation of the role of 'perceived value' in the context of information security.

3.4.1 Perceived Value

In the field of marketing and commerce, the term 'perceived value' is typically used to denote the worth of a specific product or a particular service, as assigned by the customer. The consumer's perceived value of a product or service ultimately determines the amount he or she is willing to pay.

The conceptualisation of value in the marketing world begins with the most simplistic definition of value, i.e. "*consumer's overall assessment of the utility of a product based on perceptions of what is received and what is given*" (Zeithaml, 1998). According to Fernandez & Bonillo (2007), this view posits 'perceived value' as an unidimensional constructs or variables that can be measured simply by asking respondents to rate the value that they received in making their purchases. They further mentioned that although this view is simple, it fails to reflect the complexity of consumers' perceptions of value; particularly the failure to take into account of numerous intangible, intrinsic, and emotional factors that form part of the value construct. Other researchers such as (Milfelner et al. 2011 and Eid & El-gohary 2015) believe that "perceived value" is a multi-dimensional construct in which a variety of notions (such as perceived price, quality, benefits and sacrifices) are all embedded.

Researchers such as Babin & Attaway (2000) and Lee & Overby (2004) argue that users perceived value is a combination of both utilitarian and hedonic values. Utilitarian value is described as instrumental, task-related, rational, functional, cognitive, and a means to an end while the hedonic value is a value that reflects the entertainment and emotional worth of the products or goods non-instrumental, experiential and reflective (Babin et al., 1994). In their research, Lee & Overby (2004) identified the utilitarian value to include price savings, service excellence, time savings, and selection dimensions while experiential value includes entertainment visual, escape and interaction dimension.

Hartman (1967, 1973) posits that extrinsic value, intrinsic value, and systemic value from the axiological model of the notion of value. In his model, the *axiology theory*, Hartman defines *extrinsic value* as the utilitarian or instrumental use of a particular service, whereas *intrinsic value* represents the *emotional appreciation* of the consumption. The term 'systemic value' refers to the rational or logical aspects of the inherent relationships among concepts in their systematic interaction for example between *sacrifices and returns*. Mattsson (1991) translates the three value mentioned in the axiology theory as the emotional value which focuses on the feelings of the consumers, the practical value which focuses on the physical and functional aspects of consumption and the logical value which focuses on the rational and abstract characteristics of the purchase. In his other studies with Danaher (Danaher & Mattsson 1994), they measure cognitively based satisfaction during an actual service delivery process (in this case a hotel delivery process were modelled) demonstrated that the three values could have either positive or negative influence on satisfaction, thus become its antecedents. They believe that their study demonstrated the practicality of measuring cognitively derived satisfaction during an actual service delivery process. It is postulated that these value dimensions have a significant influence not only on the customers' satisfaction but also on a prediction whether the customer will make a repeat business or not.

Another perspective for looking at 'value', as a possible determinant of the multifaceted consumer choice making, is *the consumption theory* by Sheth et al. (1991). According to their consumption theory, values can be categorised into various forms such as functional, social, emotional, epistemic and conditional. *Functional* value pertains to whether a product can perform its functional, utilitarian or physical purposes. *Social value* refers to an image

that corresponds to the norms of a consumer's friends or associates and/or with the social image the consumer wishes to project. *Emotional value* is related to various affective states, which can be positive (for example, confidence or excitement) or negative (for example, fear or anger). *The epistemic value* is concerned with a desire for knowledge, whether intellectual curiosity or the seeking of novelty that motivates this. Finally, the *conditional value* reflects the fact that some market choices depends on the situation or set of circumstances faced by the consumers.

Table 3.2 Theories of Perceived Value

Theories	Axiology Theory Hartman (1967,1973)	Consumption Theory (Sheth et al., 1991)
Type of value	Extrinsic	Functional
	Intrinsic	Social
	Systemic	Emotional
		Epistemic
		Conditional

Consumption theory posits that: (i) the consumers' choice is influenced by multiple values; (ii) the contributions of the various values is subjective to the situation and the context; and (iii) these values are independent. Other works that usedconsumption theory in determining perceived value by consumer, such as the work of Sweeney & Soutar (2001), Sweeney et al. (1996) and Williams & Soutar (2000) rule out the significance of epistemic and conditional value. Werelds and Sandra streukens (2011) compared the performance of various value measurements and concluded that customer value should be operationalised in a multi-dimensional and consequence-based way, and that customer value is best assessed by means of the methods of Holbrook (1999). Sanchez-fernandez & Iniesta-Bonillo (2007) as an outcome of their review of the previously mentioned theories suggest that Holbrook's typology (1994,1999) presents the most comprehensive approach to the value

construct as it defines more sources of value than other studies. The Holbrook's typology of consumer value will be discussed in detail in the next section.

Reflecting back on the mentioned theories above, it is clear that the customers' perceptions about the value of a product or a service helps them to determine their intention and ultimately, probably their action whether to buy the product or subscribe to a service. From the perspective of information security, there are few interesting notions that can be further explored;

i. The potential for exploring and using the same notion of perceived value in the context of assigning a value to information in-place of products or services.
ii. Exploring both the extrinsic and intrinsic factors that may have an influence on value assignment on information; particular interest is on intrinsic factors as these may come internally from an individual rather than enforced externally. Factors such as these may have potential to encourage voluntary intentions that may translate into repetitive voluntary actions.

3.4.2 Perceived Value and Compliance

In the medical field, patient's understanding and satisfaction towards their medical procedure and prescription are seen as important predictors of their compliance with the medical procedures and processes ultimately subscribed to them. For a medical practitioner, the patient's compliance is a critical factor in the efficacy of medical treatments. The patient's satisfaction usually refers to a general satisfaction with the medical attention given (consultation or treatment). Compliance is the extent to which a person's behaviour (in terms of taking medication, following diets, or executing lifestyle changes) coincides with medical or health advice given by their medical advisor. In their study on compliance towards patient's oral care, Albrecht & Hoogstraten (1998) study shows a positive relation towards their satisfaction with their dental visits and compliance towards further treatment subscribed by their dentist. In many cases, if patients rate their initial visit as a satisfactory, they express their willingness to come back for regular check-ups or further treatments.

Another study by Smith et al. (1987) on the satisfaction of patients in their doctor-patient relationship and the way they communicate suggests that there are correlations between

patients' satisfaction and their concurrent compliance in taking their medication. Additionally, their study also suggests that satisfaction may also predict future compliance. Khalifa (2004) states that one of the advantages of creating value for customers, employees and investors is that it will reinforce the cycle of superior performance. Findings of researchers such as by Hesket et al. (1997) show the existence of direct and strong relationships between, amongst others profit; customer satisfaction; the value of goods and services delivered to customers; service quality and productivity; and employee capability, satisfaction, and loyalty.

Woodruff and Gardial (1996), in their customer value hierarchy method to understand customer value, conceptualised that the customer value is a trade-off between the positive and negative consequences of product use as perceived by the customers. They also highlighted that by focusing on value creation to a more specific consequences will result in a value that is more pronounced strategic sustainable and has a competitive advantage in nature. Sweeney & Soutar, (2001) highlighted in their study that, although the construct perceived value and satisfaction are easily confused, they are distinct. They argued that satisfaction could only be attained as a post action outcome, for example, satisfaction can only be expressed by post-purchase or post usage evaluation of product or services. One critical point that their study fails to realise is that upon attaining a level satisfaction; a user may re-appraise the value assigned earlier. This reappraisal potentially changes the perceived value of the product or services, according to the level of satisfaction. From this perspective, it is postulated that although perceived value and satisfaction constructs are distinct, they still have the possibility of influencing each other. The studies mentioned above suggest that satisfaction factors not only lead to higher assignment of value by customers, consumers or patients on the product, services or prescription they bought, subscribe or assigned to but subsequently the higher assignment of value will also encourage repeat sales, repeat subscription as well as compliance with treatment.

Therefore, conclusively what can be derived from the above are; firstly perceived value is constructed from evaluation process of varieties of value construct. Secondly value the construct can be either extrinsic (influence from outside/ external to the person), for example, rewards and penalties, environment setting and provision of training, etc. or value

constructs can also be of an intrinsic value which generates from within the individual, an emotional appreciation (Hartman 1967, 1973).

Furthermore, value constructs can also be classified by its orientation of initiation, which can be either self-oriented or other-oriented. These notions are also appreciated in the model 'typology of consumer value' by Holbrook (1996, 1994), although in his topology, Holbrook's definition of extrinsic include the appreciation of the functionality and the utilitarian, instrumentality in accomplishing some further purpose. The 'typology of consumer value' (Holbrook, 1994, 1996) is based on three dichotomy key dimensions of value; extrinsic versus Intrinsic, self-oriented versus other-oriented and active versus reactive. By treating each of the dimensions above as a dichotomy and combining them into a cross-classification, the framework produced eight "Typology of customer value, as shown in Table 3.3 below. The framework and typology have been used in many pieces of research that focus on the analysis of consumers' behaviour.

Table 3.3 Typology of Customer value

			Extrinsic		**Intrinsic**
Self-oriented	*Active*	ECONOMIC VALUE	EFFICIENCY (output/input, convenience)	HEDONIC VALUE	PLAY (fun)
	Reactive		EXCELLENCE (quality)		AESTHETICS (beauty)
Other-orientated	*Active*	SOCIAL VALUE	STATUS (Success, impression management)	ALTRUISTIC VALUE	ETHICS (virtue, justice, morality)
	Reactive		ESTEEM (Reputation, materialism, possessions)		SPIRITUALITY (Faith, ecstasy, rapture, sacredness, magic)

According to Holbrook (1994), the value has a different concept from values. He stated that "value refers to a preference judgement and values refer to the 'criteria' by which such judgements are made".

Holbrook's 'typology of customer value' is seen as the most comprehensive approach to value construct because it captures more potential sources of value than other conceptualisations (Sánchez et al. 2008; Gallarza & Saura 2006). Despite held as a comprehensive approach, Holbrook typology has some limitations. It was found out that the status and esteem dimensions of the topology have very subtle differences (Brown 1999, Wagner 1999) and Holbrook (2006) conceded that categories of ethics and spirituality are closely related. Therefore, the status and esteem dimensions have been combined under the heading 'social value' while ethics and spirituality dimensions have been combined and renamed 'Altruistic value' (Sánchez et al. 2008).

Following this modification to the topology, Sánchez et al. (2008) proposed a modified model for the structure of consumer value (figure 3.2).

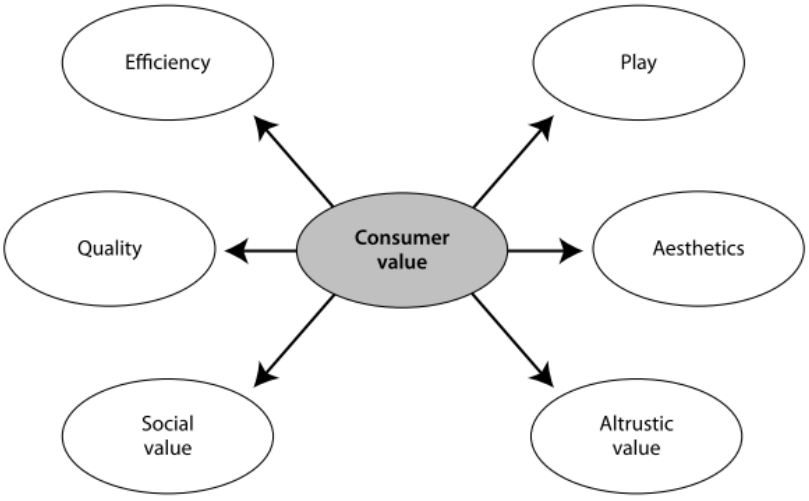


Figure 3.1 proposed model for the structure of consumer value (Sánchez et al. 2008)

The next section presents the discussion on the notion of using 'Perceived value' in the context of information security and information security countermeasures compliance by stakeholders. First, the similarity of the concept is discussed which is then followed by a discussion on how it will be implemented from the perspective of information security.

3.4.3 Perceived value in the context of Information Security Compliance

Gallarza et al. (2011) have identified several potential sources of importance that help explain the reasons why the concept of value is crucial to the marketing community. Two of the reasons outlined are seen to have similar potential importance in understanding and improving information security compliance. Firstly, in the marketing field, the concept of consumer value is inextricably linked to the major marketing-related constructs such as perceived price, service quality, or customer satisfaction. This indicates that with the creation of value and the improvement of value, the possibility of improving customer's satisfaction is enhanced. Clearly this can be viewed as a link to information security compliance, in term of creating value around information and information protection so that the user can appreciate them more. It is envisaged that once the users appreciate their information and the protection mechanism, they are more willing to comply with procedures and policies that come with them.

Secondly, the value construct helps to explain different facets of consumer behaviour that occur both before and after the purchase itself. These different facets include; purchase intention, product selection, brand choice and repeat purchase. Furthermore, Gallarza et al. (2011) suggest that the concept of value is newly understood and is significant to customer's relationship marketing. In fact, the Relationship Marketing stresses the importance of understanding affective commitment (Pura 2005) and repeat-purchase or re-patronage (Petrick 2003) intention from the perspective of value concept. Dick & Basu (1994) made a point that these two perspectives are significant to a comprehensive understanding of loyalty behaviour. Furthermore, other studies by Oh (2003) and Grace & O'Cass (2005) further suggest that perceived value is a positive influence on customers' loyalty to a product or a service. The second reason outlined by Gallarza et al. (2011) is foreseen to have a significant contribution to understanding user compliance behaviour with information security countermeasures, thus warrant further exploration. Re-patronage or repeat purchase, brand loyalty and commitment to product or services are all the value sought for in information security, in terms of compliance. The values mentioned above are believed to emerge from basic customer satisfaction. Satisfaction has been studied in the context of information security and has been suggested that user satisfaction with a system in meeting

their requirements and needs have significant influence on user's willingness to use and repeat usage of the system (Ives et al. 1983). These similarities, furthermore, increase the potential of using information 'perceived value' as influential constructs in mediating user compliance intention and behaviour in the context of information security.

The discussion above can be concluded to support three main points. The first point is that *"if the user is satisfied with a specific product or service, it is most likely that the user will associate a higher value to that specific product or services".* Value in this regard is expressed according to the user appreciation and satisfaction of the product or services he/she gets in return of what he/she exchanges for it. The next point is that, *"The higher the value associated with the product or services, the higher the possibility of the user to appreciate the system, procedure or process associated with the product or services".* Due to the realisation of the value of the product or services, it is more likely to be appreciated or treasured. The third point is that, "*users' satisfaction with products or services that they have acquired encourages repeat purchase or subscriptions and thus helps build customer loyalty'*.

This research will apply Morris B. Holbrook (1996) value creation framework and Sánchez et al. (2008) consumer model as the basis for exploring the views of stakeholders on information value in relation to their information security compliance behaviour. Specifically, the studies will concentrate on the value creating processes experienced by users in association with some of the value creation constructs highlighted in Holbrook's framework and Sanchez's model. It is important at this juncture to however highlight that although all the dimensions mentioned in Holbrook's and Sanchez's were found to have significant impacts in their studies of users' purchasing and loyalty behaviour, not all of them are seen to contribute similarly in this research. Therefore, in this regard some of the dimensions are dropped for this research. The rationale for this move is presented in the next section.

It is envisaged that by firstly, understanding what value are important to users and how users construct these value of the information assets they are dealing and secondly, understanding and exploring instances of users' construction of value in their appreciation of information protection mechanism, new influencing dimensions will be identified. These dimensions can then be worked to encourage better compliance.

3.4.4 Significant Dimensions of 'perceived value' in information security

One of the unique strategies taken by this research is to make use of the evidence in the field of marketing to investigate the impact of the similar initiative in the context of information security. Table 3.4 below outlines the difference between the approach in the marketing field and how it is going to be used in this research.

Table 3.4 A contrast of strategies of using 'perceived value' in marketing and information security

Field	Strategy	Variables on product or services	Target	Outcomes
Marketing	Creation of value for product and services	Perceived price Perceived quality Perceived usefulness	Consumer Satisfaction	Improved consumer buying intentions Possibility of repeat buys Establishing loyalty
Information Security	Assignment of value to information and information security countermeasures	Perceived Value (Information Value); Importance of information, Sensitivity of information	Users or Stakeholders' appreciation	Improved stakeholders' intention to comply to countermeasures Possibility of repetitive (voluntary) usage of countermeasures Establish loyalty to organisation

To start with, the strategy used in the marketing field concerns the processes of creating value and assigning value either on product or services, whereas, the postulated use of this strategy in the information security area would be the creation of value and assignment of value on information. Subsequently, the value assigned would develop an appreciation for that information as well as the information security countermeasures in place. Regarding the consumer satisfaction, which is the main target of the marketing strategy, the information security strategy will aim at developing stakeholders' appreciation of the information they are handling.

The dimensions or variables that are being investigated in the information security strategy will focus on three areas; the construction of perceived value or assignment of value, the realisation of the importance of the information both to the individual and organisation, and the consideration of the sensitivity of the information and its implication.

Table 3.5 Dimensions of value selected in this research

Holbrook's Model (Morris B. Holbrook 1994)	**Sanchez's Model (Sánchez et al. 2008)**	**This research**
Excellence	Quality	Information Importance
Efficiency	Efficiency	Information Sensitivity
Status	Social	Social (normative beliefs & subjective norm)
Esteem		
Ethic	Altruistic	Ethic (Customs) / Culture
Spirituality		Spirituality
Play	Play	N/A
Aesthetics	Aesthetics	N/A

Through learning and understanding of users or stakeholders' value creation or assignment processes and identifying instances of these processes that are significant to their appreciation of both the information they are handling as well as the information security countermeasures, it is anticipated that this knowledge will help in improving stakeholders' intention to comply to information security countermeasures, encourage repetitive voluntary usage and establish loyalty to the organisation.

As mentioned in the previous section, this study will not consider all the dimensions or variables suggested by the Holbrook's and Sanchez model. The dimensions selected for this study are identified in Table 3.5 above, and the rationale for the adoption or rejection of the dimensions is presented in the following section.

3.4.4.1 Information importance

Holbrook (1999) describes excellence as 'a reactive appreciation of an object's or experiences potential ability to accomplish some goal or to perform some function'. Sánchez et al. (2008) consider that Holbrook's description include some utilitarian emphasis thus relate it to the concept of 'quality'. In many studies, perceived quality is seen as an antecedent that has a positive effect on perceived value (e.g. Cronin et al. 2000; Baker et al. 2002; Chen & Dubinsky 2003; Tam 2004), whereas others have contended that quality is a sub-category of overall value (Sheth et al. 1991; Holbrook 1994; Sweeney & Soutar 2001).

In the context of this research, Holbrook's definition of excellence relates more to the objective that is exploring the potential of value construction on information from the perspective of its appreciation of the information potential ability to assist in accomplishing tasks and achieve goals in an organisational setting. This perception suggests that the sense of how important the information assist in completing one's tasks will, in turn, increase the appreciation towards the information thus equally improves the value of the information.

3.4.4.2 Sensitivity of information

The sensitivity of information has been proven to have significant impacts on how much one is willing to disclose information. The more sensitive the information according to the individual, the less willing they are to disclose that information (Rifon and Choi, 2005). Mothersbaugh et al. (2011) suggest that the failure to account for information sensitivity plays an important role in understanding information disclosure. Failure to consider the correct information sensitivity hinders progress in developing strategies to obtain sensitive information online or to adapt information requests to match the situation. Furthermore, according to (Cranor et al., 1999) sensitive information is perceived as riskier and more uncomfortable to reveal.

One of the risks of this notion is that an individual may have an incorrect perception of the sensitivity of the information. As stated by (Adams and Sasse, 1999), a complex interaction between users' perceptions of organisational security and information sensitivity was identified. Users identified certain systems as worthy of secure password practices while others were perceived as "not important enough." Without any feedback from the

organisation, users rated the confidential information about individuals (personal files, email) as sensitive, but commercially sensitive information (such as customer databases and financial data) was often seen as less sensitive. Some users stated that they appreciated printed document classifications (for example, Confidential, Not for Circulation), indicating their need for information sensitivity guidance and rules for levels of protection in the online documentation.

In the context of this research, the assignment of value according to the sensitivity of the information from the perspectives of its users or holders is important in the sense that it has an influencing factor on how much people are willing to protect the information. This is clearly defined by the empirical evidence from the researchers' findings mentioned above. To explore this notion in the field of information security is therefore also a matter of importance.

3.4.4.3 Social Value

Sánchez et al. (2008) suggest that in the marketing field, a social value is seen as a significant dimension in determining customers purchasing behaviour. In this regard, social value is defined as "*the active manipulation of one's consumption to make a favourable impression on others (status via exhibitionism) and a reactive appreciation of the prestige associated with one's possessions (esteem linked to materialism)".* Relating these assumptions to the field of information security, the main argument is to explore and understand this from the perspective of the stakeholders' normative beliefs that subsequently will determine how they perceived the social pressure on them whether to engage or not to engage in a specific behaviour. Normative beliefs refer to how stakeholders perceived important others' expectation of their behaviour towards a certain issue. In the context of information security, it is how stakeholders think their important others react or behave towards information security countermeasures. Although 'important others' generally refers people closely link to the stakeholders, for example, their work colleague, subordinates and supervisors in a closely knitted community such as Brunei Darussalam and the expectation of family ties overlaps with organisational structure, the important others may also include their spouse, family, friends and even the community.

3.4.4.4 Customs, Culture and Spirituality

In a country rich with its heritage customs and where culture is embedded in daily life, it is inevitable to expect that these customs and culture may have some impacts on how people decide to behave. To what extent customs and culture may impact information security compliance behaviour, and to establish what kind of customs and culture have the most significant impacts should make an interesting finding. Moreover, the contributions of such understanding would be beneficial to organisations to deal with how to address issues of non-compliance. Existing literature also suggests that organisational culture may be influenced by the nation's culture and customs.

Sánchez et al. (2008) framework combined what Holbrooks described as the dimension of ethic and spirituality into a single dimension namely altruistic value. Sanchez pointed out that altruistic value is described by the behaviour that displays unselfish concern for the welfare of others; selflessness. In the context of this research, the dimension of spirituality is more of interest as spiritual is closely link to the Bruneian's customs. Despite that, the dimension of ethic is not rejected wholly, as it is believed that the communal ethic in many countries in the South East Asia including Brunei Darussalam are also widely influenced or driven by their religion. Particularly, in the context of Brunei Darussalam, the religion of Islam has been its official religion since a long time ago. Thus, ethics on many issues is mainly formed by the teaching of the religion.

This makes the variable 'spirituality' an important variable to be investigated regarding its potential impacts in influencing the decision of individuals when they are faced with information security compliance issues.

3.5 Research Model

Following the analysis of the potential dimensions of 'Perceived Value' presented in the previous section (Section 3.4.4), an initial research model was developed that reflects both the multi-faceted nature of information value and the key groups of stakeholders who assign it. The aim of this model is to represent the ideas as an alternative approach towards understanding the formation of information value and adoption of information security compliance behaviour with respect of information security countermeasures. The model has been derived from both the prior discussion from this section and several theoretical views (discussed in chapter 2) on the issues of information security and compliance to information security countermeasures have also been taken into consideration.

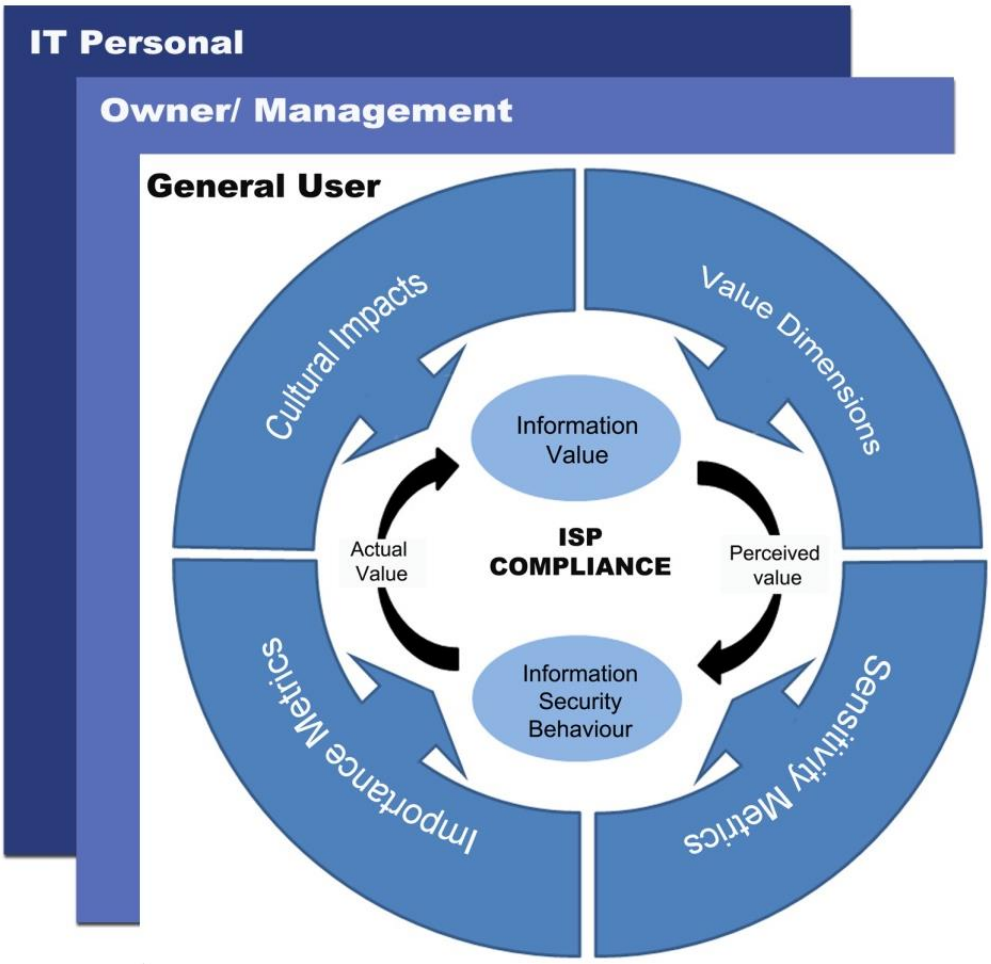


Figure 3.2 the initial research model

The research model (Figure 3.2) was used to develop a richer and more complete understanding of how stakeholders understand the value of information, which might ultimately affect their compliance behaviours with respect to information security countermeasures. The model describes the postulated relationships between stakeholders' behaviour with information security countermeasures as a result of value assigning process by the stakeholders on information. Particular interest is towards the compliance with information security policies (ISP).

The model comprises of three main components;

- The inner circle which represents the cycle of information valuation and information appreciation process by stakeholders.
- The outer circle which denotes four dimensions that are postulated to have significant influence on the information valuation and appreciation process and;
- the outer square tabs which represent the three different level of stakeholders who are significantly involved in the information security process.

The model can best be interpreted by beginning from the outer square tabs, and then moving inwards. The three level tabs represent the various level of stakeholders (Albrechtsen, 2007). It is expected that these stakeholders will have different views on the value they assign to specific types of information. For this, every stakeholder will go through a similar process of information evaluation and value assignment (the inner circles).

The *inner circles* portray the process of the formation of stakeholders' information security behaviours around information and how it may influence the value of that information. It is assumed that the process of information security behaviour begins with the stakeholder already having or assigning a value to the information resources that they are handling. At this point, the value is based on the stakeholder's assessments of existing situation, surrounding and knowledge. The assessment results in a perceived value of the information or the "information perceived value" and it is postulated that this value may help in determining the level of information security behaviour to be adopted by the stakeholders.

Gradually, the information security behaviour adopted by the stakeholders may become an indication and suggests how the information should be valued. In time the perceived information value may progress to become the actual value of the information. A value derived from the subjective assessments by individuals that have become acceptable to the group of people or the community in which the information is located (for example in a department, a unit or an organisation).

The inner circle's process is further predicted to may be significantly influenced by four major variables that form the outer circles of the model. The justification for focusing on these four variables is presented in the previous section, section 3.4.4.

This model raises numerous issues regarding the relationships between its various components and its overall efficacy in predicting stakeholder behaviour. Consequently, it is important to test this model to understand the process by which stakeholders perceive information value and how the perceived information value can influence and affect their decisions with regard to security counter-measures. It will be of particular interest to explore the 'mediating' relationship of stakeholders' perceived value of information with information security compliance, as it is postulated that stakeholders' actual behaviour towards information security compliance may significantly impact the value of information.

It is believed that stakeholder's perceived value of information will have a significant impact on how they choose whether to comply or not with the information security countermeasures instigated to protect that information. These assumptions further help to postulate that the higher the value of information is perceived, the better the likelihood of compliance with information security countermeasures. Conversely a better compliance by stakeholders may have an impact on the perceived value of the information.

3.7 Concluding Remarks

This chapter has attempted to provide insights and justifications on the identified research gaps, objectives of the research as well as detailing the conceptual framework for the research. Prior to the presentation of the conceptual framework, the development of the framework was presented. The presentation of the development of the framework shows how the dimensions used to investigate the phenomena were constructed. The basis of the theories that were used as the lenses to figure out and developed the framework was also briefly discussed.

The final discussion of the chapter introduces the initial investigative model. The initial and subsequent qualitative investigations (interviews and focus groups) were based on this investigative model. In a way this chapter discusses and outline the frameworks and the foundation that guides the development of the research.

4. METHODOLOGY

4.1 Introduction

This research is driven by questions of what, how and why that surrounds the need to better understand the information security compliance behaviour of various stakeholders in public organisations. This chapter presents the rationale for approaching the research from the chosen philosophical perspective, along with justification for undertaking the strategies of inquiry adopted. This chapter also addresses the research methods used for data collection and analysis. It concludes with a discussion of reliability, validity and ethics concerning this research.

4.2 The research philosophy

There are varying views of how research should be carried out and how it relates to the kind of knowledge being developed. A paradigm is needed to guide how decisions are made and how the research will be carried out (Guba, 1990). This enforces Kuhn's justification of a paradigm that consists of 'some *accepted examples of actual scientific practice….. [that] provide models from which spring particular coherent traditions of scientific research*' (Khun, 1996). Guba & Lincoln (1994) defined a particular set of rules and standards for practice. These rules and standards are characterised as axioms; which define the ontological, epistemological and methodological bases for different paradigms. It is important for this research particularly, to be guided by a set of assumptions on its philosophical standing. As mentioned by (Creswell, 2012), having clear philosophical assumptions help to shape how a researcher formulate the problem under study and research questions to study and how information is sought to answer the questions.

The assumptions and views on how research should be conducted may influence a research process, therefore, an epistemological consideration in research is central to the framing of the research questions and the choice of methodology according to (Bryman, 2012). One assumption would be from a scientific perspective, in which it is believed that a hypothesis should be formulated and be tested using specific measurement technique (Bryman, 2012). Another assumption, which does not totally in sync with the scientific idea, has the

perception that a more sensitive approach to addressing special qualities of people and their social institutions should be taken (Bryman, 2012; Creswell, 2012). These assumptions of how a phenomenon should be studied are called epistemological assumptions. The former assumption is known as a positivist approach while the latter is known as an interpretivist approach, which is the approach that is adopted for this research. Depending on which stands that a researcher decides to adopt will affect the way in which the study will question. Creswell (2009) argued that researchers could not be positivistic about the claims of knowledge when studying the behaviours and actions of a human. Creswell (2009, p.7) explained:

Developing numeric measures of observations and studying the behaviour of individuals becomes paramount for a post-positivist […] the accepted approach to research by post-positivists, an individual begins with a theory, collects data that either supports or refutes the theory, and then make necessary revisions before additional test are conducted.

Furthermore, a positivist assumption is greatly related to a quantifiable outcome. This assumption does not relate to the objectives of the research, which aims to interpret and represent a subjective argument into the phenomenon of information security compliance behaviour.

Another important assumption that is as important to be considered is the assumption on the nature of the social phenomena, which is known as ontological assumptions. Ontological assumptions are how social issues are seen respective to the social actors. One perspective of such assumptions is an objectivist position in which the social actors and the social issues are seen as separate entities and that the social issues are objective and have a reality external to the social actors (Bryman, 2012). Meanwhile, another perspective on these assumptions argues that social issues are social constructions resulting from the action and perception of social actors. This kind of assumption is known as constructionism or a constructivist assumption.

For this research, it is believed that the social actors play great roles in the formulation of the phenomena in the study. Therefore to understand the phenomena, it is important to be able to appreciate the interpretations by the participants (social actors) on their subjective

social actions. This adaptation is also in appreciation of (Bryman, 2011) suggestion that subject matters in social research have a different nature from natural sciences'. Ontologically, for this research it is believed that the social actors play an important role in defining and constructing the phenomena in the study. Therefore, it is important to understand adequately the different constructs attained by social actors particularly from the interactions between individuals. Since the research questions are instigative in nature, it helps to define the stance taken by the researcher as an interpretivist-constructivist approach.

This approach takes into consideration the view of an interpretivist/constructivist as mentioned by (Thomas 2009); Knowledge is everywhere and is socially constructed, all kinds of information are valid and worthy of the name 'knowledge' even 'things of the mind', specific accounts inform each other and the act of trying to know should be conducted such that the knower's value position is taken into account in the process. Creswell (2003) defines that the interpretivist/constructivist researcher tends to rely upon the "participants' views of the situation being studied" although at the same time recognises the impact of the research on their background and experiences. Again in (Creswell, 2012) the same position is described as social constructivism. The core of such position is to develop subjective meanings of participants' experiences with the goal to rely as much as possible on the participants' view of the situation.

Additionally, the researcher felt that his role as a researcher also includes; to understand and interpret the situation, has the duty to partially create the meaning of the phenomenon, realising that a pre-understanding of the phenomena and issues is also important and that he has to accept influences both from the science of nature (existing theory) as well as personal experiences in the field of the research.

4.3 Research Approaches

There are two main approaches to research; deductive and inductive. A deductive approach starts with a predefined theory, in which a theoretical proposition is tested through a selected research strategy, for example, empirical scrutiny (Bryman, 2012). A top-down approach to induction process starts with observation and interpretation of the phenomena under study through the lens of the participants and ends with the development of a theory of the construction and explanations that arise.

Although it is typical for research to adapt a singular approach, it is not uncommon for the researchers to combine both approaches in their researches. Combined approach complements the research questions by allowing the tenets of social phenomenology to be integral to the deductive process while still allowing for themes to emerge directly from the data using the inductive process (Fereday and Muir-Cochrane, 2006).

Due to the nature of the phenomenon under study possess both the possibility of deducing from existing theories as well as the opportunity to further understand the issues through the lens of the participants in the field, the author has taken the stance of approaching the research using the combined approaches of both inductive and deductive (figure 4.1).

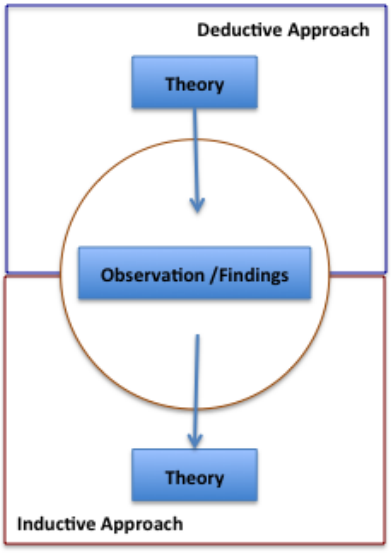


Figure 4.1-mixed approach of deductive and inductive

4.4 Research Strategy and Design

Reading through the research literature one would come across different classifications and definitions of terms used. For example the research methodology model put forward by (Saunders and Tosey, 2013), classifies research strategies as consisting of techniques used to answer the research questions. Meanwhile in (Bryman, 2012) classifies the techniques presented by (Saunders and Tosey, 2013) are either classified as research strategy or research design. Other researchers such as (Creswell, 2009) use the term strategies of inquiry and research methodologies is used by (Mertens, 1998). Due to this multiple classifications, therefore, for this research, the classification put forward by (Bryman, 2010) is preferred as it provides an unambiguous overall framework for the complete research process.

So in reference to (Bryman, 2012), research strategy is a general orientation to the conduct of social research. For this (Bryman, 2012), outlined qualitative, quantitative and mixed methods research that is the combination of both qualitative and quantitative strategies. The choice between any of the strategies outlined is much related to the objectives of the research and the philosophical view of the researcher.

4.4.1 A Qualitative strategy

With the reference to the objectives of the research and the stands of a philosophical view taken for this research it is just appropriate for this research to adopt a qualitative strategy. There are several reasons to justify this decision; these reasons are in line with the characteristics for adopting a qualitative strategy highlighted by (Bryman, 2012; Creswell, 2012; Crotty, 1998).

To start with, from an epistemological view, this research adopts the interpretative view in which the emphasis is on the words of the participants rather than the quantification of the data collected. This epistemological adaptation directly rejects the practices and norms of natural science and positivism, which rests towards the use of quantitative strategy. Similarly, the ontological view adopted by this research points towards a qualitative strategy.

One of the characteristics of qualitative strategy highlighted by (Bryman, 2012; Creswell, 2012; Crotty, 1998) that is not of an agreement with this research is the view on the research adopted in this research is the approach. It has been argued (Bryman, 2012; Creswell, 2012; Crotty, 1998) that a qualitative research strategy is particularly suitable for research studies which adopt an inductive approach. However, for the reasons presented in section 4.3, it can be argued that a qualitative approach is equally suitable when adopting a mixed of inductive and deductive approach, such as that being employed in this study.

4.4.2 A pragmatic approach

The research methods and instruments for this research are determined by the nature of the research questions and the objectives of the research, which indicate a pragmatic view of research. In a pragmatic research study, the researcher first focuses on the research problem, and then uses whatever approaches might be helpful in understanding this problem (Creswell, 2009). Researchers like Holmes (1992) and Rossman and Wilson (1985) have also noted that a pragmatic approach is one that focuses on the research problem, rather than methods, and uses a range of approaches available to understand the problem. Furthermore, Creswell (2009) outlined the key philosophical assumptions for pragmatic research, upon which this research was based:

1. Individual researchers are free to choose the methods, techniques, and procedures of research that best meet their needs and purposes.
2. Pragmatists do not see the world as an absolute unity.
3. The truth is what works at the time.
4. The pragmatist researchers look to the "*what* and *how"* to research, based on the intended consequences – where they want to go with it.
5. Pragmatists agree that research always occurs in social, historical, political, and other contexts.
6. Pragmatists have believed in an external world independent of the mind as well as that lodged in the mind.
7. Pragmatism opens the door to multiple methods, different worldviews, and different assumptions, as well as different forms of data collection and analysis.

In relation to this research the above points are all valid. Particularly, with the uncertainty and subjectivity of the phenomena under investigation points number 5 and 6 explain why a pragmatic approach is most suitable. This research also practices the key philosophical assumptions number 7 in which various data collection approach are used. More importantly, various assumptions were also made (Chapter 3). Therefore, the design of this research is taking into consideration the philosophical assumptions listed above.

4.4.3 Qualitative survey

Often the term 'survey' is used as shorthand for statistical surveys, as many researchers automatically equate it to the use of a 'questionnaire' as a tool for data gathering. Therefore, research, which involves a survey, is typically associated with quantitative research.

Although it remains far less visible, within the methodical literature (Jansen, 2010), surveys can also be usefully employed in qualitative research studies. In qualitative research, survey studies describe the diversity of certain cognitions or behaviours in a population using semi-structured interviews with a small sample of population members (Jansen, 2010). This is distinctive from the typical statistical survey, which, analyse frequencies in member characteristics in a population. The main keyword here is between frequencies and diversity. What this research is interested in is the presentation or interpretation of the phenomenon understudy by the stakeholder of the issues under investigation. Therefore, identifying and understanding the diversity of perspective on the problem is the core of the research. This research adopts a qualitative survey as an approach to study the field of interest.

The methods, techniques and procedures were selected based on their helpfulness in understanding the problems under study. The next section presents the research design and methods planned for this research.

4.5 Research Methodology

A Research methodology outlines the techniques to be used for the collection and analysis of research data. This section will provide a discussion on how data for the research were sampled and gathered. An overview of the research strategy is presented in Figure 4.2, and its key features are more fully discussed in the sections that follow.

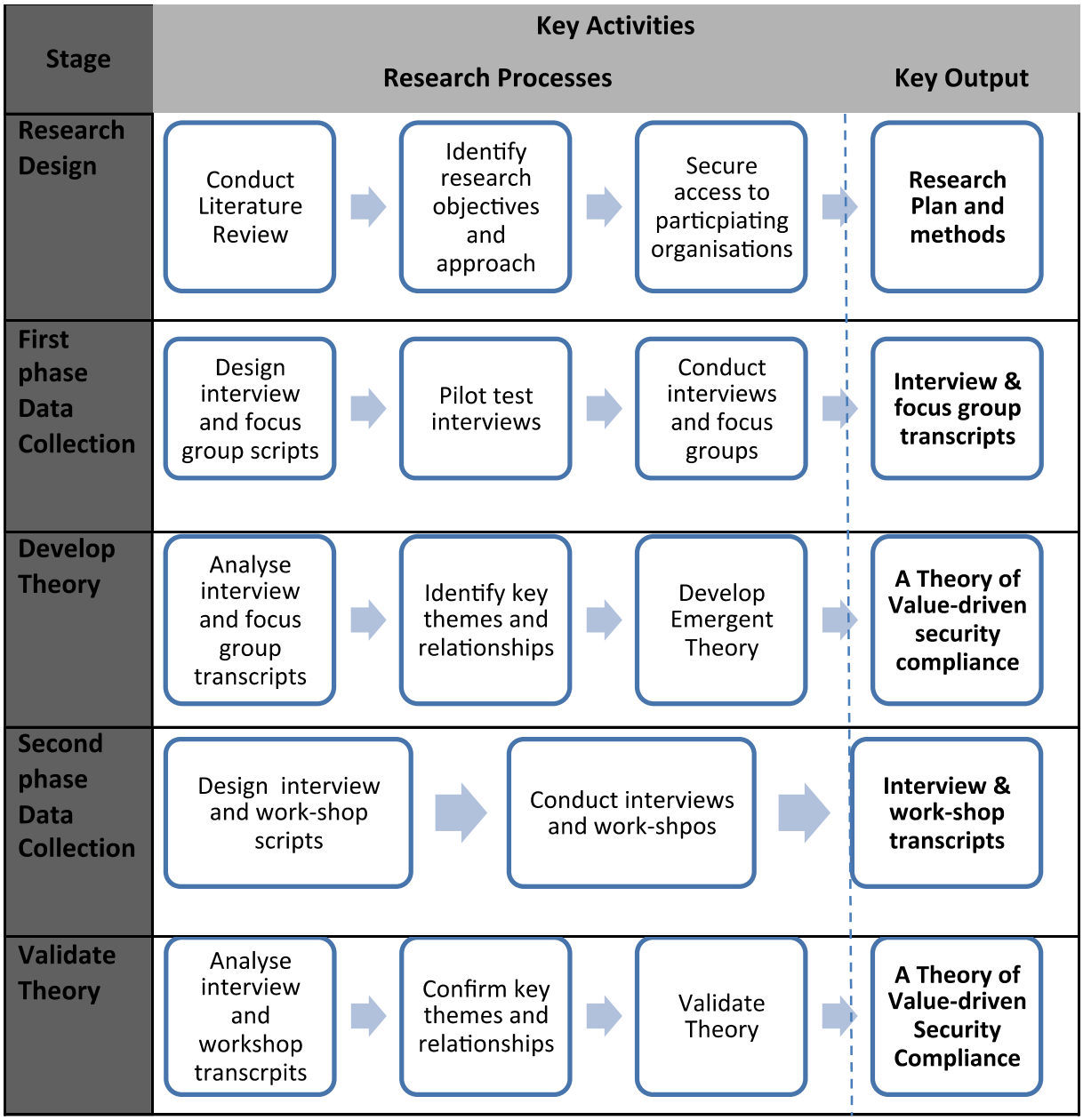


Figure 4.2 An Overview of the Research Approach and Methods

During the first phase, the primary data collection instrument was the semi-structured interview, which allowed the researcher to consult a wide variety of stakeholders. An interview guide was constructed, which included a number of common questions, as well as some more general prompts, which encouraged respondents to share their own experiences and perceptions about a broader area of interest, in their own words. Moreover, to help focus the interviewees' thoughts, a number of scenarios were included in the script, as these have been found to '*stimulate purposeful discussion*' (Kim, 2012, 305). Prior to its use, the interview script was piloted tested on five experienced computer users, and a number of adjustments were made prior to the commencement of the first phase data collection. The interviews were either tape-recorded or detailed notes were recorded, depending upon each interviewee's preference. Ultimately, a total of 42 face-to-face interviews were carried out for the first stage. Of these, 37 interviews were audio recorded while detailed notes were hand-written for the other five, as they were reluctant to have their interviewees recorded. To provide a broader perspective, and to triangulate the findings, focus groups were also used. More specifically, in the first phase four focus groups were used, each comprising a mix of stakeholders, in an exploratory manner to gain insights into the information value assignment process and its relationship with security compliance.

Next, the critical element of the theory development process was the conduct of a rigorous analysis of the significant quantities of qualitative data that had been collected. Consequently, the interview and focus group transcriptions were imported in a rich text format to NVIVO, which facilitated their coding and annotation, using '*in vivo codes*' and '*marginal remarks*' (Miles and Huberman, 2013). The underpinning philosophy of the analysis strategy was one of dialectic hermeneutics, whereby the researcher's: '*understanding of the whole has to be continually revised in view of the reinterpretation of the parts*' (Myers, 1994; 56). The researchers would keep re-visiting their interview transcripts and other documentary evidence, and where necessary initiate follow-up phone-based interviews, to help integrate the individual pieces of evidence into a coherent whole (Butler, 1998). The end product of this analytical process was an emergent theory of *value-driven security compliance*.

During the first phase interviews, all interviewees were asked if they are willing to participate in further activities, and ultimately a total of nine follow-up interviews were conducted. Moreover, a further four participants, who had not been able to participate in the earlier interviews were recruited, giving a total of thirteen second phase interviews. In addition to being used to clarify issues and fill in gaps in the understanding of the issues, these interviews also proved to be an ideal opportunity for canvassing participants' feedback on the emergent theoretical model. In a similar vein, a total of three confirmatory focus groups were conducted, each comprising between 5 and 7 individuals, to seek the groups' feedback on the theoretical model. For this exercise the focus groups were differentiated by employee type, so that we could determine whether the model made sense, from the perspective of a group of computer users, a cluster of IT professional and a group of more senior managers. Details of the lists of all interviews and focus groups are attached with this thesis as appendix F and appendix G respectively.

As with the theory development process, the point of departure for the theory validation process was an analysis of the qualitative data that had been collected, through the preceding data collection initiative. The overarching aim of this validation process was to sense check (Alvesson, & Kärreman, 2007) our emergent theory, to ensure that it was credible, in the context of the interviewees and focus group members' experience of information security compliance.

4.5.1 Data Sampling

The main focal point for the data collection exercise was Brunei Darussalam, which being a developing country is relatively under researched, and it was anticipated that it would therefore act as a good example for other developing countries (Henninger, 2013).Brunei Darussalam is a small country with the land area of 5765 km2, situated on the north-western coast of the island of Borneo. It shares the island with the Malaysian states of Sabah and Sarawak, as well as the Indonesian province of Kalimantan. The country's small population of 423,000 people (Gov.bn, 2016) comprises a mixture of several ethnic groups with a Malay majority. Governance in Brunei conforms closely to the Middle Eastern pattern of dynastic monarchy, with the exception that Brunei has wrapped itself in the cloak of

'mono-culturalism' (Yapa, 2014) that is Malay Islam Beraja (MIB). The system of government in Brunei is an Islamic monarchy, in which Islam makes up the economic, legal, political, civil, cultural and social fabric of the country. In running the government, the Sultan is assisted by 12 ministries and 101 government departments and agencies. The dependence of the Brunei economy on oil and gas resources has led to a larger government sector, which limited the role of the private sector.

Having decided to focus upon Brunei Darussalam, the next decision was which sector or sectors to target. Ultimately, public sector organisations were chosen as the sampling domain, as the researcher had particular good access to such organisations. Perhaps more importantly, as information is a key asset to such government agencies, its appropriate handling is vital to the safe and effective delivery of public services (Yang & Maxwell, 2011). Departments and agencies need to be confident that their information assets are safely and securely stored, processed, transmitted and destroyed, whether managed within the organisation or by delivery partners and suppliers [Burden, 2009]. Equally, government have a legal obligation and duty to safeguard personal data entrusted to them by their citizens and businesses (Kim et al, 2014). In striking the right balance between enabling public services and sharing and protecting data, public sector organisations must assess and manage the risks to the services they provide and to the confidentiality, integrity and availability of the information assets they are formally responsible for (Khatri & Brown, 2010). Whether organisational information be located in the private or public sectors, there is a growing recognition that, as an increasingly valuable resource, it will need to be protected from theft and unauthorised access by people who are not its intended users (Kayworth & Whitten, 2010), and the key mechanism in this respect is the information security policy.

The fact that more than half of the work force in Brunei Darussalam is in the public sector, made it possible to make use of snowball sampling and convenience sampling techniques (Bryman, 2012). The initial contact for the recruitment of participants was Brunei's E-government National Centre (EGNC) and gradually, after the revision of the sampling requirements, invitations for participation in the research was extended to various other

government ministries and institutions. The participants were mostly recruited with assistant from Brunei e-government Centre (EGNC), a government institution that looks after all Brunei's e-government initiatives and it is also presumed by the public as an institution that looks after information security initiatives. The reason for the engagement with EGNC was for the convenient in accessing participants for the study. EGNC staffs are seconded to every government ministries under different departments and units as IT support staff. Since they are position in the various ministries, they were able to assist in recruiting the required participants. Some of the participants were also recruited from lists of friends and personal contacts that work in the public sector.

At this stage of the research, the interest is to understand the variations of representation on various variables i.e. perceived value, value assignment process and the factors that may influence the stakeholders' perception and information evaluation. These variables will be explored from the perspectives of different level of stakeholders in an organisation as well as across organisations.

The researcher managed to recruit participants from 10 ministries of the total 12 government ministries in Brunei Darussalam. Two ministries namely ministry of Industry and permanent resources and the ministry for religious affairs was not represented in the first phase interviews. The participants cover the three categories of the stakeholders' level; people in the management, personnel from Information technology or information security and normal users, which was intended for the research. When it came to the number and types of individuals that were ultimately involved in the study, it was decided to target a wide and diverse range of individuals, as this leads to a better and richer understanding of the research phenomenon (Corbin et al, 2008).

Table 4.0 Ministries that was represented in the first interviews

Name of Ministry
Ministry of Education
Ministry of Affairs
Ministry of Foreign Affairs

Ministry of Development
Ministry of Communication
Ministry Health
Ministry in Defence
Ministry of Finance
Ministry of Youth and Sports
Ministry of Home Affairs

Additionally, a convenience sampling method was also used to recruit some of the participants from the researcher's list of friends and family members who are working in the public sector. According to (Bryman, 2012), a convenience sample is the one that is easily available to the researcher by virtue of its accessibility. The samples participate in interviews, focus groups and workshops. These methods of data collecting are the focus of discussion in the next section.

4.5.2 Interviews

The interview is a purposeful discussion between two or more people (Khan and Cannell, 1957). Interviews are used to gather valid and reliable data that are relevant to the research questions and objectives (Saunders et al., 2003) and it is the most widely employed method in qualitative research (Bryman, 2012).

Leading authors in the methodological literature classifies interviews to fall into three main categories; the structured interview, semi-structured interview and unstructured interview (Bryman, 2012; Creswell, 2012; Saunders et al., 2003). A structured interview also known as standardised interview consists of fixed questions and all respondent will receive the same interview stimulus. Interviewees are often also offered a fixed range of answers. An unstructured interview is the opposite of the structured interview. An unstructured interview is guided only by a list of topic or issues prepared by the interviewer that needed to be covered. There is no specific sequencing of questions, therefore, the unstructured interview is usually informal (Saunders et al., 2003). Often the interviewee is given the

opportunity to talk freely surrounding the issues to be discussed. Towards the middle of the continuum, which runs from the highly structured interview through to the completely unstructured interview, lies the semi-structured interview. In a semi-structured interview, the interviewer will have a list of themes as well as some questions to be covered although these may vary from interview to interview informal (Saunders et al., 2003).

Regarding this research, the semi-structured interview is considered to be the most appropriate kind of interview to be adopted. Firstly, since the research has a mixed approach of an inductive as well as deductive approach, the research will have ready certain themes to discuss as well as the need of some in-depth answers from the participants of the interviews. Secondly, although the researcher expects varying representation from the participants at the same time the research is also guided by an investigative framework (section 3.5 of the last chapter), this is much in line with several IS researchers e.g. (Doherty et al., 2012; Hu et al., 2007). In order to verify the interview questions and structure a pilot study was carried out. The next section discusses the pilot study in details.

Table 4.1 *Details of all Interviews*

Phase	Ministry	Interviewee Coding		
		Users	IT Specialists	Managers
Phase 1: Initial interviews	MOHA: Ministry of Home Affairs	MOHA2 MOHA3 MOHA4	MOHA1	MOHA6
	MID: Ministry In Defence	MID4	MID2 MID3	MID1
	MOFAT: Ministry of Foreign Affairs & Trade	MOFAT1	MOFAT2	MOFAT4
	MOE: Ministry of Education	MOE4	MOE2 MOE3	MOE1
	MOC: Ministry of Communication	MOC1 MOC3	MOC2	MOC4
	MOF: Ministry of Finance	MOF2 MOF3		MOF1
	MCYS: Ministry of Culture		MCYS1	

	Youth & Sports			
	MOH: Ministry of Health	MOH1 MOH2	MOH3	
	MOD: Ministry of Development	MOD1 MOD5	MOD3	
	PMO: Prime Minister's Office	PMO2 PMO3 PMO8 PMO9 PMO11 PMO12 PMO13	PMO5 PMO10	PMO1 PMO6 PMO7
Phase 2: follow up interviews and additional interviews.	MID: Ministry In Defence	MID4	MID2	MID1
	PMO: Prime Minister's Office	PMO14 PMO17 PMO18		PMO22
	MOE: Ministry of Education	MOE3 MOE4		
	MORA: Ministry of Religious Affairs		MORA2	MORA1
	MIPR: Ministry of Industry & Permanent Resources		MIPR2	MIPR1
Total Interviews:		**27** Users	**15** IT Specialists	**13** Managers

4.5.2.1 Pilot Interviews

A pilot study was carried out for the interviews; five pilot interviews were done with the Brunei Government's staffs that were in the United Kingdom. Some of the design issues that were tested in the pilot study include; the appropriateness of the terms used in the questions, gauging the depth and breadth of the answers to the questions, the length of the interview and the sensitivity of the questions. The pilot sessions also provide practice sessions for the researcher as the interviewer, particularly in exercising various probing techniques. The recorded interviews were transcribed, analysed and changes were reflected in the actual interview questions. The schedule of the pilot interviews is attached as appendix E. Although the success of the pilot study does not guarantee the success of the actual survey, it has given the research with two advantages. Firstly, it has provided a testing ground to ensure the feasibility of the questions in terms of exploring participants' understanding and any complication towards the instruments, which then can be adjusted. Secondly, it helps in identifying the weakness of the instrument, unforeseen challenges as well as identifying problems with the protocols.

The objective of the pilot study was to firstly, to check whether questions listed in the interview list are well understood by the participants and yield the expected range of responses. Secondly, the pilot study was also used to assess the validity of the interpretative model (section 3.5.1). As an outcome of the pilot study (interviews) some of the questions were altered in the ways they were asked. This is because some of the pilot study participants do not understand the terms used in the question although without realising they are practising what is asked in the questions. So for such instances, a simple brief is given to the participants before the questions were asked. On the dimensions denoted within the interpretative model, some participants were not able to relate to some of the dimensions and variables listed. As this is a very early stage in the study, it was not much of a concern, as it is believed that with a wider number of participant in the actual interviews better relations and representations of these variables is expected.

4.5.2.2 First Phase Interviews

The interview questions were designed to support the research objectives that focused on several dimensions. These dimensions include values (Holbrook's value dimensions), sensitivity and confidentiality of information, perceived importance of information both to individual and organisations as well as cultural issues. These dimensions are discussed in details in section 3.4.5 under chapter 3 of this document. Most of the questions were design to understand the issues of information security experienced and expected by the participants that affect their compliance with the information security policies (standard operating procedure to many). The questions were also meant to elicit the reasons behind behaviours towards specific information security issues. The early picture of the situation shows that there are various factors that influence the behaviours on information security issues. These factors (reasons as described by some stakeholders) are different from one stakeholder to another but possibly pointing to some common general dimensions.

In the first phase of the interviews, a total of 42 face-to-face interviews were carried out for the studies (table 4.1). 37 interviews were audio recorded while five interviewees refused to have the interviews audio recorded. Nearly all participants were comfortable discussing their roles and views towards the issues discussed, and only a few interviewees answered the questions in a cautious way and rather protective.

Conducting the Actual Interviews

The EGNC kindly provided an interview room to for the interviews with a few exceptions in which the interviews were conducted at the interviewee's office. Permission to voice records the interviews were sought from each one of the interviewees before the commencement of the interviews. The recording was used to facilitate the transcription process that was done at a later stage. Field notes (Miles and Huberman, 1994) were taken during all interviews and particularly where no voice recording was permissible the field notes became the primary reference. Field notes are also important in capturing the reflection made by the researcher in capturing the essence of the interview and the general impression of how the interview went. Unsolicited accounts of the interviews can in effect

be a source for revealing information or opinion or can even be one of the most significant parts of an interview (Hammersley, 2007).

Where available, documentation to support participants' reports of the interviews was also requested. Access to such documentation is crucial as it provides alternative insights and deeper understanding of the research context (Bowen, 2005). A significant amount of documentation was collected from the participants for such purposes.

The first stage interviews adopted an exploratory approach in which the main aims was to explore and understand participants' representations of issues and notions of information appreciation in term of how the interviewees assign value to the information, information security behaviours and processes or procedures linked to the development of these behaviours. It is also important to note that the decision on the number of participants to be interviewed was based on several factors. The first factor regarded was that, the researcher felt that to have a fair distribution of the participants and to gain wider insights from different public institutions or organisations. To further strengthen this notion, each ministry must be presented by at least three participants, which belong to the different levels of the stakeholders. These level are the end-user level, the IT personnel level and the management level.

Secondly, the principle of theoretical saturation was also considered to determine whether it would be necessary to conduct further interviews. Theoretical saturation in this context can be regarded as a situation when new concepts have been appropriate, adequately and fully explored and; therefore no new further insights are deemed to be available (Bryman, 2012). Consequently, the motivation is not to maximise the number of interviews, but rather to be saturated with the information being sought, and thus focusing on quality, rather than quantity (Bowen, 2005). Concerning the information gained from the interview process, the conversations with the research participants were voice recorded and then transcribed verbatim. According to (Britten, 1995; Gill et al., 2008) voice recording of interviews is regarded to be more reliable and accurate than written records. Writing notes at the time can interfere with the process of interviewing, and notes written afterwards are likely to miss out some details.

Recording of the interviews was categorised into “rich info interviews’ and “normal interviews”. During the interviews, the interviewer has identified the interviews which according to him yield richer information as priorities. The interviews with richer information are called “rich info interviews” while the other interviews are called ‘normal interviews”. The researcher has personally transcribed the “rich info interviews” while the “normal interviews” recording was transcribed by third parties. The researcher still needs to go through the recording of the ‘”normal interviews” while inspecting the transcriptions to check for errors as well as to pick up any hidden meanings from the conversations. There were two problems with the third party transcription; firstly the person transcribing did not understand the terms used and might unintentionally use other similar sounding words. Secondly emotional and literal meaning might not be understood and might not be presented in the transcription.

By checking the transcriptions from the third parties while listening to the actual recordings, this allows the researcher to come closer to the data. Some deep understandings on the participants’ statements were discovered using this process. Going through the transcripts over and over again also provide the opportunity for the researcher to be able to insert initial coding and make marginal remarks. This process is suggested by Miles and Huberman (1994) and Bryman (2012) to appreciate the context of the interviewees’ statements.

It will allow the interviewer to: be highly alert to what is being said; to follow-up or to further probe wherever necessary; and also to draw attention to any potential inconsistencies in the answer received.

4.5.2.3 Follow-up Interviews

In the second phase of the study, follow-up interviews were conducted with the aim to strengthen or support the previous data collected. The objectives include clarification of some unclear issues in the first round of study such as clarifying several statements and issues that were not clearly understood in the first round of interviews. The follow-up interview also aims to take the opportunity for a further collection of data on the evidence and pattern on the factors identified in the earlier interviews.

The objectives of the follow up interviews were;

i. To fill in gaps, where uncertainty on certain information was realised.
ii. To validate identified patterns, themes and findings from the previous data collection exercise.
iii. Used as a respondent validation method, firstly as a venue to confirm on issues reported by previous participants and secondly as a quality measures in the research as mentioned in section 4.7.

A total of nine follow-up interviews were conducted with participants from the previous stage of interviews. During the earlier stage of interviews, participants were asked if they are willing to participate in further activities such as a follow-up interview or answering further questions offline or online. The details of the volunteers were taken and they were asked to attend the follow-up interviews. In addition to the interviews conducted with the previous participants, several new interviews were also carried out. Four participants were recruited from the unrepresented ministries in the first stage of the interviews. Apart from collecting information on their views on the issues surrounding information security behaviours and information security compliance, the four participants were also showed the proposed model and asked to comment on it. The four participants were recruited from the ministry that was not represented in the earlier interviews. With the addition of the four interviews, the research has managed to cover all the ministries in the Brunei Government.

4.5.3 Focus Groups (Exploratory)

Focus groups are useful to obtain several perspectives about the phenomena or issue under discussion. Unlike one-to-one interviews people can build upon one another's responses and come up with ideas, they may not have thought of on their own. They are particularly beneficial for bringing together a range of people or stakeholders (i.e. staff, students, local authority, community, and local businesses). By including the focus groups in the data collection, it is expected to be able to provide a good opportunity to reach a consensus on certain topics or issues.

According to (Bryman, 2012) a focused interview is about asking questions about a particular situation that is an important element in focus groups. Furthermore, focus groups consist of two research methods: it is a group interview and the interview is focused.

According to Krueger, (1994) focus group interviews are useful in obtaining information, which is difficult or impossible to obtain by using other methods. Using focus groups means that the researcher can intervene into the conversation and pose questions to probe what somebody just has said. According to Bryman (2012) the use of focus groups has not only a potential advantage when a jointly constructed meaning among the members of the group is of particular interest. Participants' perspectives are revealed in different ways in focus groups than in individual interviews, for example through discussion and participants' questions and arguments. However, Bryman cautions that there is a possibility of problems of group effects in a focus group situation that must not be ignored. A similar issue was experienced in the running of the focus group and that make the researcher realise the importance of treating group interaction as an issue when analysing data from the focus groups.

Four exploratory focus groups were carried out for the qualitative studies (Table 4.2). All of the focus groups represent the mixed level of participants from the three categories of the stakeholders. However, due to some restrictions, only one of the focus groups session were audio recorded. The participants of the focus groups were recruited due to their experience from a particular situation, which in this regard was information security and information security compliance behaviour.

Four focus groups were done for the qualitative studies. All of the focus groups represent the mixed level of participants from the three categories of the stakeholders. The participants for all four focus groups came from different ministries. The mixed source of participants provides an advantage to the discussion with different perspectives on the issues under discussion.

All the focus group were given the same subject to discuss. The main subject is the issue of information security in their work place which includes; information security and protection, value of information and compliance with information security countermeasures. The researcher led the discussion by giving a short brief on the keywords and descriptions on the objectives of the discussion as well as a description of the issues to be discussed.

4.5.4 Confirmatory Focus Groups

The confirmatory focus groups (second phase of the data collection) were done in a workshop style of qualitative data collection. A workshop style data collection technique is a good comprehensive, focused discussion technique that helps the researcher to reach consensus on the topic of interest (Eller et al., 2014).

There were three focus groups done, one for each of the stakeholders' category. Since there were small numbers of participants (5-6 people in each group) the plan to do the focus group activities as a small group of 3-4 people was abandoned.

The main objectives of the confirmatory focus group were:

- To share findings of the previous study represented in a model.
- To obtain feedback from the participants on the validity of the model.
- To capture new data that may arise from the discussion of the framework.
- As a platform for sharing of experience and expertise on matters related to the research with the aim of using this information to improve the existing model and further understanding the issues under study.

The confirmatory focus groups were run in a briefing-discussion-summarise fashion. The researcher started by giving a short briefing on the model, the result of previous study and the issues that will be discussed. Next, the participants were given some time to discuss the issues amongst themselves with close moderation by the researcher. During the moderation, the researcher took note on points and ideas brought up by the participants. The points highlighted by the participants were then discussed in more detail before the summarising session. Confirmation from the floor was needed before proceeding to the next topic of discussion.

Three separate follow-up focus groups were conducted. Each focus group was attended by different levels of stakeholders (Table 4.2).

Table 4.2 *Details of all Focus Groups*

Phase & Type	Group Code	Participants type	No. of Participants
1 - Exploratory	FG#101	Mixed	4 participants
1 – Exploratory	FG#102	Mixed	4 participants
1 – Exploratory	FG#103	Mixed	5 participants
1 – Exploratory	FG#104	Mixed	5 participants
2 - Confirmatory	FG#201	IT Specialists	7 participants
2 – Confirmatory	FG#202	Users	5 Participants
2 - Confirmatory	FG#203	Managers	7 Participants

The confirmatory focus groups were split into three sessions; each session took around 30 to 45 minutes. The three sessions discussed the topics such as the conceptual model derived from the research (chapter 5), information value and information value assignment (chapter 6) and the factors that influence the valuation of information (chapter7). A brief introduction to the topic was presented at each session and then the floor was open for discussion and comments from the participants.

4.5.5 Scenario based study

A scenario is a brief narrative, or story used to describe the hypothetical use of one or more systems to capture relevant information. Scenario setting has been used in many pieces of research for example; to simulate learning environment and improve learning (Furnell et al., 2002), optimise processes and policy (Westhoek et al., 2006), understanding users' concerns and preferences about privacy in e-commerce (Ackerman et al., 1999), capturing relevant information for population health and health management monitoring (Bullot et al., 1997) and used as projections of future system usage and helping in requirements identification (Sutcliffe et al., 1998). Sutcliffe et al. (1998) in their study, also highlight various other used of scenario in different studies, such as to simulate taxonomies of events in safety critical systems and environments and to explore theories of human error in high-cost

environments. Furnell et al. (2002) Use pre-defined case base scenario to set up a simulated real-time environment to study participants' action by presenting the participants with a scenario and the security issues to be considered. This approach simulates a real environment in which the participants need to apply real-time decision-making in choosing their action. This approach also provides the ability to influence participants' action by providing them with various alternative solutions, thus enforce learning. Similarly, the study by (Albrechtsen and Hovden, 2010) used scenario based workshop to ignite discussion on possible actions when faced with some information security issues, although the objective of the exercise was aimed at providing learning outcomes, it also provided some data collecting opportunities. In other studies, such as of Bullot et al. (1997), used scenario to illustrate connectivity between various data collecting methods and highlight the specific data need to be collected and extracted, thus this provide an indirect triangulation of data.

Scenarios could also be topic focused, such that presenting the desired situation to be tested rather than using a probing process of semi-structured questioning that is time-consuming (Furnell et al., 2002). Ackerman et al. (1999) in their study of privacy in e-commerce provide their participants with four on-line scenarios to collect and study their concerns and attitude towards e-commerce transactions.

Relating to the above use of scenario, it is summarised that the use of scenario-based questions in this study will provide for the following:

- Scenario based inquiries help in setting up the environment, thus avoid the waste of time for the interviewer probing the interviewee.
- It is postulated that participants will be able to relate to the pre-defined scenario either from individual experiences or experience related by others thus will yield a rich information collection exercises.
- Although it is expected that some of the participants will not have experienced the pre-defined scenarios (or they does not realise that they have gone through them), scenario-based questions will still be able to project their intention to behave.

Scenario based Questions

For the studies of this research, it is planned that scenario-based approach will be used to enhance the data collection. Scenario-based questions will be used to structure the interviews as well as the focus groups. Scenario-based questions will be used to explore the interviewee's personal point of view based on a pre-determined scenario in which mainly decision and choices have to be made.

For the focus groups method, it is expected that by setting up scenario participants will be able to share experiences and knowledge between members of the group through facilitated participation, collective dialogues and considerations processes. It is, therefore, foreseen that a scenario-based interviews and focus groups will be able to facilitate the successful elicitation of information that can be used as building blocks for further investigation using quantitative study.

To achieve the objectives of the study, this is outlined in the previous section; a set of '*critical incident*' scenarios was utilised. It was envisaged that the discussion relating to issues of compliance could be set around these scenarios. The selected potential incidents for the interviews and focus group discussion include clear desk policy, password disclosure, usage of portable device and software infringement. These 'critical incidents' were derived from mandatory internal controls typically recommended for organisations to implement to ensure Information Security efficiency (Home Civil Service, 2012) and outlined as potential incidents to information security threats (Tajuddin, 2010). The scenario based incidents are presented as an appendix in this document under '*Appendix A – Scenario Based Questions*'

The above section presented various methods of data collection used in the research. These methods are spread across three phases of data collection. To summarise, the following table, table 4.3 show the various data collection approaches used in the research which is spread across the different phases of data collection. The last column of the table provides information on the number of groups or participants for each of the methods.

Table 4.3 *Data collection methods used*

Data collection stages	Methods	Remarks
Pilot	***Interview***	5 participants (Bruneian residing in the UK) Used of scenario based questioning
1st Phase	***Interview***	42 individual participants (represent different level of stakeholders) Used of scenario based questioning
	Focus Group	4 Groups (mixed participants form the three types of stakeholders
2nd Phase	***Follow-up Interview***	9 participants Used of scenario based questioning
	Confirmatory Focus Groups	3 groups (each representing one type of stakeholders) Key issues were discussed

4.6 Analysis of Data

In the previous section of this chapter, it has been mentioned that this research adopts a pragmatic approach. The idea is to be open on the choice of techniques and tools that help in either the collection of data as well as the techniques in which the data is being analysed.

This research will utilise a framework based partially on the approaches of grounded theory (Strauss and Corbin, 1990, Matsuo et al., 2008, Glaser and Strauss, 1967). As defined (Glaser and Strauss 1967), grounded theory is "the discovery of theory from data systematically obtained from social research". Although grounded theory has been regarded as one of the most influential and widely used strategies for conducting qualitative

data analysis (Bryman, 2008) this research will only be using two of its key principles. Firstly, it will partly look to develop theory out of data (Creswell, 2009) and secondly it will adopt the principle of approaching the data analysis in an iterative way (Miles and Huberman, 1994). Miles and Huberman (1994) pointed out that utilising the iterative approach characteristic of the grounded theory is expected to help in yielding a deeper and richer understanding of the real meaning of the participants' statements.

Although grounded theory was initially seen as the primary analysis technique to be used for this research, it was not possible to adopt an exclusively grounded theory approach, as this wouldn't be appropriate for a study which is to be guided by the use of a theoretical framework. Generally, the analysis will adopt the technique suggested by Creswell (2009) as depicted in figure 4.3 below. Although the design to be carried out is in a linear way, some of the stages will be in an iteration process until an acceptable condition is achieved. It is also important to highlight that the stages are not necessarily carried out in order.

In order to ensure a thorough analysis, a software product called NVivo was utilised to support this research. To this end, the researcher underwent a 16 hours training programme, to familiarise himself with using Nvivo as an analysing tool for unstructured data. A similar type of software product called CAQDAS or Computer Assisted/Aided Qualitative Data Analysis Software are highlighted by earlier researcher such as (Bryman, 2008). Due to the overwhelming amount of data collected in a qualitative survey, it is typical for a social researcher to use similar software in order to make their coding, retrieving and storing of data are much convenient and faster. Although software such as Nvivo has potential in assisting the process of coding and analysing qualitative data, it is important to remember that, how the coding to take shape and the interpretation of the data are still totally the responsibility of the researcher.

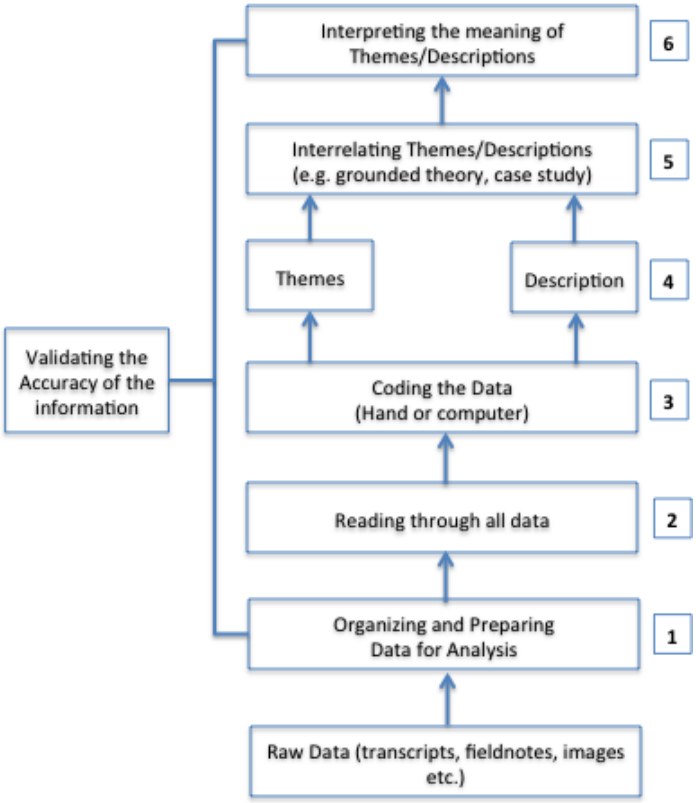


Figure 4.3 Data Analysis in Qualitative Research (Creswell, 2009)

The analysis was approached from two dimensions; firstly, the analysis focused on how individuals responded to the questions asked and secondly, it focused on the responses from a different group of stakeholders.

The transcribed interviews were coded by reading and rereading each of the interview scripts in Nvivo, and then making remarks through the use of memos, where necessary (Miles and Huberman, 1994, Bryman, 2008). The remarks or 'marginal remarks' (Miles and Huberman, 1994) consist of notes on what is being coded; the idea in discussion; interpretations; or determining their interrelation with other parts of the interview data. According to (Bryman, 2008) iterative reading of the transcripts and the remarks made are beneficial as they will provide familiarisation to the content, the more the researcher are familiar with the transcripts and be able to reflect back to the actual interviews, better understanding of the tacit or underlying meaning within the data can be achieved.

Subsequently, key patterns and emerging themes will be identified (Bowen, 2005, Miles and Huberman, 1994). The themes that are of interest to the research will be in line

with the intention to gain insights arising from the identified research objectives outlined in the preceding chapter. The processes mentioned above are iterative and it is best represented by the figure 4.3, which shows the iterative nature of the processes. The interview transcripts were also be constantly referred to, in order to reduce the risk of losing the contextual background or narrative of the findings. In most instances, reading the interview transcriptions helps to gain deeper insights and understanding of what an interviewee was saying. Thus, the effort was able to reduce the risk of "decontextualizing data" (Fielding and Lee, 1998), as well as the possibility of being disconnected or uninvolved from the findings.

For the first phase of the data collection exercise, forty-four one to one interviews and four focus groups were carried out. The analysis of the data began with creating an initial broad coding framework (Miles and Huberman, 1994). The coding framework was initially based on the theoretical Interests that guided the research questions but at the same time any salient issues that arose in the data were also translated into codes. Therefore, the analysis started with a list of coding, pre-established criteria decided from the review of the literature. Table 4.4 shows the initial coding framework.

Table 4.4 The Initial coding framework

Organising themes	**Basic themes**	**Descriptions /Remarks**
Importance Metrics	Individual	Consists of representation the importance of information from the perspective of individual as well as how they see it from a communal lens.
	Organisational	
Information Sensitivity	Information Context	Descriptions of the sensitivity of information by the stakeholders from the context in which the Information is used, stored and communicated as well as based on the standard classification of
	Information Classification	

		the information according to where the stakeholders reside.
Culture	Organisational	Representation on how different level of culture and customs affect stakeholders perspective of information value and compliance with its protection
	National	
	Customs	
Spiritual		How religious and beliefs affect stakeholders perception on information value and handling of Information.
Social	Workplace	Stakeholders' representation on how social issues might affect their Information value assignment and how they treat their information and its protection.
	Outside	

Transcripts were coded both top-down using the previously identified coding scheme, and also bottom-up with each theme fleshed out with more detail and new codes added. Each interview was coded and the codes brought together into categories.

As mentioned earlier in section 4.3 this research employs a mixed approach of deductive and inductive approach, therefore the analysis of the data also deploys what is described as a 'general inductive approach' keeping in mind that new theme and codes may also arise from the analysis. Miles and Huberman (1994) describe such an approach as qualitative analysis and propose three main activities;

- Data reduction - the process of 'selecting, focusing, simplifying, abstracting and transforming' the raw data;
- Data display - 'an organised, compressed assembly of information that permits conclusion drawing';

- Conclusion drawing and verification.

The decision to couple the inductive approach with the earlier mentioned deductive approach is in line with Miles & Huberman's (1994) recommendation of using the qualitative analysis with a provisional set of codes. Initial codes come from both pre-defined codes as well as defined from what is seen from close reading of the data, an iterative process of comparing data with data (Charmaz, 2006). This process is also similar to the list of processes suggested by Thomas (2006).

Although Charmaz (2006) suggested that coding is done word by word, it is not feasible in this research. Rather, segments of texts in the form of phrases or paragraphs were used rather than any predetermined size. The phrases and paragraphs were chosen by their meaningful content. These meanings were developed into definitions of codes and memos were written about the codes, reflections and observations about the data by the researcher. A memo is a useful method of recording ideas and potential concepts that occur to the researcher as they are going along and continues all through the analysis. Writing successive memos throughout the research process keeps the researcher involved throughout the analysis and helps to increase the level of abstraction in the narrative of the research (Charmaz, 2006).

The results from the initial coding may be a long list of descriptive codes summarising the data but the next level in the coding process is what Miles and Huberman term ‘pattern coding’ (1994, p.69). It is a way of grouping initial, descriptive codes into ‘explanatory or inferential codes, ones that identify an emergent theme, configuration, or explanation’ (Miles and Huberman 1994, p.69). Pattern codes are generated by ‘looking for threads that tie together bits of data’.

Emerging themes (or categories) were developed by studying the transcripts repeatedly and considering possible meanings and how these fitted with developing themes. Diagrams (mind maps) were used to focus on what was emerging and to link different stakeholders’ themes into major influencing factors represented by the stakeholders. In regards to this research, all the processes mentioned were done iteratively until it is evident that no new themes emerged, which suggested that major themes had been identified (Creswell, 2009).

4.7 Quality Criteria

There are plenty of discussions in the literature regarding how to ensure the quality of qualitative research in term of proving and ensuring their reliability, credibility and validity (e.g.Mason, 1996,Lincoln and Guba, 1985,Guba and Lincoln, 1994, LeCompte and Goetz, 1982). It is important to highlight that it is not the objective of this research to make detail comparison of these variations.

There are two schools of thought if it comes to quality in research. The first school of thought is from the quantitative side of research, which defies the use of quantitative quality measures in ensuring quality in qualitative research. As mentioned by (Creswell, 2012), (Ely et. al.,1991) asserts that 'the language of a positivistic research is not congruent with or adequate to qualitative work'. Alternatively, as a second school of thoughts (Guba and Lincoln, 1994; Lincoln and Guba, 1995) used the terms; credibility, authenticity, transferability, dependability, and confirmability. Terms that they claimed to be more natural in replacement of internal validation, external validation, reliability and objectivity to ensure the trustworthiness of the research. Along with this perspective (Lincoln and Guba, 1995) has describe a series of techniques that can be used to conduct qualitative research that achieves the criteria they outlined. Creswell (2012) recommended that qualitative researchers should engage at least two of the listed techniques in any of their studies.

Engaging, the suggested evaluation criteria must be taken with precaution as some of the criteria may cause conflict. Taking into example peer audits or external audits, which are used to establish dependability criterion are more time consuming and may involve substantial costs to the researcher. Another issue that may arise is that when using member-checking or respondent validation, the risk of research participants becoming defensive or goes into a state of denial once the findings are revealed to them. Having known the techniques and criterions outlined above it is also important to highlight that "*we can never be certain about the truth of any account since we have no completely incontrovertible way of gaining direct access to the reality on which it is based*" (Bryman, 2012).

Therefore, without totally ignoring the alternative assessment criteria suggested in the extant literature, this research would take into consideration in adopting a few techniques in order establish rigour in the research. In this regard, there are a few methods that will be used in this research to ensure quality. The methods for each of criterion adopted from (Lincoln and Guba, 1995) is outlined in the following table.

Table 4.5 Quality assurance methods used in the research

Criterion	Definition	Methods used to ensure quality in this research
Objectivity/ conformability	Freedom from bias or explicitness about bias	• Being explicit in the theoretical assumptions underlying the research • Describing the methodology in detail so the process of the research can be followed and it is transparent • Keeping a 'research diary' and using memos, so an 'audit trail' is created by thoughts and activities
Reliability/ dependability/ auditability	The degree to which the research process is consistent, clear and stable across time and methods	• Making clear the philosophical stance was taken by the researcher • Recording respondents words verbatim • Transcribing carefully to provide an accurate rendering of respondents words • Keeping records (as above) of activities • Checking, and writing memos about, the codes and their meanings
Internal validity/ credibility/ authenticity	Findings should make sense and be credible	• Presenting quotes in the report from respondents • Use of constant comparison methods during analysis - comparing data to data and case to case • Using appropriate tabulations (Silverman 2006,p.299; Miles and Huberman 1994, p.252 Qualitative research does not mean excluding simple counting techniques to indicate variance or prevalence
External validity/ transferability/ fittingness	The extent to which the results have a larger import is transferable to other contexts and	• Provide comprehensive information on the context in which the research is carried out; provide a 'rich' description • Careful and thoughtful sampling; being explicit as to method of

	whether they 'fit.'	sampling • Being explicit about areas of uncertainty • Presenting work for peer review through writing for publication
Utilisation /application /action orientation	The usefulness of the research and who may benefit from it	• Ethical concerns are clearly addressed • Suggestions for further research

4.8 Constraints and limitations

With more than 15 years' experience in the information Technology and Security area, it is difficult for the researcher to approach the research without any form of preconceived notion that may exist due to the researcher's views rooted in his underlying values and experiences. Nevertheless, efforts have been taken to ensure that the research is not unnecessarily influenced by this aforementioned situation. In this regard, it is recognised that the research needs to be as far as possible, neutrally conducted and analysed in an unbiased view without any pre-set judgement. As the research is also adopting an interpretive approach, it is hugely important for the researcher to be able to exhibit the skill to effectively engage, investigate and learn how possible interactions might have taken place from the viewpoints of the participants (Chen and Hirschheim, 2004).

4.9 Ethical Consideration

It is the norm for any research that involves the collection of data and information from people and about people to pass through an ethical clearance. Apart from the normative practices of the ethical researcher, it is also a requirement from the university as that several ethical issues are considered to establish safeguards that will protect the rights of participants. These safeguards may include informed consent, protecting participants from harm, and ensuring confidentiality.

Therefore, prior to any data collection activities in this research, Loughborough University's ethical clearance checklist was completed. The recommendations of Loughborough University's Ethical Advisory Committee's Code of Practice on Investigations Involving Human Participants were fully adhered to throughout the whole process of this research. More specifically, the following issues were considered:

1. All interviews and observations were conducted in research respondents' natural environment (e.g. participants' offices and some even preferred coffee shops) at a time and place that suited the participant.

2. All interview respondents received and read the Participant Information Sheet (see Appendix C), stating the nature, objectives and duration of the research.

3. Prior to any data collection activities, Informed Consent Forms (see Appendix D) were sought from interview respondents and verbal consent was sought from observation participants.

4. Participants had been informed of their right to withdraw from the investigation at any time before they signed the Informed Consent Form.

5. Participants were assured of the confidentiality of data gathered during the research. Each participant was assigned a code and all data was stored in that code rather the name of that participant.

6. All data was stored in their original forms on the PC in a secure building and was password protected. Also, all information will be destroyed within six years of the completion of the investigation.

4.10 Concluding remarks

As a conclusion, this research is driven by a qualitative approach guided by a philosophical view of interpretative and constructivism. A pragmatic stand was taken in terms of tools and techniques used in the studies, for example, the adaptation of some of the principles of grounded theory.

Consistent with the selected philosophical idea and strategies of inquiry, data was collected from semi-structured interviews, focus groups and workshops. These data was then analysed, employing a thematic analysis approach with some techniques borrowed from the grounded theory analysis.

This mark the end of the methodology discussion, and the next chapters, chapter 5, 6 and 7 will present the discussion on the findings of the research.

5.0 Perceptions of Information Value

5.1 Introduction

Collectively, this chapter and the following two chapters, chapter 6 and chapter 7 present the key findings of the research. Each of these three chapters will focus primarily on discussing the significant findings, relating to one of the three research objectives of the research. Figure 5.1 below shows how the various elements of the results are distributed across the three chapters.

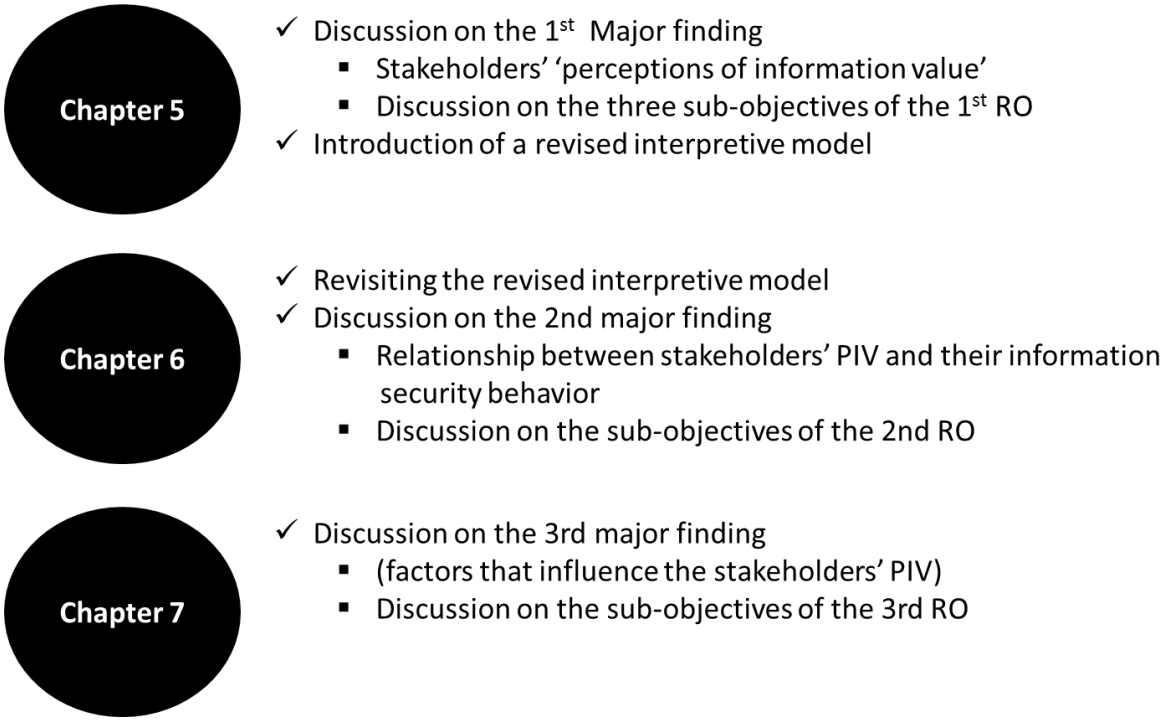


Figure 5.1 *Chapters discussing the research findings*

The results in this chapter are based on the analysis of the 'first phase' data collection, which comprised of the pilot study, and the first substantive qualitative study that consists of one-to-one interviews, focus groups and workshops. In particular, this chapter will focus on one aspect of the fundamental findings of the research, namely the stakeholders' 'perceptions of information value'. Exploring the potential of 'perceptions of information value' in the context of information security is one of the main objectives of this research as

outlined in chapter 3. As mentioned in the literature review, the motivation for exploring stakeholders' 'perceptions of information value' was based on the practical adoption of this distinct construct in the marketing and health fields. Consequently, in the context of information and its security, it is envisaged that the stakeholders' 'perceptions of information value' might affect their attitudes to its protection, and so this chapter will consider whether stakeholders develop clear *'perceptions of information value'*, for the information they handle, and how such values are assigned. This chapter will review and critique the initial interpretive model, in light of the initial data collections, as well as present and justify a number of enhancements that were made to it.

The aim is to obtain representations from the multilevel participants on the issues defined under research objective one (figure 3.3). Furthermore, this chapter will also present the findings in relation to each of the sub-objectives developed under research objective one. Therefore, the structure of this chapter is as follows; the succeeding section will first introduce the finding related to the stakeholders' 'perceptions of information value'. This is then followed by discussions on findings related to each of the sub-objectives defined in chapter 3. Next, a revised version of the interpretive model is introduced, and its significant to the research is explained and justified. This chapter is ended with some concluding remarks.

5.2 The concept of information 'value.'

The first objective of this research (section 3.3.1), is to ***understand the extent to which stakeholders develop clear 'perceptions of information value', and the processes by which they assign value to the information that they handle***. Particularly, the primary interest is to explore whether stakeholders, who are engaged in information security, assign any kind of value to the information they are handling. Subsequently, if such perception exists, other questions that need to be answered are; how is the information value formed? What are the processes involved in the assignment of the value? And what are the factors that could influence the process of information value assignment?

With particular relation to the findings on 'perceptions of information value', the analysis of the first phase data collection revealed that it is, indeed, common for stakeholders to assign a value to the information that they use. These instances of 'perceptions of information value' are typically the result of the subconscious process of value assignment by the stakeholders. Whether they realise it or not, one way or another, the stakeholders are making a judgement and trying to rationalise how much they should value a specific piece of information, at an appropriate moment in time, and in a particular context. Although there is no explicit mention of the exact term 'perceptions of information value', the respondents provided numerous accounts of actions and references as to how they attributed value to the information that they used.

This research was initially guided by a conceptual interpretive model as depicted in chapter 3 (figure 3.4). The model indicates that the 'perceptions of information value', in the context of information security, are generated from the individual information value assigning processes of stakeholders, within an organisation. It is also postulated that the information value assigning processes are influenced by several factors. In addition to exploring the research objective using the research model, the findings from the first phase data collection were also used to examine the validity of the initial interpretive model, and then make any required modifications, accordingly. In light of this exercise, a revised interpretive model is introduced at the end of this chapter and the justification of the changes will be highlighted throughout this chapter.

To better explain the findings of the first research objective, the findings are sub-divided according to the three sub-objectives. These three sub-objectives primarily relate to the validity of using the construct 'perceptions of information value' and the processes involved in evaluating and assigning the value to the information, as adopted by the stakeholders. The exploration of the three sub-objectives, in turn, will provide the evidence that stakeholders do create clear 'perceptions on information value' and use these as a reference point, in the context of information security or information protection.

The next sections in this chapter will discuss the findings according to the three sub-objectives. The discussions in the next sections will be based primarily on quotations from the interview transcripts, which demonstrate the respondents' interesting reflections on their perceptions of information value. These excerpts also point to various categories of intrinsic and extrinsic factors, which affect stakeholders' decision-making when assigning a value to the information they are handling.

5.2.1 Stakeholders' Concept of Value

The **first sub-objective of RO1** is ***to explore the concept of 'value' in the context of information handling and information security and to understand how meaningful this concept is from the perspective of stakeholders***. Identification of any approach used by stakeholders to assign value will confirm that the notion of 'perceptions of information value' has some validity. This first sub-objectives opens up questions like, *how does a stakeholder value information? How do they measure the value? What kind of measurement unit do they usually use?*

Generally, in the field of economics, the 'value' of something, for example, an object or service, is based upon the utility it provides. Utility is, therefore, a term to describe the satisfaction or the usefulness of an object or a service (Al-Hamdani, 2009). The more utility an item has, the more value human beings are willing to assign to it. In this way, utility can be synonymous with the subjective human value. However, utility in this context cannot be compared to a market value, which is expressed in dollars, due to its aggregated and impersonal nature. Similarly, in the framework of this research finding, value or specifically 'perceptions of information value' ' are defined in terms of the utility that can be derived

from it. In particular relation to this sub-objective, outcomes from the initial analysis revealed the following findings. An early indication that the concept of 'value' is indeed useful in the context of information handling and information security is supported in the excerpt below:

> **PMO-06** *I'm dealing with relevant information, this information is crucial to the core function of the department, so as an officer, I'm responsible for ensuring its security.*

The stakeholder excerpt above is based on his/her perception of the value of the information he/she is handling through, firstly, the position he/she is assigned to the organisation and secondly on how important the information is to him/her and the organisation. A stakeholder towards the top of an organisational hierarchy (managers and IT specialist) would expect to have more responsibility for the information that he or she handles. These expectations build perceptions and beliefs that the information he or she controls is relevant both to his or her work as well as being critical to the functionality of the organisation because he or she holds a significant post in the group. Meanwhile, a user level stakeholder within the organisational hierarchy (usually subordinate staff for example; clerk and support staff) may feel that due to their more lowly position in the organisation they don't necessarily handle data that is crucial to the functionality of the organisation. These perceptions are also the outcome of beliefs that the information they are processing does not provide them with any specific, personal benefits. These notions, motivate the user level stakeholders to perceive that protecting information is not compulsory, therefore the tendency of assigning a low value to the information is common. This widespread perception from lower ranked staff that the information they handle has little value, because of their relatively unpretentious status, is reflected in the following quotes:

> **MCYS-01** *I'm nobody in the organisation; I'm not involved with any relevant information or data. More senior people will look after the security*

> **PMO-17** *I'm a junior clerk in the finance department but I'm only handling information on staff salary not like my senior colleagues they handle more relevant information.*

The above perceptions by the lower level stakeholders are sometimes supported by the same view from their superior. Such view from a superior would only provide more excuse for the lower level stakeholders to strengthen their perceptions on which they build their beliefs on.

> **MOD-03** *They are only clerks, doing the mundane things (changing letters and so on) the clerks don't need to have security as they are handling non-important data.*

Stakeholders within the higher posts similarly share the view that the position of the post-holder have impacts on the value that they assign to their information. They perceived that with the posts they are in, comes higher responsibilities of protecting the information. As can be seen from the quote, below, they believe the information they handle is of more importance both to the organisation as well as themselves if compared to user level stakeholders:

> **MID-01** *Lower ranks staff they don't understand the importance of some information, they just give out this information to friends and family for them this may be safe but not for higher level or rank like us… we went through proper training*

The subsequent excerpts show that although some stakeholders do not consider their job is that significant to the organisation, occasionally they admit that they do handle information that they think is more sensitive and does warrant better protection.

> **MOHA-01** *I don't believe that my job is critical, I don't believe that the information I handle is secret, but sometimes we have some information on prisoners, that should be confidential.*

The succeeding responses indicate that stakeholders may also base their perceptions of information value on what they think the sensitivity of the information is, as well as how applicable the information is to them:

> **PMO-01** *I'm also doing the budget, this is highly classified information, it must be secured, if it's only information on staff and students, then it would not be that important to be 100% safe.*

> **MOHA-04** The *information we have is really sensitive, people will get worried and may panic if they learn about all the problems we have in Brunei, security of the information we have is really important.*

The following excerpt is an indication that not only the stakeholder makes a value judgement about the information, which he/she is handling, but it also indicates that his/her information security behaviour is adjusted accordingly:

> **PMO-03** *I consider all information that I managed personal and therefore sensitive. I don't like people to be nosy around my work. I keep my desk tidy and clear all the time.*

Perceptions of the value of information are also influenced from the perspective of religion and spirituality. Although not directly linked to the formulation of 'perceptions of information value' the notion that the religion provides guidelines on the ethic of working and obeying instructions helps the stakeholders in formulating the importance of securing or protecting the information that they are entrusted with, as demonstrated below:

> **PMO-02** *My religion does not permit us to do anything bad, so we must follow rules and regulations. If the information is said to be confidential we must treat it as it is; we cannot share that information*
>
> **MIPR-*01*** *our religious practice teaches us, to be honest, and trustworthy in our life, the same goes to our work; we need to treat things, as they need to be addressed.*
>
> **MOD-05** *the religion of Islam and all the other religion in the world teaching are towards being trustworthy and obey instruction as long as it is on the right path. Upholding security of information is considered one of the directions from our superior so we must obey to that.*

Closely linked with the perspectives of religion and spiritual practices above, following instructions from superiors are also common factors, for stakeholders, when formulating their perceptions on the value of information. Obeying instruction is also closely linked to the norm of culture in this region. The leader or superior is always seen as knowledgeable, knows better and benevolent, and therefore refusal to follow their instruction can be viewed as a matter of disgrace, as reflected below:

> **MOHA-03** *We don't have any policy; we work according to our superiors' instructions or command. So it is up to the person who gave us the direction, it may also change*
>
> **MOE-04** *I trust my boss; I will follow his instructions because he knows the security*
>
> **MOF-01** *The upper management should be able to show us what to do with information security; they must take the first initiative to demonstrate the*

> *importance of being secure I rate the information that I'm handling as very sensitive, my boss says that no other people should see it.*

Apparently, similar to the field of marketing and health, it is evidenced that in the context of information security and information security compliance, there are comprehensive references made to 'perceptions of information value'. The stakeholders are developing clear perceptions of information value, based on various issues or factors that they assumed are relevant to them and based on the issues or factors that provide them with the most utility. Most of the time, stakeholders at various levels within an organisation, formulate their own perceptions of the value of the information they are handling and in some instances they may also develop perceptions of the value of their colleagues' information.

Generally, the value perceived or assigned are higher on information that is personally handled, as compared with information that is the responsibility of other stakeholders. This indicates that, if the information is considered to be owned by the stakeholder, then there is a higher likelihood that they will assign a higher value to it. These valuations of information and the assignment of value upon the information are also dependent upon the context in which it is undertaken. Therefore, information is categorised either as information personally owned or information held by other stakeholders.

Personally owned information is information that is within the dominion of the stakeholder i.e. the information is available or accessible to the particular stakeholder because his or her tasks depend on or revolve around that information.

> **PMO-07** *my work is concerning financial matters, there are important to me and it is crucial for the organisation. It is of high value to me so the security is crucial.*
>
> **MID-02** *the information that we handle are highly classified and imperative to the safety of the nation.*

For example, a clerk in an organisation will have in his or her possession the personal information of the organisations staff because it is his or her job to look after the welfare of the organisation's staff. Meanwhile, information that is considered to be under the dominion of other stakeholders is seen as owned by the other stakeholders.

> **MOE-02** *I'm more concerned with the Information that's my responsibility; another information is looked after other colleagues.*
>
> **MOHA-03** *I'm responsible for the information trusted with me, I'll make sure it's protected. It's the same with others they also have information that is entrusted to them, logically they need to maintain its security.*

Logically, information that is within one's dominion is considered to have a higher value than the information that is outside their personal responsibility. This notion might arise due to the perception that the management of the information (including its protection and security) is the responsibility of the owner of the information or whoever has the possession of the information.

> **PMO-05** *Each and one of us (staff) should help and protect the information under our jurisdiction. The information I'm dealing with is important for my work so I need to ensure its security.*

Due to these perceptions, the value placed on particular information becomes subjective. Coming back to the example of the welfare clerk, a complex perception of information value will arise. The actual value of the information might not be understood and shared by all stakeholders, as each stakeholder will stand by their own perception of the value they have assigned. Unless the stakeholders make the value assessment of the information from the same perspective used by the other stakeholders, they might not assign the same appropriate value on it. Understanding how the value of information changes from the perspective and evaluation of one type of stakeholder to another would help different stakeholders to understand and appreciate the 'perception of information value' derived by another stakeholder.

The interviews data also suggests that stakeholders assign a different value to the different type of information. This notion is presented in the following excerpts, in which some information is perceived to be more important than others:

> **MOE-03** *I deal with various type of information, some general information for example student and staff data and some important information for example financial information.*

Furthermore, the interviews data also suggest that different stakeholders assign dissimilar value even to related information, particularly if they think that the information is not crucial to their work. The succeeding excerpt shows the explicit contrast with the preceding passages. In this example, the related 'staff information' is perceived to have distinct value by two stakeholders:

> **PMO-12** *the most important information that we dealt with is staff personal information. The consequences of such data, when compromised, can be devastating.*

To summarise the above presentation, it is clear that there are variations in the interpretation of value as epitomised by the stakeholders. Stakeholders build their concept of value from the various viewpoints such as their post, their scope of responsibilities, how they perceive the importance of the information, their perceived sensitivity of the information and depending on their belief system. Additionally, it is also learned that these interpretations are very subjective depending on the context in which the information is being used. Another conceptual view articulated by the stakeholders is related to the ownership of the information. Ownership of information plays a crucial role in determining the 'perception of information value' of the information, for example, an owner of information may assign a higher value to his or her information compared to a mere user of the information. Responses from the stakeholders also signify their realisation that the concept of value derived from the information potentially denotes what sort of action (behaviour) is to be taken by the stakeholder.

5.2.2 Diverse perspectives of stakeholders

The **second sub-objective** of RO1 seeks to explore ***whether 'perceptions of information value' vary from the perspective of different groups of stakeholders***.

In the context of this research, there are various groups of stakeholders. First of all, as portrayed by figure 3.4, the stakeholder could be the owner of the information, who is usually in the organisation's management, an IT specialist or a general user. In the context of this research, this categorisation will be called the 'level' of the stakeholders. The justification for the classification according to levels was discussed in the section 2.3.2. Some of the responses from stakeholders (also mentioned in the previous section) suggest that stakeholders from different levels would have different 'perceptions of information value' based on their own particular perspectives. The following excerpts are taken from the interviews with the management level and IT specialist stakeholders:

> **MOFAT-04** *regardless of the classification, all information must be treated with an attitude towards maintaining its security.*
>
> **PMO-07** *my work is concerning financial matters, there are important to me and it is crucial for the organisation. It is of high value to me so the security is essential.*
>
> **MID-02** *the information that we handle are highly classified and very important to the security of the nation.*
>
> **MOHA-03** *I'm responsible for the information trusted with me, I'll make sure it's protected. It's the same with others they also have information that is entrusted to them, logically they need to maintain its security.*
>
> **PMO-05** *It is within our job description as information security office (ISO) to ensure the protection of all the information in the organisation.*

Collectively, these responses suggest that stakeholders who are at the management level or that have IT background, express a high level of concern about the security of the information they are handling. Both the management-level and the IT specialist-level stakeholders' also show some sense of ownership of the information, which they handle. According to (Jafri 2015), when employees and team members feel the ownership about their work, they respond with more positive motivation for the work they do. Similarly, in this context when a stakeholder assumes ownership, he or she showed more positive

valuation on the information he or she is handling. On the contrary, the following responses from the user-level stakeholders show that they have less concern over the security of the information they are processing:

> **PMO-16** *as the information I handle are not confidential and sensitive; I only need basic IT and information security knowledge. I guess that is the reason why I was never given any training on IS.*

The above stakeholder suggests that the value of the information he or she is handling, is not significant thus it is sufficient for him/her to have little knowledge of information security. This attitude clearly indicates that she does not give much thought on the issue of information security. The excerpt also indicates that the stakeholder believes that if the information is to have more significant value, better security knowledge (information security measure) has to be provided for the information. The above notion is further supported by the quote from a security officer that explains the general attitudes of users in a department:

> **PMO-05** Although *they are computer literate (referring to users) they are not Information Security (IS) savvy, meaning they know how to use the computer but beyond that they don't know anything about securing information*

The followings are other excerpts from the interviews that indicate how user-level stakeholders' view differs from their other colleagues who are in management and IT levels:

> **MOC-01** *at my level, I'm not really exposed to any classified or confidential information*

The above is the response from a user-level stakeholder when asked about the importance of information protection from her perspective. Her respond suggests that she assumed the information she is handling is not highly valued, therefore, this indicates that she has less value assigned to the information she is handling. The same sentiment is expressed by another user-level stakeholder below.

> **PMO-13** *my work is delivering letters and documentations as long as I keep them with me all the time it should be safe. I refuse to use a secure bag because I don't carry any money, most are only letters.*

It has also become apparent that as well as being made by individual stakeholders, perceptions of information value may also be done collectively by a group of stakeholders, which will be referred to as the 'workgroup' (section 2.6). Consequently, 'perceptions of information value' could be derived from either an individual (discussed in section 3.2) or the workgroup perspective (workgroup PIV). A Workgroup perceptions of information value (WPIV) is the value perceived on specific information which is collectively accepted in a group of stakeholders. The WPIV might originate from the PIV of an individual stakeholder, who then lobbies for it to be accepted by other stakeholders. Over time, this value is agreed to by all or majority and it may become the de facto value of particular information. Therefore, a WPIV is a value that a stakeholder believed other stakeholders assign or agree on a particular piece of information. As with the espoused value, the workgroup perception may emionate from managers or IT specialists, but it typically comes in the form of informal advice, rather than an explicit dictat. The workgroup PIV might be expressed by other stakeholders directly or value that is perceived based on interpretations of the behaviour of the other stakeholders.

This further categorisation shall be known as the 'type' of the stakeholders. Due to a different level and the various types of stakeholders, it is expected that a variation in 'perceptions of information values' may arise. It is also envisaged that since there is a possibility of misalignments between these perceptions, it may ultimately lead to inappropriate information security behaviours.

It has been possible to conclude that the perspectives of stakeholders from the two different types are indeed often different. This is because the perceptions of information value from an individual stakeholder's perspective may not correspond with the common perception of information value by the majority members of a work unit. In a collective society, such as Brunei Darussalam, collective views are common. These collective views are generally more accepted by the society rather than individual views. It is not uncommon for an individual stakeholder to change his/her belief when challenged with a different view from a workgroup, especially to gain conformation. Such conformity is brought about either by a desire to; fit in, be liked, to correct or to conform to a social role (Saul McLeod, 2016). In some cases, an individual shareholder may have to forego his own 'perception of

information value', and adopt the workgroup perception. This is despite the fact that he or she believes that his or her perception of the information value may be more valid and reliable. The following quotations support the view that quite often perceptions of information value are heavily influenced by workgroup behaviours and attitudes:

> **PMO-07** *this department is very strict when it comes to the security of certain information, I was reminded a few times regarding the confidentiality of the information and how to handle them.*
>
> **MOCYS-03** *colleague here is more supportive in term of ensuring information protection. Information is highly valued; this is shown through high compliance behaviour. You will get told off by your peers if you do something wrong eventually everyone is information security conscious.*

The above responses show examples in which a workgroup shows positive views on the PIV of the information they are handling compared to some individuals in the department or unit. Meanwhile, the excerpts below indicates how workgroup views on PIV have overcasted the stakeholders personal perspective on the PIV of the information they are handling:

> **MOD-TA** *my boss is not strict at all. Tasks are not appropriately aligned. People can have access to information they shouldn't have access to. Basically, security of information is weak. I have to follow the trend here; otherwise, they'll see me as 'mengada2' (arrogant).*
>
> **MOE-02** *the working environment is different here from my previous office, here colleagues are more relaxed regarding information security, information is shared regardless its classification. Sometimes it's easier to follow suit.*

One issue that may arise from this would be, where the stakeholders start to exercise similar behaviour practised by the workgroup despite its appropriateness. The variations found from the two perspectives will be discussed in detail in section 6.2.1.3.

The findings above suggest that stakeholders may be grouped according to the categorisation as depicted by figure 5.2 below. It has been proven that different groups of stakeholders (figure 5.2) develop different perceptions of information value according to the level of which they belong to. PIVs also varies depending whether they are made from the perspective of an individual stakeholder or from the perspective of a workgroup.

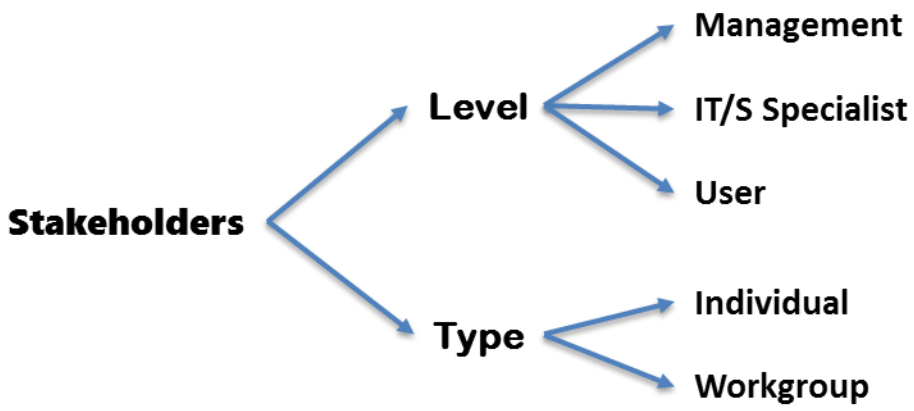


Figure 5.2 Stakeholders' grouping

In other instances, an organisation will make clear statements on the importance of information, so that the information can be appropriately protected. Typically, such statements are explicitly articulated in official documents such as security policies, best practice documents or written instructions as suggested by the following responses:

> **MID-03** *We have a written down instructions that are with the security officer; it includes the guideline on how to handle documents. It is not allowed to bring our its device into office, not even smartphones. This is to reduce virus attacks and to avoid unauthorised movement of data.*
>
> ***PMO-15*** *the protective security manual provides guidelines on different classification of information so we can better protect our information.*

The above responses highlight the processes of espousing the value of information. When any information is given such an explicit and well promoted valuation it will be termed the '*espoused value*'. The espoused value may come in the form of authoritive directive from managers or an IT specialist within an organisation. This value is seen as the standard valuation of that specific information according to the characteristics set by the top management at least. In a public sector setting, the espoused value typically comes from, or is formulated by, the very top management. Espoused values generally consists of the organization's official viewpoint which include documents that describe the organization's values, principles, ethics, and visions (Schein, 1999, p. 17). To a public organisation, the espoused value is what they perceived the actual value of the information they are currently dealing with. Therefore, it is expected that everyone in the organisation will demonstrate security behaviours that commensurate with the espoused value of the information.

Subsequently, the Perceptions of information value based on the espoused value of specific information.

In general, t is expected that the espoused views are communicated in the form of written documents such as information security policy as suggested below:

> **PMO-15** *the government through the ISD office provide all departments with the Protective security manual (PSM) as a guideline on how to work with certain categories of information.*

Indirectly, the mentioned PSM above act as the medium in which the government espouse the value of the information handled in the government organisations. However, there are also other methods found in which value of information may be espoused. Edgar H. Schein (2010) suggested that when a group is first created the prevailing proposal provided by the superior on a particular task may become the valid solution. This notion suggests that espoused views are not restricted to instructions or guidelines laid down in policies alone. In several cases the organisation clear views on information is also communicated through verbal instructions from the like of managers or information security experts in the organisation as suggested by the responses below;

> **PMO-09** *in our department we follow what our boss tells us, he says what is confidential and what's not. We follow his guidelines on how to protect our information.*

> **PMO-12** *from time to time the IT people comes and give us a briefing on the rules and regulation of handling information and remind us on the importance of the information.*

The above responses show examples in which espousing value is one of the processes in the Information value assigning process. They are also strong indicators that the feasibility of espoused value as one of the influencing factors to value assignment and the formulation of stakeholders' information security behaviour intention. Further detailed discussion on espousing information value and views on espoused information values will be presented in section 6.2.1.1.

5.2.3 The Value assigning process

From the responses discussed in the earlier sections, it has become apparent that the value assigned to a particular piece of information by a stakeholder equates to their 'perceptions of information value'. Furthermore, as it is envisaged that 'perceptions of information value' will ultimately have a significant influence on the stakeholders' information security behaviours, it is important to identify the basis on which the valuation is undertaken. This is done by addressing the third sub-objective of objective #1, namely: ***understanding the overall approaches or instances by which stakeholders assign value to information, particular in relation to its protection and security*.** These instances are examples or cases of activities related to information valuation and assignment as experienced and shared by the stakeholders. Most of the value assigning, undertaken by the stakeholders, appears to be performed subconsciously. More specifically, users didn't explicitly refer to the value they assigned to their information as their 'perceptions of information value', rather they implicitly value their information, by associating it with other characteristics, such as importance, sensitivity, confidentiality and cultural norms. The failure to explicitly recognise the value assigning processes could be due to several reasons. First and foremost, stakeholders do not pay much attention to the processes of value assigning as the processes to them are monotonous series of action and are of impulsive actions. Secondly, these processes are most likely to be copied from their peers or seniors.

It has been found that initially, Individual stakeholders may have established their own perceptions of information value (PIV) which is their antecedent perceptions. An antecedent perception of information value (APIV) is a stakeholder's personal or individual perception of the value of the information he or she had at some point prior to the point in time when he / she consciously re-evaluates their perception. Consequently, the APIV might be changed in the information value assignment process. The antecedent PIV of the stakeholders might have been based on their prior perceptions of the sensitivity, confidentiality, and utility of a particular piece of information.

However, after reflecting on a specific situation, or having consulted some formal policy documentation, or asked the advice of other stakeholders, who might have different

perceptions on the importance of that information, then their APIV might be modified. Therefore, there is a revision in the stakeholder's antecedent PIV and the revised PIV now becomes his current PIV. The following response indicates the above point:

> **PMO-11** *before I'm involved with recruitment, I don't see the importance of protecting staff personal information, now I understand the importance and why they need to be protected appropriately.*

These clearly indicate that the PIV assignment has become quite a complex process as it involves more than just the individual perceptions as perceived in the initial interpretive model. The excerpt below advocates the complexity of the PIV's assignment process:

> **MOFAT-01** *if we are not sure, we always ask for our boss for confirmation on the importance of the information, how we should deal with it.*

The above excerpt shows an instance where a superior view on information value is taken into consideration during the stakeholder's information valuation. Similarly, there are cases suggesting that a workgroup's view of the 'perceptions of information value" also plays a role in influencing the stakeholder's information valuation process. For example, a stakeholder who highly value the information she is handling based on her experience in her previous working place has to reevaluate her PIV due to input from her current workgroup's view:

> **MOE-02** *compared to my previous department, people here are more relaxed, they don't highly value their information, many does not follow proper procedure in protecting the information. The information may not be as important here.*

Furthermore, the outcomes of the behaviours of people around the stakeholder as well as the outcome of their own behaviour also have some influence on the information value assignment process.

> **MOFAT-01** *It happened twice; two staff got into trouble because of leaking data. It is a reprimand for all of the staff that the information here is highly confidential. It shows staff that this is wrong (compromising data).*

The above excerpts suggest two points, firstly the outcome of behaviour has some effect on how other stakeholders' view the value of the information. The outcome of the behaviour of the two staff members concerned also motivated stakeholders to re-valuate their own

views on the value of the information they are handling. Secondly, the imposition of a transparent penalty, also has the effect of conferring an 'espoused' value to the particular information in question.

The findings above present several instances in which a stakeholder assigns value to the information when taking into consideration its protection and security. It has also become apparent that the process of information valuation or value assignment is more complex than initially thought and this was not able to be presented sufficiently by the initial interpretive model. Therefore, there is a need to revise the model and explore this process more fully in the phase 2 data collection exercise.

With regards to the research objective RO1, the result obtained under the first research objective not only answers the question as to whether there is the potential for using 'perceptions of information value' in the context of information security, but it also indicated that the 'perceptions of information value' may have a significant role to play in influencing the stakeholders' decision making on what kind of information security behaviour to adopt.

5.2.4 The needs to revise the interpretive model

Due to the findings under the three sub-objectives as presented in the section above, the existing conceptual view on the value assigning process has changed. Referring back to the initial interpretive model (figure 3.2) and the underlying conceptual framework (figure 3.3), it is clear that the initial model is not sufficiently sophisticated to present a clear and comprehensive representation of what is going on within the process of value assignment and the creation of perceptions of information value. Consequently, it has been necessary for the model to be revised and a new model to be developed in order to capture all the insights learned from phase 1 data collection exercise. The new revised model should be able to conceptually portray all the issues, concerns and processes identified during the initial studies. Amongst the findings from the initial studies, the factors that drive the creation of a new revised model are as follow.

- a diversity of views as to what is meant by the term 'perceptions of value', as reported by the stakeholders, called into question the original, rather limited, conceptualization, as presented in the initial model. In the initial model, there were only two concepts of value projected i.e. actual value and perceived value. From the findings, there are four concepts of value which are rooted in the 'perceptions of information value' or PIV. The four value are; PIV, antecedent PIV, workgroup PIV and espoused value;
- the structure of the stakeholder grouping or categorisation proved to be more complex than initially thought. In place of a single view in the earlier model, the revised model should be able to accommodate perspective from both individual and workgroup perspectives. The value assigned to specific information varies amongst different level of stakeholders and between types of stakeholders;
- It is apparent from the instances described by the stakeholders that the process of information value assignments is a complex process. Not only are the individual opinions of the stakeholder's significant, but influences from other perspectives also need to be taken into consideration.
- The overview of the process assigning a value to the information and the creation of a 'perception of information value' as portrayed in the initial model was quite inadequate compared to the new understandings learned during the initial studies. As a result of the findings mentioned above a new revised interpretive model is design and will be presented and discussed in the next section.

5.3 Revised Research Model

This section explains the evolution of the research model, described earlier in this document (Figure 3.2). Changes and improvements to the model are highlighted and justified and an updated conceptual model is presented. The information valuation and assignment process envisaged as described in the initial research model have been subjected to a significant process of reflection and enhancement. What became apparent during the analysis of the first phase data is that there were different lenses through which 'perceptions of information value' are viewed. Additionally, the findings, as discussed in the preceding sections, have enriched our knowledge of the information value assignment processes and their relation to information security behaviours. Therefore, there has been a need to re-appraise and enhance the model accordingly. The revised model, based upon the findings presented in the previous sections, is shown below (Figure 5.3).

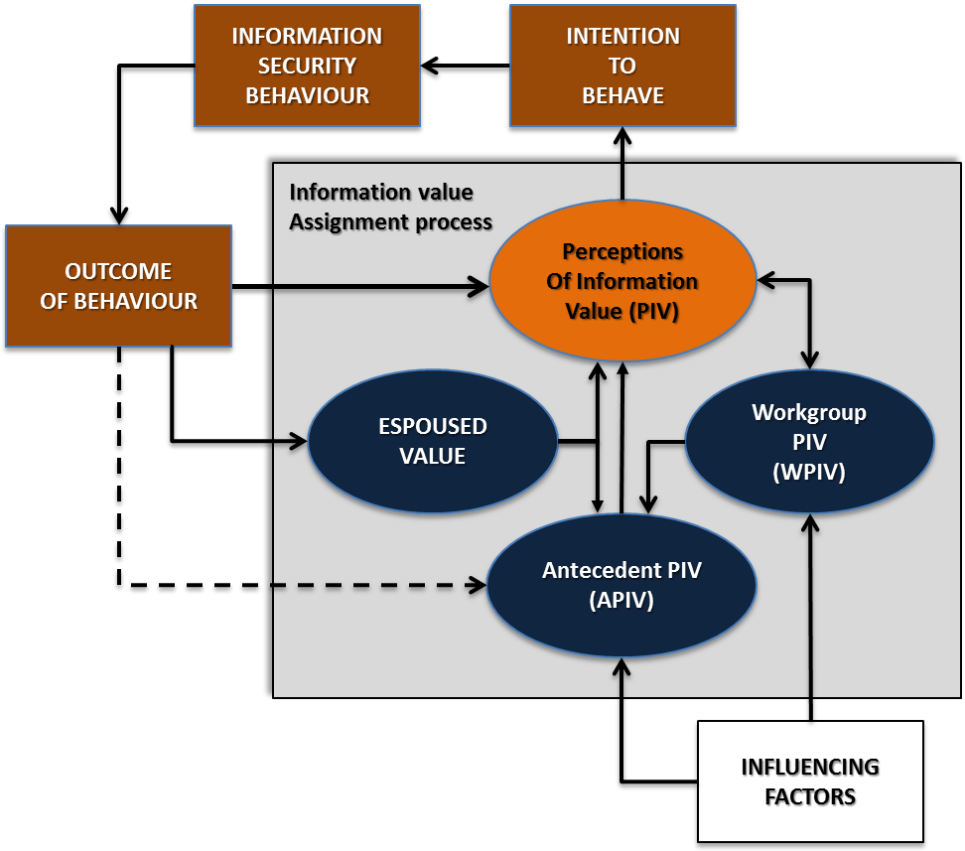


Figure 5.3 The Revised information 'Value assignment process' model

Based on the first phase of data collection it became apparent that the real interest was focused on the central element of the initial research model (Figure 3.2, repeated below for clarity), which represents the concept of the information valuation and information appreciation process, as enacted by stakeholders. Figure 5.3 above reflects the expansion and refinement of this original concept.

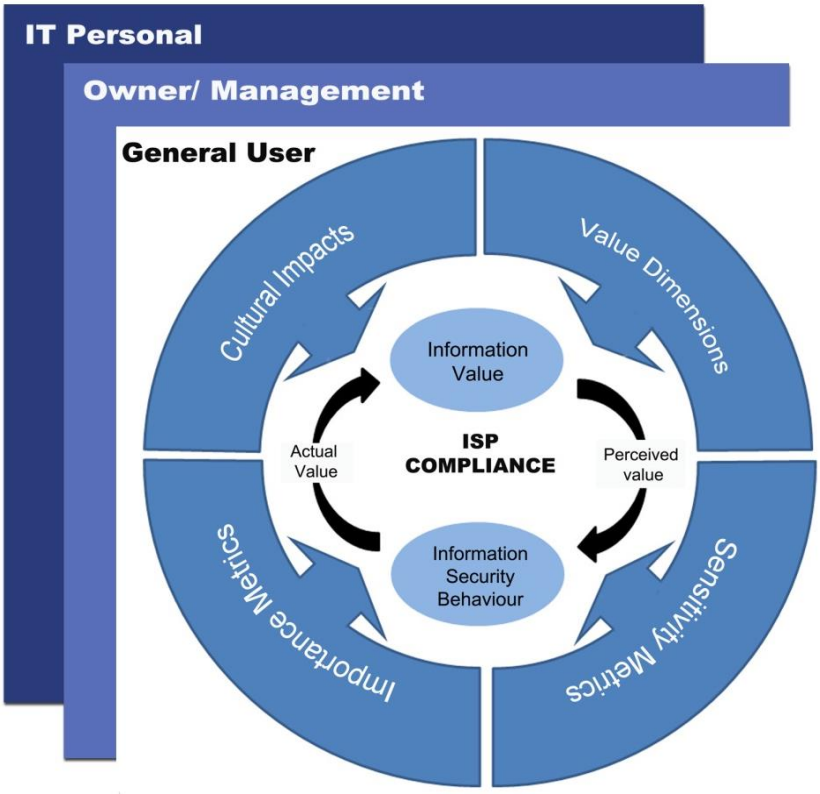


Figure 3.2 the initial research model (repeated from chapter 3 for clarity)

The variables that were around the periphery (figure 3.2) are still perceived to be as important as they were originally. However, since evidence of a wide variety of additional influencing dimensions were found in the first phase data collection, this selection of factors has now simply been entitled 'influencing factors', as represented by the white box (figure 5.3), and these factors will be more fully presented and discussed in chapter 7.

Similarly, the focus on the three stakeholder classes is still valid, although in the revised model it has no longer been explicitly represented, as the revised model is predicated on the assumption that the information assignment process and the resultant security behaviours are all enacted by the three original classes ofstakeholder.

However, the most significant changes that were enacted upon the initial research model to transform it into revised research model can best be articulated in relation to the following three, key elements;

- the revised flow of of the value assignment process;
- the new understanding on the interpretation of 'perceptions of information value', and;
- the formation of information security behaviours.

The following sections, will more fully review the enhancement of the revised model, in relation to these three, key elements.

5.3.1 The flow of the assignment process

In the initial research model, the value assignment process was represented as a one-way clockwise flow. However, upon reflection, it was realised that such a representation did not adequately portray the actual communication and flow of information through the information value assignment process. In hindsight, it was realised that the construction of information flow in the initial model, which was mainly based on the outcome of the literature review, was rather too simplistic. Based on the analysis of the data collected, during the first phase, it became apparent that many of the flows between specific elements of the assignment model are, indeed, bi-directional. Where bi-directional arrows are presented, it means that both the elements have influence over each other. For example, the stakeholders' 'perceptions of information value' may be affected by the host organisations' espoused value, but over time the organisation's espoused value may be reshaped by the stakeholders' 'perceptions of information value' (figure 5.3). This relationship and all the other flows of the process will be described in the next chapter.

5.3.2 Revised interpretations of perceivedvalue of information.

One of the most important new insights that is reflected in the revised model relates to the way in which stakeholders' assign their 'perceptions of information value'. Early indications from the first phase data collected suggest that there are two distinct interpretations of the 'perceptions of information value', namely, 'perceptions of information value' (PIV) which is

value of information perceived from the view of an individual stakeholder, and workgroup 'perceptions of information value' which is 'perceptions of information value', as the synthesis of the collective views of a specific group of stakeholders, working in the organisation (WPIV). In the initial research model (figure 3.2), the perspective of 'perceptions of information value' was restricted to an individual view and the perspective of an individual as a member of a group of stakeholder was also inadequately represented.

Both of these initial interpretations of 'perceptions of information value' are still important, as each has a significant impact on how a stakeholder may choose his or her behaviour towards information security countermeasures. However, in many cases, it was reported by respondents, that these two perspectives are not always in sync with each other; i.e. more often the value perceived from the perspective of an individual stakeholder differs from the value perceived by the group of people around him, or her (workgroup). The excerpts that suggest the above points is presented in section 5.2.2. The differences in the perceptions will provide the stakeholders with a continuum of perceptions. The stakeholder might appraise the range of perceptions before they make any decision on the value they will assign on the information. In other words, the value formulated from the appraisal of perceptions is believed to be a rationalised one taken by the individuals with plausible reasons. This two variations will be known as the stakeholder's PIV to denote the stakeholder individual perceptions and workgroup PIV to denote the work group perceptions (figure 5.3). The mentioned variations of perspectives of PIV will be discussed further in section 6.2.1.4 in the next chapter.

In contrast with the initial research model, additional concepts of value were expressed by particpiants in the first phase data collection. Apart from the two constructs addressing the individual's and the workgroup's perceptions of the value of information, there may be a far more formal and transparent valuation of information, namely the 'espoused value of information'. The espoused value of information is the one that is formally articulated by a senior manager, on behalf of the organisation, and it has been found to be influential in the stakeholder's value assigning process. A brief introduction on espoused value has been presented in section 5.2.2 above and a detail discussion will be presented in section 6.2.1.1 in the next chapter.

Following the first phase data collection, it was also recognised that the individual Information 'perceptions of information value' has two different variants, namely: the 'perceptions of information value' and the antecedent PIV (APIV). As discussed in section 5.2.3 previously a stakeholder's APIV has an important role to play in the information value assignment processes and it has a complex relation with the other concepts of value. The complexity is denoted by the incoming arrows from the other value elements and the influencing factors. These illustrations suggest that an individual's established view of the value of a piece of information [APIV] may change because of the influence of competing perspectives, such as the perceptions of their workgroup or the espoused view of the organisation Changes to the APIV can also be triggered through the influence of their own perceptions based on their own experiences of the information or as a result of the reaction to previous security behaviours or an outcome of a particular behaviour. For example, a stakeholder's perception may change if he / she is made aware that a disciplinary action was taken on a colleague due to negligence in sharing confidential information. As a result of observing this action, the stakeholder might update his/her perceptions of value on similar information. Further, a detailed discussion of the antecedent perceptions of information value is presented in section 6.2.1.3. In figure 5.2, the different types of PIV are illustrated with the oval shapes and will be referred to as value dimensions.

5.3.3 Formation of Information Security Behaviours

In the initial research model, the information security behaviour is conceptually viewed as a single element. Analysis from the first phase data collection revealed that the information security behaviour is made up of several conceptual stages. In the revised framework (figure 5.3,) it is suggested that information security behaviour is initiated with an intention to behave by the stakeholder. It is the stakeholder's intention to behave which may potentially be influenced by the value elements as indicated by the following excerpts.

> **MID-01** *it also depends on one's intention, for us, our intention is to protect the sovereignty of the country. Therefore, our information is of high value. That's why security is important.*
>
> **PMO-15** *AET provision will increase staff good intentions to select appropriate behaviour as they are more capable of handling the security needs.*

Ultimately, a stakeholder's information security behaviour may have some organisational outcome associated with it; a good behaviour may be rewarded and an inappropriate behaviour may be penalised. The outcome of behaviour, whatever it might be, may affect how the stakeholders view the information. Furthermore, when an inappropriate behaviour, fails to trigger a suitable penalty, then it may be interpreted that the information is less valued. The excerpt below supports this notion:

> **MOH-02** *Despite some non-compliance behaviours, no one, has been penalised or reprimanded. Maybe they think the information is not that important to be protected.*

To reflect these ideas, in the revised model, the originial, single information security behaviour is now represented by the three brown boxes namely, intention to behave, information security behaviour and outcome of behaviour.Therefore, it was important to explore this notion more fully in the phase 2 data collection exercise. More specifically, a fuller discussion of information security behaviour is presented under section 6.2.2.

To conclude,the revised framework now explicitly reflects the idea that the *stakeholders' 'perceptions of information value' has a significant role in determining their intention to behave* and subsequently their selection of behaviour towards information security issues. The framework also more fully represents the processes that have been found to occur during the 'perceptions of information value' assignment process (shaded box). This process is called the information value assignment process. The model also illustrates the existence of complex relationships within the value elements as well as a relationship between the value elements and the information security behaviours. To more fully understand these complex relationships, the framework will be further explored and validated using the insights gained from the phase 2 data collection exercise.

5.4 Concluding remarks

The chapter has mainly discussed one of the major findings of the research i.e. to ***understand the extent to which stakeholders develop clear 'perceptions of information value', and the processes by which they assign value to the information that they handle***. In a way, this chapter has provided strong evidence for the existence of references made to 'perceptions of information value' of information by stakeholders. The findings that were reported in this chapter are summarised below;

i Reference to 'perceptions of information value' is in existence in the context of information, information valuation and information security.

ii The formulation of a 'perceptions of information value' of information is through a process of information value assignment by the stakeholders that will be discussed further in chapter 6.

iii The process of value assignment is influenced by several factors that help determine the range of value of the information. Detail discussion on the factors identified will be presented in chapter 7.

iv The 'perceptions of information value' of information by the stakeholders generate influences on the behavioural intention of the stakeholders towards information security countermeasures.

Furthermore, this chapter has also introduced some discussion on the second major finding i.e. the information value assignment processes which help to set the scene for a more detailed discussion in the subsequent analysis chapters, i.e. chapter 6 and chapter 7.

6. PIV and Information Security Behaviours

6.1 Introduction

This chapter starts by revisiting and validating the revised view of the information value assignment processes as portrayed in the conceptual model (figure 5.3). The validation is based primarily on the results of the second phase data collection exercise. However, having revisited the information value assignment process, the bulk of this chapter will then focus on addressing Research Objective 2. Therefore, this chapter is divided into two main parts. The first part presents a richer description and validation of the revised value assignment process.. These value elements are the essential components of the 'value assignment processes' that helps in determining the stakeholders' 'perceptions of information value'. Meanwhile, the second part of this chapter will continue to present the findings with specific reference to the second research objective. The second objective of this research aims to *explore and understand the relationship between stakeholders' 'perceptions of 'information value' and their resultant 'information security behaviours'*. In particular, this part of the chapter will provide a detailed exploration of each of the three sub-objectives of research objective 2, as originally presented in section 3.6 in chapter three of this thesis. It is important to note that as well as being important research issues in their own right, each of these three sub-objectives also relates to an, as yet unexplored, element of the interpretive research framework (figure 5.3). This section ends with concluding remarks.

6.2 Revised view of the assignment processes

After the analysis of the 2nd phase data collection had been undertaken, some new insights on the value assigning process were gained, particularly in regard to the different lenses through which stakeholders may make interpretations about the value of their information. These various ways of perceiving information value, when analysed, fit into four main categories, which are referred as the 'value elements' (section 5.2.1). The four categories are espoused value, antecedent PIV, workgroup's PIV and PIV.

There are several characteristics identified regarding the value elements;

i. The value elements represent different categories of value perceptions, and they apply to all types of stakeholders.
ii. The value elements are perceived at different stages of the process.

The value elements are represented by the blue and orange ovals in figure 6.1 below. The next sections present and discuss in further details how these value elements are constructed and derived.

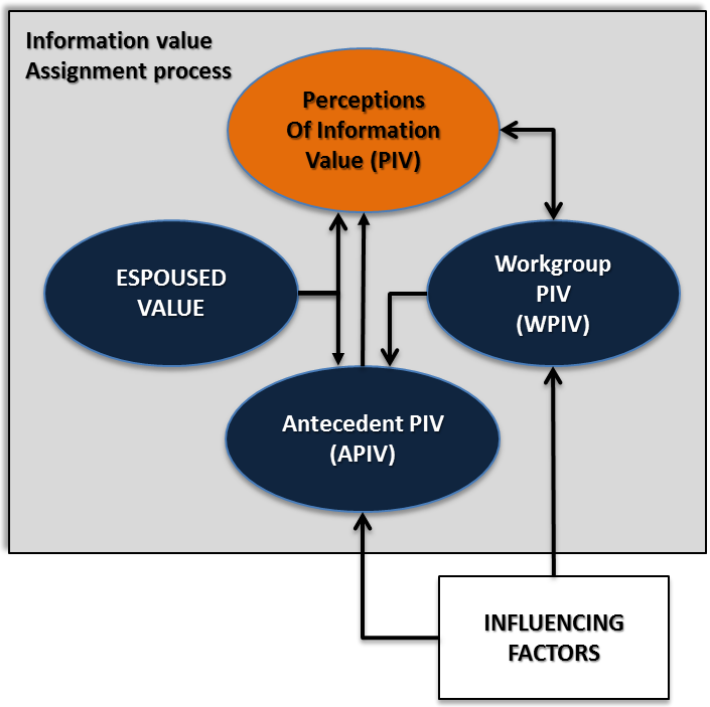


Figure 6.1 The value elements in the information value assignment process

6.2.1 Information Value elements

6.2.1.1 Espoused value of Information

One of the value concepts depicted in figure 6.1 is the espoused value. They are several variations of how a value may be espoused to the stakeholders as discussed in section 5.2.2 and section 5.3.3 in the previous chapter. Largely, It was found that the espoused value of information does have some effect on the stakeholders' information value process and PIV regardless of the medium in which the value of information is espoused. Further evidence was obtained from the 2nd phase of data collection to support the above findings which are shown in the following excerpts:

> **MOE-04** *through the written guidelines we know how to value our information, we can be more organised and manage our information better.*
>
> **MOFAT-01** *we have guideline book describing the classification of information in our work. It shows us why certain information is more important than other.*
>
> **MOHA-02** *a proper policy would make our work a lot easier. Then everyone will know what information can be shared and what are confidential.*

The above responses clearly indicate that espoused value by the organisation can help stakeholders to valuate appropriately the information that they have.

The espoused value is PIV articulated widely to a wider audience through the different medium of communication such as policy documents, emails or may be communicated in meetings that stress the importance or value of a specific piece of information. Espoused value is a shared understanding of the value of information that is communicated to everyone or a significant number of people. The following responses show how managers in two ministries espouse the value of information to their users and staff:

> **MOEHI-01** *We inform our users on the importance of protecting information during a briefing during their Ta'aruf (Orientation) Week for students and through KUPU SB official website.*
>
> **MOHA-05** *We used e-mail and our internet portal to inform our staff on issues of the security of information.*

The following responses from the user level stakeholders support the above point of how PIV in an organisation is being espoused to a significant audience:

> **PMO-08** *on the security of information, we rely so much on our boss. He tells us what is important and what is not.*
>
> **MOC-02** *we are given briefing on how to treat information in this department by our superior*

Additionally, it also provides guidelines on how a stakeholder should treat the information. Although there is no indication of negativity regarding espoused value by the stakeholders, any initiative in espousing value must be made clearly and concisely. Moreover, the documents in which the value is espoused must be made known and accessible to stakeholders for it to make impacts. The above-mentioned points are expressed in the following responses:

> **MID-01** *it is important to have the policy document accessible so that staff can read and understand it for example on how to properly handle information, this will avoid them from guessing.*
>
> **MOC-02** *some policies does not clearly define what has to be done. We have two different policies and some of the contents are different.*
>
> **PMO-05** *the PSM is general, and it up to the interpretation of each of the HOD, this might not be ideal for some staff. Some may not be that literate in this area.*

It is typical for a department or section to be entrusted for the formulation of the organisations' espoused value. In the case of Brunei Darussalam, the development of the espoused value for government ministries, departments and units are carried out by the Information Security Department at the Prime Minister Office. Additionally, information value is also espoused through another form of unofficial written documents as well as verbal instructions from the managers or IT specialist.

Furthermore, several responses from the stakeholders suggest that the provisions of information countermeasures by the organisation may also be seen as an act of 'espousing' the value of information from the perspective of the stakeholders. To them, a provision and implementation of information security countermeasures signify that the organisation highly value their information.

> **PMO-15** *the public key infrastructure (PKI) project signifies that the information we are handling is sensitive, confidential thus it is necessary to be protective.*
>
> ***MOHA-02-02*** *after the incident, the policy has changed, we are not allowed to bring in any smartphone anymore, and this is to avoid sharing of sensitive and confidential information.*

Consequently, the absence of countermeasures, to the stakeholders, might signify that the organisation is not that serious regarding the security of the information they are handling. Indirectly, this may also mean that the information may not have significant value to the organisation.

> **PMO-08** *I don't recall if there is any policy on information security, maybe we don't handle valuable information.*

It is also found out that in some instances, the **espoused value** may fail to convey the value of the information to the stakeholders. There are several reasons shared by the stakeholders of why espoused value might be ignored. Some stakeholders think that the espoused value is not addressed to the right people. Some user's level stakeholders may not understand the content of the policy. The following responses suggest the above-mentioned notions:

MID-2-01 *What the information meant to the organisation were not properly related or made known to staff. Most of the time, the information policy is left to the head of units or departments to translate and most of the time it is not entirely understood.*

PMO-2-01 *There is indication given, but it is an only indication. Not exactly how accurate information is to be handled, it is a grey area.*

MOHA-2-01 *The value of information or how the value should be derived is not explicitly specified. It is not clear who should do it.*

Due to the unclarity of the instructions, stakeholders might take the easiest way out i.e. to ignore the espoused instructions.

6.2.1.2 Workgroup perceptions of information value

Another type of 'value' identified from the research is the Workgroup 'perceptions of information value' (section 5.3.2). The workgroup perceptions of information value must not be mistaken with the previously discussed espoused value. Workgroup perception of information value (PIV) is the value perceived on specific information which is collectively accepted in a group of stakeholders. The workgroup PIV might originate from the PIV of an individual stakeholder, lobbied to be accepted by other stakeholders. Over time, this value is agreed to by all or majority and it may become the de facto value of particular information. Therefore, a workgroup PIV is a value that a stakeholder believed other stakeholders assign or agree on a particular piece of information. The workgroup PIV might be expressed by other stakeholders directly or value that is perceived based on interpretations of the behaviour of the other stakeholders.

Although the workgroup value is similarly derived from instructions of others and usually it is learned from someone who is superior to the stakeholder as with the previously mentioned espoused value, the espoused value is considered to be the official views whereas the workgroup perceptions of information value is a more commonly accepted value. More often, a workgroup PIV is more intimately acquired for example when a stakeholder seeks the advice from his superior or other members of his group on how to treat a piece of information. This is in contrast with the dissemination of espoused value which typically targets wider number of audience.

> **MOE-03** *If I'm in doubt I'll ask my superior for guidelines, I just follow what they tell me. So I know which information is important.*

Another point that differentiates the two values is that a workgroup value may not be equal to a value espoused by the organisation, as the workgroup value is mainly created from the perspective of the members of the group. The workgroup's PIV, although might not be in-sync with the organisation's espoused value, may be the mutual de facto of the value for that specific information by the workgroup. The following quote presents an example that suggests other people perceptions (Workgroup's PIV) from the perspective of a stakeholder, does matter. For example, to avoid being ignored by other stakeholders, they have to follow

what is commonly considered as acceptable by the group although the PIV may go against his or her PIV or APIV.

> **MOHA-01** *you cannot say no. People will hate you. Why do I have to share, this is not right… so people will hate you for that. So, in a way, in the person mentality, "oh no. This cannot be it, people will dislike me. I do not want that… So, that is the mindset of people*

The impulse of being accepted by the community is also another influential factor to the valuation process. The expectation that other stakeholders possess commended characteristics will help stakeholders to cultivate a compliant attitude. In a reverse impact scenario, due to the expectation of others a stakeholder may develop and display appropriate attitude and actions and in return others will see these actions and reactions as taking protective measures and perceived that the information dealt with is in need of the appropriate protection. This in return may raise the value of the information.

> **PMO-17** *To be seen as trustworthy, for me, I keep the information safe, like so that people can trust me.*

Likewise, the workgroup perception of information value is also prone to be influenced by the perceptions of information value of an individual stakeholder.

6.2.1.3 Antecedent perceptions of information value

The antecedent PIV has been briefly introduced in the previous chapter under section 5.3.3. Succeedingly, more evidenced will be explained to justify its role in the value assignment process. It is found that an APIV value is susceptible to intrinsic or extrinsic factors that are personal to the stakeholder. It is also affected by what the individual knows about the information he or she is handling. Knowledge about the information may include; how important it is to him or her personally and what function does the information serves. Benefits expected from protecting the information and the consequences faced if protection of the information is defied also considered as knowledge about the information. It is assumed, and as suggested by (Bell, 1999), that humans act rationally and need reasons to perceive reality adequately. Hypothetically this means that stakeholders will as an individual or as a group of people evaluate reality and plan their actions accordingly. The following excerpts from the interviews present evidence in support of the statements stated

above. Each one of the following quotes also indicates the APIV as described by the stakeholders at the moment of time:

> **MOF-01** *the budget for example since I'm holding the budget (approving budget allocation) for me it's very sensitive and confidential. If there are information leaks, people can manipulate it. Moreover, misused them.*
>
> **MOE-01** *for us the protection of students and staff information is our priority; it may look trivial for others, but this information can be manipulated by attackers and cause unwanted consequences.*
>
> **MID-02** *the Navy teaches us the value of information before we took it for granted but now we understand that a lot of information is confidential and need to be secured.*

As mentioned in section 5.2.3 the APIV of stakeholders evolves. An indication of such changes is supported by the above respond from stakeholder MID-02 indicating changes in his view towards the value of certain information before and after joining his workgroup. Another example of an APIV would be, where a stakeholder that has just been transferred from one organisation to another will have a pre-existing perception of the value of information which was influenced by the environment and context of his former group. Following a period in which he or she can observe, learn and make judgments with respect to the setting of his or her new environment, the stakeholder will be able to rethink and reappraise his or her perceptions of the value of their information. At this stage, the reappraised stakeholder's 'perceptions of information value' will become his or her 'perceptions of information value'.

The following respond further suggests that perceptions of information value in some cases have to be revised to be able to work in harmony with others:

> **MOD-05** *in my previous workplace, security on information is quite tight. Here, it is more laid back; a lot of staff does not care. This is how it works here; you've just had to follow suit.*

An APIV may also change periodically, for example, as and when they handle the information, once the information is beyond their dominion and their responsibility they have less value on the information. For example, in the case of a stakeholder who manages the annual budget of an organisation, information on the budget will be highly appreciated

and highly protected during budget process but may be less valued when the budget processing is done. Evidence to this notion are; where stakeholders based their valuation on the importance of the information to their work and where they are held accountable for the information.

> **PMO-02** *when the information is within my jurisdiction, I will make sure that it is protected but I don't know if it's then going to be another person responsibility, it is then their responsibility to look after it.*
>
> **MID-03** *some staff will only consider the information relevant if they are directly responsible for it, or it has importance to their work. Otherwise, they won't care much.*

Undoubtedly, in some cases, the APIV of a stakeholder may remain unchanged in spite acquiring new knowledge on the information. On the other hand, it is realised in some cases, revision of PIV does not happen in spite acquiring new knowledge on the information or not acquiring any new knowledge for that matter. For example, a stakeholder who has established an APIV on a payroll information will stick to his PIV if he does not acquire new knowledge related to the payroll's information he is handling. The responses below shows example where a stakeholder's PIV does not change despite learning new information or otherwise:

> **MOD-03** *some of the information I handle is sensitive and confidential, I believe I give them appropriate protection as no one advise me otherwise.*
>
> **MOHA-02** *I ignore what people think and say about approaches, for me I know what I'm doing and I'm going to stick with it (clear desk).*

6.2.1.4 Perceptions of information value

As mentioned in section 5.2.3, stakeholders' PIVs can be categorised into antecedent PIV and the actual PIV. The stakeholder's perception of information value is a stakeholder's ***rationalised*** opinion of the value of the information he or she is handling (using, storing or communicating). The perception of information value is the result of the process of value assignment made by the stakeholders. As depicted in figure 5.3, a perception of information value is formed from the rationalisation of information fed by various value elements. Specifically, the perception of information value may be influenced by the stakeholder's antecedent PIV; his or her workgroup's PIV as well as the presence of any value that has

been explicitly espoused by their organisation. The stakeholder's PIV may also be affected by the outcomes of behaviour displayed by their community. On completion of the process, the PIV will become the antecedent perceptions of information value (denoted by the bidirectional arrows in the diagram).

In some cases, the WPIV value might surpass their APIV. Therefore, in some cases, the behaviour of their superior may be seen as dictating how the information should be evaluated. The following response shows that, to the stakeholder, performing unacceptable behaviours is acceptable because their superior is doing the same.

> **MOH-01** *if we are discussing with the patient's family, for example, some doctors will blurt out confidential information to family members.*

Apart from depending on other's perspectives, stakeholders are also influenced by how they perceived others expected them to behave;

> **PMO-17** *To be seen as trustworthy, for me, I keep the information safe, like so that people can trust me.*

> ***MOFAT-01*** *I think, regarding personal, like, how you do things and get recognise. Regarding self-satisfaction, you get the job done in the best way that you can do. It is like, okay, this is the best thing I can do, and my boss is satisfied with my work.*

> **PMO-22** *Disciplinary action should be taken if we are not responsible, then people will take it seriously, sometimes government servants just take it for granted.*

Another finding indicates that the APIV at times does not help much in improving a stakeholder's PIV. An example of this is a situation where the stakeholder felt that the countermeasures installed for the information; added on to his or her workloads, he or she does not have the self-efficacy in using the countermeasures and where the stakeholders do not see the reason behind the introduction of the countermeasure.

> **MOF-01** *We need to use the token to encrypt our data before sending any e-mail, but I have a problem activating it most of the time it gives me errors. So I stop using it.*

> **PMO-2-1** *We have given them instruction to use them but they are reluctant.. they say that the token is ugly they have to carry the token every way….*

Furthermore, other factors such as hierarchical priorities in which people with authority can get access to information without being question are common. The issue mentioned above relates to the characteristic of power distance index (PDI) in the nation cultural traits (Appendix B) which stipulates that in a country that scores high in their PDI, the hierarchical order is well accepted, everybody has a place, which needs no further justification.

> **MOHA-07** *sharing confidential information cannot be done. It considered sensitive.... but if the officer wants to read them then we have to give it to them*

As depicted in the model in (figure 6.1) the value elements, antecedent perceptions of information value and the workgroup perceptions of information value are also influenced by several influencing factors. Evidently, from the literature, there are numerous factors that can affect how a stakeholder chooses to behave in the context of information security. The influencing factors indicated in the model were sourced not only from the literature but also most importantly, from the perspective of the survey participants. In fact, the factors mentioned in the interviews were found to have more significant impacts on their value assigning processes. These factors cover the dimensions of value based on importance, cultural influence, altruistic, social and sensitivity as mentioned in the investigative framework in chapter 3 of this thesis.

Overall the model suggests that the process of information value assigning is iterative and each of the value elements depends on the outcomes of the other value elements. The flow of cycle in the model suggests that over time with the right level of strong influences and appropriate motivation an appropriate value can be assigned to the information. In turn, the assigned value will result in more positive behaviours that are conforming to the organisation's information security countermeasures.

6.2.2 Information Security Behavior elements

The revised conceptual framework (figure 5.3), illustrated three elements of behaviour that are an intention to behave, information security behaviour and the outcome of behaviour. The intention is one's plan on how to achieve or how to do something, a personal statement on their determination to perform an act from the information security perspective. In the context of behaviour, an intention to behave is the course of action a stakeholder (for

instance) plans to take on a specific issue. For example, a stakeholder plans to or has the intention to display compliance behaviour towards information security countermeasures implemented in his office. In general, behaviour is defined as the way in which one acts or conducts oneself, especially towards others or specific issues or in a specific environment. Specifically in the information security dimension, information security behaviour describes the actions of stakeholders that relates to information security protection and particularly conducts towards countermeasures laid down to ensure the security of information.

Typically, a behaviour starts with an intention to perform the behaviour i.e. '*intention to behave'*, than only the intention may be translated into an actual behaviour, which in this context the '*information security behaviour'*. Once the behaviour is executed, there will be an 'outcome *of behaviour' to it. An outcome of behaviour* is the consequences faced by the stakeholder as a result of choosing and executing that specific behaviour. For an example, an expected behaviour towards 'a clean desk policy' would be keeping one's desk clean, storing away all-important documents and locking the PC or shutting them down if away from the desk. It may be common for some stakeholders to practice the behaviour above but because of certain beliefs and issues, for some stakeholders, this behaviour may go against their norm. Therefore, there are two resultants of behaviour from the 'clear desk policy' example, a behaviour conforming to the policy and behaviour that is not conforming to the policy. An outcome of the clear desk behaviour is a reward or acknowledgement for adopting clear desk behaviour and a reprimand or penalty for a non-clear desk behaviour.

Typically, every organisation has a set of information security policy or at the least a framework or some guidelines to be followed, when addressing information security issues. An information security policy lists down the do's and doesn't advocate by the organisation for its members to adhere to. This aims to achieve and maintain a desired level of protection on their information. The policy is a working document that provides guidance on the 'means' of information security management, as well as the desired ends (Stahl et al., 2012). A similar notion is expressed in the response from the stakeholders below:

> **PMO-05** *the Protective Security Manual (PSM) is intended to provide indirectly instructions to staff on how to treat information and how to react to situations that involve information security and protection.*

> **PMO-15** *the government has initiated a protective security manual, which is given to information security officers appointed in every government ministries and departments. The PSM is an abstract from BS9997 and ISO27001; the ISO need to extract the information and develop a policy for the use of their office.*

This view is also in line with the aim of introducing information security policy as suggested by Doherty et al. (2009), which is to safeguard proactively the availability and integrity of information resources. Indirectly, the organisation is initiating the value of the information under their jurisdiction by providing their stakeholder's guidelines for their information security behaviour. Unfortunately, in some cases, despite the intention of the organisation, the set of behaviour displayed by the stakeholders may not match the outlined behaviours. Despite this reported initiative and the launch of the protective security manual, many stakeholders at the user level express their unawareness on the existence of such guideline. There is a contrast between the owner level stakeholders beliefs and the expression made by the lower stakeholders. Findings from the data show that there is little evidence that appropriate information security behaviour guidelines are available to the stakeholders:

> **MCYS-01** *so far I have never come across any written policy stating what to do and what not to do. So in general if we provide staff with new PC, we only give them verbal instructions and advice on how to work securely, but there is no written policy.*
>
> **MOD-01** *I think there is a written document on the policy on information security with the security officer but I have not read it. But I think it should be around, the guidelines on how to handle these documents.*
>
> **MOE-12** *I'm not sure if there is any policy or guideline on information, there might be one, I'm sure there is one but I don't know about it.*

As a result, these inconsistencies (availability and awareness) of the information security policy would create misunderstanding and misconceptions of what the acceptable behaviours are. For an example, if a stakeholder is not aware of the existence of an information security policy he or she might create a perception that security of information is not a main priority of the organisation. Furthermore, not having a guideline on how to react to situations involving information security may leave the stakeholders in the dark and not knowing how to appropriately react to the situations. This can lead to bad consequences to both the stakeholder as well as the organisation.

6.3 Stakeholders' PIV and their Information Security Behaviour

This section will present the findings on a question that is the primary driver of this research, i.e. the relationship between PIV and information security behaviours. The analysis of the data suggests that the stakeholders' 'perceived information value' and their information security behaviour have some relationships. The relationship between the information security behaviour and the stakeholders' perceptions of information value is pivotal to the whole process of improving information security compliance. Fundamentally, both information security behaviour variable and the PIV influence each other in an iterative loop. The idea is that high PIV will encourage better intention and subsequently will produce better information security behaviour. On the other hand, good information security behaviour will have a good outcome of behaviour and (as mentioned in the previous section) will have a significant influence on the stakeholders' PIV. This relationship suggests that the higher the PIV by stakeholders on a particular information, the more encouraged they are to perform or exercise appropriate information security behaviour. One slight change found regarding the above assumption is that the influence of PIV over information security behaviour is not a direct one. Instead, it is mediated through the intention of behaviour. Therefore, in theory, the PIV of a stakeholder determines his or her intention to behave (figure 6.1) and subsequently, the intention will turn into an action or a real behaviour. The model of the processes that is represented in figure 6.2 which is a subsection of the revised conceptual model (figure 5.3) will be used to test the research objective 2 which is to ***explore and understand the relationship between stakeholders' 'perceptions of 'information value' and their resultant 'information security behaviours'.*** The following subsections will present the three sub-objectives design for RO2 of the research.

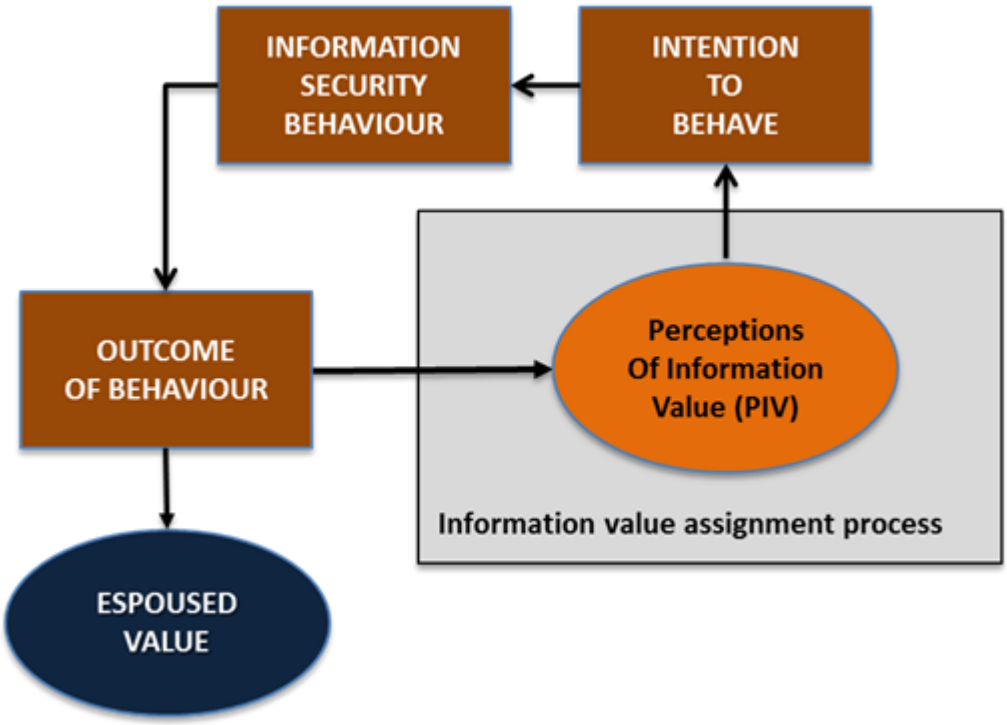


Figure 6.2 the relationship between 'Perceptions of information value' and the information security behaviour variables

6.3.1 Intention to comply, mediating influence of PIV

The Following discussion presents the findings of the research, based on the first sub-objective of RO2 that is to explore whether there is a ***relationship between stakeholders' 'perceptions of 'information value' and their resultant 'information security behaviours, and the extent to which this is mediated through 'intention to comply''***.

It is found that the stakeholder's intention to behave becomes the mediator between his PIV and his information security behaviours. As underlined by many social-cognitive theories used in Information Science and information security research, intention to behave potentially predicts the actual course of behaviour taken. Fishbein & Ajzen (2011) suggests that intention to behave is the best predictor of actual behaviour. According to them, the intention is the cognitive representation of a person's readiness to perform a given behaviour, and it is considered to be the immediate antecedent of behaviour. Individual intention to perform a given behaviour is central to their proposed theory of planned behaviour. Intentions are assumed to capture the motivational factors that influence

behaviour; they are indications of how hard people are willing to try, of how much of an effort they are planning to exert, to perform the behaviour (Ajzen, 1991). It is also predicted that a strong intention to perform a particular behaviour will result in a higher likeliness of performing that behaviour.

However, intention does not always translate into the actual behaviour due to perceived or actual obstacles in exercising the actual behaviour (Burns et al., 2012). Burns et al. (2012) postulate that for the intention to turn into an actual behaviour, it goes through three different stages. Each of the stages will have some factors that influence the intensity of the intention. These factors may include perceptions of their readiness to perform the action, other people expectations as well as the conduciveness of the environment there are in. Furthermore, and more importantly according to (Burns et al., 2012) the stronger their intention to behave the better the position they are in performing the actual behaviour. In the context of information security, it is postulated that the more intense the intention is, the better the chances for it to be translated into an actual behaviour. The Following excerpts from the interviews suggest that intention plays important roles in determining the actual behaviour of the stakeholders:

> **PMO-06** *It depends on a lot of the intention of the person; if his intention is to protect the information, then he will surely try his best to provide protection to the information.*

> **MOC-03** *Our religion teaches us to get our intention right; then you can do the right things. If you have the right intention to follow the rules and protect the information than you will follow the rules.*

Subsequently, it is also proven that post-cognitive appraisal of factors significant to an information security issue would help to formulate stakeholder's intention on how to react on the issue. Specifically, upon the creation of PIV on specific, a stakeholder would have decided and plan how they would react towards an information security problem, for example, complying with an information security countermeasure.

> **MOHA-04** *I think I would have a better intention towards the protection of the information I'm handling if I have the knowledge on what to secure and how to do it (protection).*

The above responses clearly indicate that the relationship of influence between a stakeholder's PIV and his or her behaviour are mediated through their intention. Therefore, encouraging stakeholders to have a good intention towards information protection would encourage the formation of acceptable and appropriate behaviours from the stakeholders. This finding is of particular importance, as this will provide an alternative perspective from which an organisation be able to encourage and manipulate stakeholders' intentions through motivational gatherings.

6.3.2 Influence of other stakeholders' behaviour

One of the sub-objective created to support RO2 is to ***explore and understand whether the stakeholders' PIV is affected by other stakeholders' information security behaviours***. Similar, to the finding on the influence of other stakeholders' PIV, it was envisaged that other stakeholders' information security behaviours would also be influential. It is evidenced from the interviews that other stakeholders' information security behaviour do have some influence on the stakeholder PIV. For example, in cases where a stakeholder is new to the environment or he or she is only making rational judgement occasionally, other stakeholder behaviours are an excellent source of reference. These behaviours may indicate the acceptable ways to treat information in that particular environment or community. Another source of reference would be the outcome of the behaviours, in this sub-objective particular interest is the outcome of the behaviour of other stakeholders.

It is one of the findings of this research that the outcome of behaviour produces some substantial impacts on the stakeholder's PIV. The influential nature of the outcome of behaviours has been briefly discussed in the previous chapter under section 5.3.4. It is believed that the behaviour displayed by other stakeholders represent their PIV of the information they are handling. The outcome of behaviour relates to the resultant implications of particular information security behaviour. For example, a user doesn't use a virus checker and then gets into trouble because he corrupts all his information, or, a user realises some unprotected information is valuable and is praised by the boss for adding some password protection. When an outcome of information security behaviour is perceived to be negative, for example, if a stakeholder is reprimanded or penalised other

stakeholders are expected to make a lesson out of the incident. This relationship is made clear by the diagram in figure 6.2. In supporting the above-mentioned relationship, the following excerpt shows that the outcome of behaviour is seen to have significant influence on how a stakeholder perceived other's valuation of the information;

> **PMO-02** *I have not seen or heard of any people penalised for information security breach, I have heard about people reprimanded for coming late to work and other disciplinary matters. We must be doing well in term of the information security.*

In the above excerpt, the stakeholder assumed that how they deal with the information should be correct and acceptable. Otherwise, they should have been reprimanded.

> **MID-04** *the prosecution of the perpetrator changes how staff treat information. We have had improved compliance with countermeasures than before.*

The above extracts reinforce the claim on the significant of the outcome of behaviour. In most of the cases, the outcome of behaviour is made as an example or as a measuring stick on how specific information is valued. It is also found that that the outcome of behaviour also has the influence that can result in changes made to the *espoused value* and therefore will indirectly influence the PIV of the stakeholders. (The relationship of information espoused value and stakeholder's PIV is discussed in section 5.2.2).

> **MOHA-03-1** *due to the incidents, only director-level officers are allowed to initial important documents.*

Another participant suggests another example of how the outcome of behaviour has influence on the espoused value, as stated below:

> **MID-03-01** *after the information leak on social media, the importance of some information is stressed and only authorised personnel were allowed to carry smartphones while on duty.*

Another issue that may arise is when a stakeholder executes a behaviour that is not necessarily reflecting his PIV on the information but based on other stakeholder's behaviour and views. An example of this case is where a stakeholder chooses his behaviour to align with the norm of his workgroup instead of his PIV. In cases such as this, although the

stakeholder performs similar behaviour with the rest of the group, it may not reflect or change his antecedent PIV. Albeit, it is not impossible for a stakeholder to revise his PIV based on the behaviour of the group. The above notion is expressed by the following response from one of the stakeholders:

> **MOH-02** *the doctor talks about the confidential patient information with placement students and others. This information is considered confidential but I guess it's ok since some of the doctors does it.*

The excerpt indicates that, although the stakeholder realises that they are dealing with confidential information, it was not reflected in the behaviour of his superior. Therefore, he might adopt the same behaviour although he still believes that the information is still confidential. It would be devastating if the stakeholder would revise his PIV to accommodate the behaviour of his superior. Below are some responses from other stakeholders that reflect a similar mindset:

> **MOE-02** *Its different from my previous office, here it is more relax, Info-security is not a priority.*
>
> **PMO-14** *I don't usually do it, but here everyone does it, information is treated with the highest importance. (Referring to clean desk policy)*

The above responses have made it clear that the outcome of behaviour does have an impact on the-the value espoused by the organisation; changes the expected information security behaviour and encourage stakeholders to review their PIV on certain information. The examples presented above, provide ample evidence that the outcome of behaviour (as a resultant of other stakeholders' behaviours) does have an impact on a stakeholder's PIV. This evidence, therefore also provide validation on the relationship of a stakeholder's PIV with other stakeholders' Information Security Behaviours.

6.3.3 Influence of stakeholder owns behaviour

The previous section has presented findings that address the second sub-objective of RO2. This section will discuss the findings from the third sub-objectives of RO2, which is ***to explore and understand how a stakeholder' 'perceptions of information value' is affected by the results of their own 'information security behaviours***.

If a stakeholder believes that the information he is handling has a high PIV, then they are more willing to comply with the countermeasures implemented. The following respond from a stakeholder who earlier in the interview expressed that he has a high PIV on the information he is handling believes that their behaviour (in the department) are appropriate because no one has been reprimanded for doing something inappropriate:

> **MOC04** *None of us have been reprimanded on matters relating to Info-security, I guess we are doing what's appropriate in term of information security.*

The responses above clearly indicate that the outcome of a stakeholder's own behaviour could affect his own 'perception of information value'. This could be a conformation on the PIV he or she assigned on the information. Subsequently, it also validates that their information security behaviours are conforming to the expectation of the organisations. In the above particular case, there is no outcome of behaviour stated and to the stakeholder, this suggests that his information security behaviour is appropriated and accepted. If his behaviour is not acceptable, he would have been reprimanded.

Although this kind of relationship is beneficial in terms of strengthening the beliefs of the stakeholders, it can also raise the issue of fault assumptions on the right way to behave. A stakeholder perceived that if there has never been any penalty or reprimanding happened, therefore, they assume that their behaviours are correct and acceptable. This may not be all true; their behaviours might not be appropriate but there could be no monitoring procedure installed making it impossible to catch the bad behaviour or they might not be aware of what sort of behaviour is acceptable. As mentioned in the previous section, where there is no policy available it is difficult for the stakeholders to judge what kind of value are espoused by the organisations and what kind of behaviours are acceptable.

6.4 Concluding remarks

In conclusion, this chapter has presented the processes of information value assignment, as the stakeholders experience it. Furthermore, it has provided a richer picture and validation of each of the various value elements and information security behaviour variables that make up the overall process. Overall, the presentations and justifications made in this chapter have contributed to the better understanding of the role of perceptions of information value in information security compliance behaviour. A more concrete achievement was a detailed understanding of the process of information value assignment by the stakeholders. The insights reported in this chapter can potentially be used to enhance, motivate and change behaviours towards information security issues.

More importantly, this chapter demonstrates that there is an important relationship between stakeholders' 'perceptions of 'information value' and their resultant 'information security behaviours'. The relationship defines that the value assigned by the stakeholders have indirect impacts on the information security behaviour mediated through 'the intention to behave' of the stakeholders. This relationship indicates that a high valuation on the 'perceptions of information value' will improve the intention of the stakeholder to carry out appropriate behaviours.

Finally, this chapter has also set the ground for presenting the next findings and discussion on the factors that have influencing impacts on the value assignment process elements that will be discussed in the next chapter. The main discussion of chapter 7 will present the outcome of exploring the RO3 through its sub-objectives.

7. Factors Influencing the Value of Information

7.0 Introduction

The revised conceptual framework (figure 5.3) denotes that there are relationships between the value elements and some external factors. This chapter will present and discuss these factors and the relationships between these factors with the value elements. Therefore, this chapter will present the findings relating to the third research objective (RO3) - ***to understand the factors that influence the stakeholders' 'perceptions of information value', which in turn affect their resultant 'information security behaviours'*** - and its two sub-objectives***.***

This chapter is divided into five sections. The first section describes in detail the term 'influencing factors, as used in the context of this research. The second section presents the influencing factors that have been found to have an influence on the stakeholders' antecedent 'Perceptions of Information Value'. These influences are recorded from the perspective of an individual stakeholder. The factors that were considered to have influences on the workgroup perception on the value of information are presented in the third section. The third section is followed by the presentation of factors found to have a common influence over the value elements. The chapter ends with some concluding remarks.

7.1 Influencing Factors

This section will describe, the factors, how they affect the various elements and more importantly to highlight that these factors may ultimately be manipulated to help enhance the value of the information, to members of the user community. This might be done by helping stakeholders to focus on those particular factors that will provide the most positive impact on the value of the information that they are handling.

Influencing factors, in the context of this research describe the various elements or issues that were claimed by the stakeholders that have influential impact on their information valuation processes. The findings from the interviews analysis suggest that two of the value

elements i.e. stakeholders' antecedent 'Perceptions of Information Value' and the Workgroup 'Perceptions of Information Value' are liable to be directly influenced by several factors. By contrast, there were no evidence from the data analysis of any direct impact of the factors on either the 'Perceptions of Information Value' or the Espoused value. These key findings have been summarised in Figure 7.1.

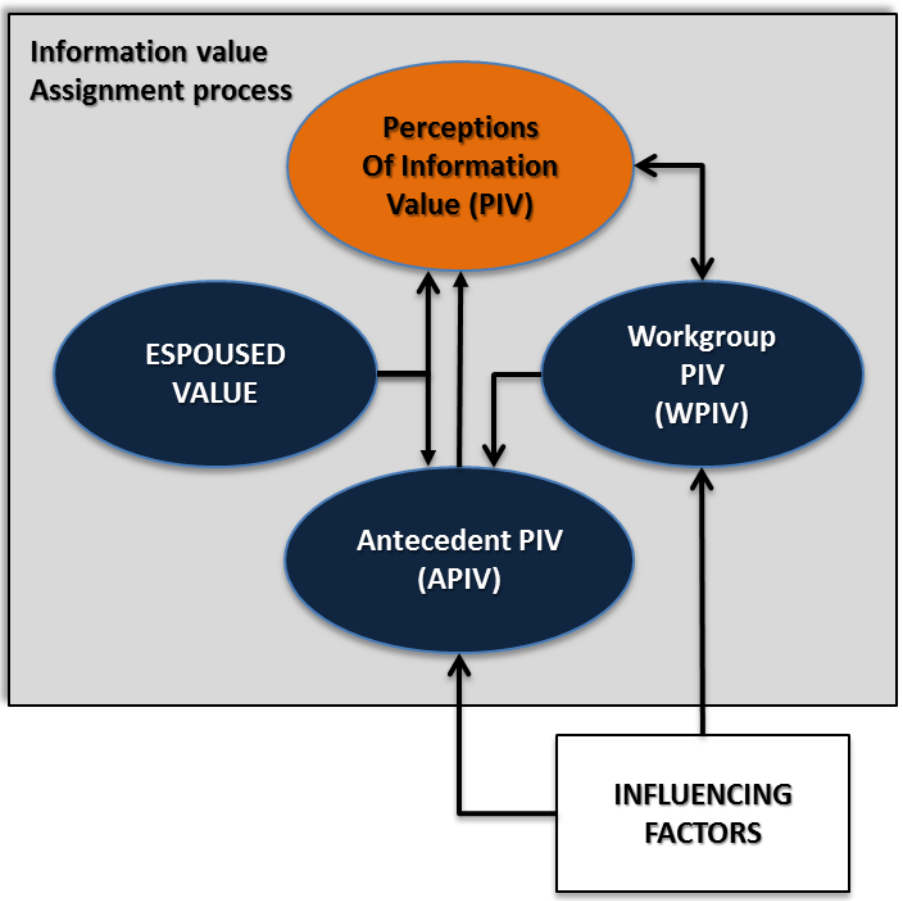


Figure 7.1 *Part of the information value assignment process model*

Initial insights from the review of the literature identified four broad categories of factor that may have an influence over stakeholders' perceptions of information value. The four dimensions are cultural impacts, importance metrics, sensitivity metrics and value dimensions.

During the interviews, the stakeholders shared a wide variety of factors, which had influenced their thinking when developing their 'perceptions of information value'. As the

stakeholders' reflections on influencing factors were analysed, it became clear that in some cases there were factors that falls outside the four initial dimensions. Consequently, some new dimensions were created and the existing dimensions were expanded to take account of these new insights. Table 7.1 below shows the changes to the dimensions identified from the initial interpretive model (Figure 3.4).

Table 7.1 *New identified influencing factors.*

Initial interpretive Model		**New factors identified**		
Cultural Impacts		*Organisational Culture*	*National Culture*	*Trust*
Sensitivity Metrics		*Sensitivity of information*		
Value Dimension		*Social value*	*Faith (religion)*	
Importance Metrics		*Organisational priorities (OP)* *OP – Ministerial Jurisdiction* *OP – Monetary*	*Individual Priorities (IP)* *IP – Awareness Education and Training* *IP – work Context* *IP – Task-related* *IP - Leadership* *IP – Instruction* *IP – Peer action & environment* *IP – reward & Penalty*	

The changes to the initial dimensions include:

- The dimension 'information sensitivity' is now further classified by the context it is applied to. Stakeholders' perceptions of information sensitivity typically follow a standard communicated by the organisation, which is an official government information classification standard. Inevitably, at times, the sensitive nature of information also depends on the context in which it is used, handled or stored. An

example of this would be, any information that applies a standard sensitivity classification would have their rating change if it involves prominent persons. The influence or the authorisation held by high-rank officers in the government provides them with unlimited access to information. Another example would be where access to the information is granted if the request comes from the superior despite the classification of the information.

- A more common factor that most stakeholders can relate to is the 'importance of information'. The term priorities were used in place of the phrase importance due to the varied meaning of importance expressed by the stakeholders. Priorities are furthered categorised into individual priorities (IP) and organisational priorities (OP). These signify that some of the priorities are from the perspectives of individual stakeholders and some are defined from the perspectives of the stakeholders as a group within the organisations. Furthermore, in most situations there are more than one importance factors related by the stakeholders and for situations where they are multiple factors, they may have to set priority on a factor that they think is more important to them. As depicted in table7.1, the IP is further subcategories of seven factors and the OP has two more subfactors. The full discussion of these factors will follow in the next sections.
- Along with the factor of social value, faith or religion is also commonly quoted as one of the factors that have potential in influencing stakeholders' valuation processes as well as their decision to behave. Therefore, the initial value dimension is further categorised into faith or religion and social value.

Various representations of the factors mentioned above were identified through the descriptions made by the participants based on their accounts of dealing with their own information. Evidence presented suggests that there is a close link between the mentioned factors and their processes of assigning a value to information and subsequently the stakeholders' 'perceptions of information value'. There are also clear indications that these factors mediated through their intentions, indirectly help to influence the information security behaviours they decide to adopt. Therefore, the identification of the usage these factors provide further evidence that stakeholders do assign a value to their information and therefore have a clear 'perceptions of information value' on the information that they

are handling. In the interviews, the stakeholders were asked to either respond to the discussion either from their individual perspective, or from a collective perspective as a member of a workgroup. The stakeholders were asked about how they think the other stakeholders, either individually or, as a group would react to the same issue. Based on the above methods of inquiry it was possible to make distinctions between the factors to determine whether the primary impact of each is either on the antecedent 'Perceptions of Information Value' or the Workgroup 'Perceptions of Information Value', or indeed, in some cases, upon both the value elements (figure 7.1). Both of the value elements play important roles in shaping the stakeholder's rationalised 'Perceptions of Information Value'.

It is not an easy task to measure the impact of something that is subjective in nature, and to do so accurately is even a more challenging one. Therefore, due to this subjectivity, no precise measuring tool was devised or used to measure the impact of the mentioned factors on the value elements as to be able to quantify them. The impact measurement here is based on how the stakeholders felt that these factors might, or might not, change the way they think about the value of the information. The impact measurement is also based on how the stakeholders think other stakeholders feel how the factors might or might not change their (the other stakeholders) thought of the value of information. To summarise, it was decided that the more the factors were cited or mentioned or represented by the stakeholders, the higher the potential of the specified factors is in influencing the stakeholders' perception of the value of information.

One method used to measure or differentiate the capability or potential influences that the factors have on the value elements is by categorising the factors into either Primary or Secondary impact factors. Primary impact factors are factors that are believed to have more impact on the value elements while factors with secondary Impact are factors that are thought to have less influence on the value elements. It is assumed that the more a factor is brought into the discussions (interviews), the higher the potential for it to be incorporated into their daily procedure and the greater the possibility that it have to do with influencing the stakeholders' decision-making. Another aspect from which the impacts of the factors were measured is based on the intensity and how passionate the factors were discussed by the stakeholders and the expression on how much they were influenced by the factors.

In the second phase of data collection, these factors were presented to the three different groups of stakeholders and their feedbacks were collected and analysed. The stakeholders were asked the validity of the factors according to their experience in handling information. They were also invited to reflect on the significance of the factors on their information valuation process. The analyses of this feedback not only have improved the understanding of the factors, but it also helped validate the earlier judgements regarding the relative strengths of each influencing factor. Consequently, these groups of stakeholders have verified the impact level of the different factors.

It is believed that objectivism integrates subjectivity and objectivity because it argues that objective knowledge requires active, sophisticated subjective processes. These subjective means may include perception, analytical reasoning, false reasoning, logical deduction, and the distinction of essences from appearances (Ratner, 2012). For this reason, it is believed that the subjective valuations mentioned above are valid and furthermore may enhance the objective comprehension of the phenomena.

Having validated the factors, it was possible to segment them into two categories, namely driving forces and restraining forces. The factors that influence the justification or rationalisation of the stakeholders to achieve positive value on the information they are handling are labelled as driving forces. The restraining forces are the ones that may impede the stakeholders to the positive valuation of the information or provide unwanted influence on their behaviour intention.

Force can either be driving or a restraining one and may be present in both categories, for example in figure 7.2; the IP (AET), IP (rewards & penalty) and OP (min Jurisdiction) in figure 7.3 appears as both the restraining and driving forces. The reasons for this are first because different stakeholders experience the impacts of these factors differently; these forces may be seen as giving different effect to them. Secondly, the forces may have second ends to it, taking as an example the IP (AET). If proper awareness education and training are provided for the stakeholders, they may see it as an advantage and it will increase their self-efficacy in carrying out the information security countermeasures. From this juncture, it is considered as a driving force. On the other end, those who are not sent for any AET will

have a low sense of self-efficacy. Furthermore, as reported by the stakeholders because of this, they assumed that the information they are handling did not actually in need of protection. From this point of view, the IP (AET) then becomes a restraining force. Another thing that needs to be highlighted is that although some of the forces may appear in both categories and may impact both value elements, they might affect the value elements in different levels.

The following sections will present the factors that may influence the antecedent 'Perceptions of Information Value' of the stakeholders. Section 7.3 presents the factors that were found to have an impact on the stakeholders' antecedent 'Perceptions of Information Value' while Section 7.4 presents the factors that were found to have an impact on the workgroup 'Perceptions of Information Value'.

7.2 Factors influencing stakeholder's antecedent PIV.

This section presents a detail discussion on the factors that were found to have influence over the stakeholders' PIV. These are factors that are personal to the stakeholders, which are from the stakeholders' individual perspectives. These factors are claimed by the stakeholders' to have a beneficial impact on them personally, i.e. the factor was able to provide the utility with the stakeholder were hoping for. For example, many of the stakeholders claimed that they exercise good information security behaviour to protect the information they are handling because the information is crucial in completing the task they were given. This section of the chapter will present those factors that were considered from a stakeholder's perspective to have an influence on their value assignment process and subsequently thought or proven to have an impact on their resultant behaviours. These factors will be categorised as 'individual priorities' or IP, for short.

7.2.1 Individual Priorities (IP)

The process of evaluating the importance of information at the individual level occurs when a stakeholder assigned a value to the information as a result of the assessment. The assignment of value is usually based on a current or near-future prediction of needs. There are a few different perspectives from which the importance of information has been

represented in the interviews. Individual priorities describe factors that are regarded from the perspective of an individual stakeholder. All of the reasons mentioned are used to justify an action or the stakeholders consider these factors are priorities or important to them individually. The term important or importance is also used to define personalization of information, for example, if stakeholders felt that the information belongs to them and they will be held responsible if anything happened to the information they would be more willing to protect them. A manager in one organisation expressed this;

> **MOF-01** *I handle the budget, information on approved budget is very sensitive. If such information leaks, they might use the information to their interest. I will be held responsible for this. This is why it is important for me to protect and secure the information I'm working with.*

The importance of information is also associated with the reasons for which the information is being protected or secured. One reason expressed by the stakeholders is to uphold the trust invested by their superior or peer onto them.

> **MOHA-03** *If we are assigned a particular task or being trusted with some information we need to be able to value them and protect them. When we can achieve those, we felt that we can be trusted. We need to maintain peoples' beliefs in us.*

One translation that relates to the importance of information gathered from the interviewees is linked with their position in the organisation. Stakeholders with high rank in the organisation are susceptible to an assessment by subordinates, superior and peers. The assessment will reflect and affect the status and reputation of the stakeholder being assessed. For a stakeholder who is concern about his or her status and reputation, showing how much information should be valued and leading with appropriate compliance behaviours are important to be respected by others. The reason for this is that higher-level officers are expected to set a good example; their action denotes how their subordinates behaviour towards information security countermeasures.

> **MOD-02-01** *we need to lead by example, for instance by displaying good information security behaviour and upholding the rules and regulation that we have on information handling. Through this way, we will be able to promote good information security and earn respect from our men.*

Another translation of the Importance of information by the stakeholder relates to the meaning of the information to the stakeholders. The information becomes relevant to a stakeholder and worthy of protection if the information provides some sense to them. In this regard, it's a subjective individual sense. The following excerpts indicate some of the different 'meanings' of the information to the stakeholders.

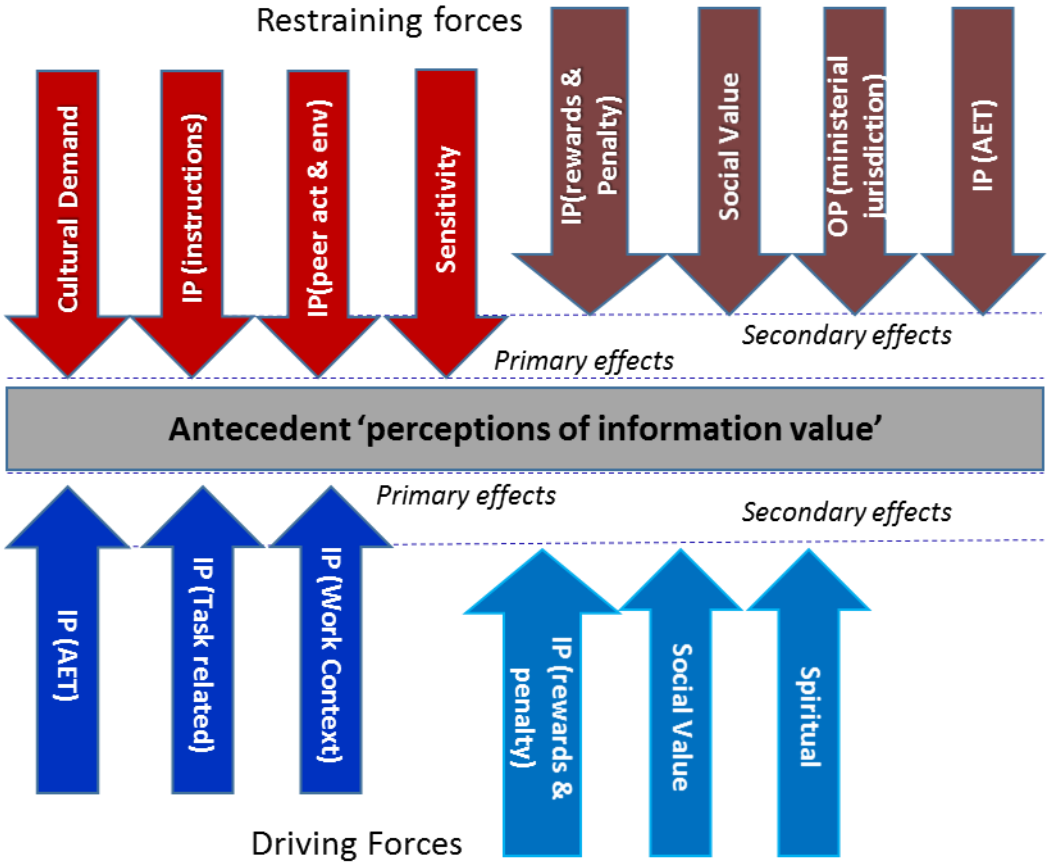


Figure 7.2 Influencing factors on antecedent 'Perceptions of Information Value'.

> **MOC-01** *I keep all my information safe because, I will be held responsible if anything goes wrong and by keeping them safe, my boss is happy with my work.*
>
> **MOE-04** *It is my responsibility; I'm expected to secure the information I'm working with. It's important for me to seen as being responsible and all.*

The representation or translation of 'importance' does not stop here, as mentioned earlier there are variations of the translation made by the stakeholders. The next sections will present the most common variations of the 'importance of information' according to the stakeholders. These differences are claimed to have significant to the stakeholders' rationalisation of the value of information.

7.2.1.1 IP (Task Related)

One of the dimensions of information valuation commonly used is how the information explicitly facilitates the accomplishments of the stakeholders' tasks. The more the stakeholders need the information to perform and accomplish their duties the higher will they assign the value to the information? This valuation, in turn, would encourage positive information security behaviours. Information is considered to be important in many cases where it is perceived to facilitate decision-making, problem-solving, understanding and planning during the regular course of work.

> **PMO-02** *the information that I'm dealing with is all about viruses and viruses attack, it is not confidential at all, but it is important for me, for my monthly report, etc...*
>
> **PMO-11** *my work involves preparing the budget, information that I handle is important for me to accomplish this task so it needs proper protection*

The IP (task-related) factor of influence as mentioned in the above examples become a driving force (i.e. it provides means for the stakeholders to accomplish his tasks) that brings strong influence over the stakeholders' information value assignment. It is suggested that this factor generates a primary effect on the stakeholder's antecedent 'Perceptions of Information Value'. This relation is portrayed by figure 7.2 showing the IP (task-related) as an upward arrow.

7.2.1.2 IP (Rewards and Penalty)

Rewarding stakeholders or imposing some sort of punishment for their behaviours indicates the concerns of the organisation on the way information are being handled in the

organisation (Herath and Rao, 2009). From the perspective of an organisation, reward and penalty would encourage good information security perceptions amongst their stakeholders. More importantly, from the viewpoint of the stakeholders, the existence of a reward system and the provision of penalty also signify how much the organisation value the information they are dealing with. Ultimately, the provisions of rewards or punishment by the organisation provide a de facto value assessment reference for the stakeholders. Furthermore, the provision of some sort of rewards and penalty shows that information is being appreciated and that it should be highly valued and consequently appropriate information security behaviour should be adopted. The following quotes from the stakeholders support this perspective:

> **PMO-02** *If there is a proper penalty system, staff will understand how the organisation value the information. If they don't abide by security procedure, they will be reprimanded and penalised. Equally, a proper reward system would signify the same.*
>
> **MOFAT-01** *I think it all depend on the organisation, if they reward people because of good behaviour and penalise them for bad behaviour then we will know that the organisation have a high value on the information we have.*
>
> **PMO-22** *Disciplinary action should be taken if we are not responsible, then people will take it seriously, sometimes government servants just take it for granted.*

The above, responds from stakeholder PMO-22 indicates that the provision of penalty would become a driving factor for the stakeholder to appreciate the information she is handling. Any reward or penalty system should be made clear to the stakeholder, if the stakeholder is not even sure if such system exists, they will have a different perception of what messages the organisation is trying to convey to them in the context of information security. The following responses, the non-existence of reward or penalty may become indicators to stakeholders that the information are not that valued and in this case, reward and penalty may become a restraining factor in influencing the value assessment process by a stakeholder:

> **PMO-18** *there are no clear rewards when it comes to information security, information is valuable but sometimes management just doesn't care. Maybe it's difficult for them to implement (penalty) or it's not worth penalising.*
>
> **MOH-03** *Reprimanding of security offends would be the perpetrator and us and it is not made public. I think because of this they believe that we don't really value our information.*

There are also indications that some stakeholders perceive that to secure a promotion or for their work to be recognised they must be able to value and handle information appropriately. Therefore, on anticipation of some form of development in their work, it is perceived that one must be compliant and display positive information security behaviours:

> **MOD-01** *to be promoted to this position I need to understand the value of information, especially for the army and be able to act (behave) accordingly. Our information is crucial to the country.*

Here, reward in term of a job promotion is seen and has become a driving factor for a stakeholder to treat the information under his jurisdiction appropriately. On the other hand, some user level staff expresses their counter perception on the promotion issue, as they consider what they do for the organisation is only of limited significance:

> **MCYS-01** *I don't deal with relevant information or data… that is all prepared and looked after our higher management. I'm only a user level staff there are more superior people above me*.
>
> **MOC-04** *Staff with IT background and good understanding will have responsibility for information security. Otherwise, it will be neglected.*

These quotes indicate that some user level stakeholders believe that important information is only handled by higher-level staff and because of that, and that they (user level stakeholders), therefore, have less responsibility for protecting the information. This notion suggests that the responsibility for information security comes with the job description. Therefore, this indicates that a reward scheme such as promotion is believed to provide more appreciation for the value of the information.

One other finding made from the data collected is that the provision of penalties seems to have less impact than rewards as expressed in the following response:

> **MOH-02** *I have never seen or heard of public taking action (suing or charging) staff for any wrongdoing, inappropriate behaviour and may include Information security issues.*
>
> **MOF-02** *because sometimes if there is anything like a penalty, e.g., disciplinary action that one is considered like very confidential so we cannot disclose to others if possible….only the relevant parties should know.*

The penalty is seen to have less significant over rewards may be because of several reasons. For example, there is little or no substantial evidence that proper penalisation was given to the perpetrator. Most of the stakeholder when ask, said that they have not seen or heard of anybody that has been penalised for breaching information security. Only particular cases were made public, due to this the public is not aware of other penalised cases. Most of the news on penalties given due to information security breaches are only heard through 'hearsay'. The improper regulation of a penalty system will result in users disbelieving in the system thus may have little or no impact on their valuation process. Therefore, perceptions on the use of penalty lean more towards a restraining force than a driving force in regards to influence on the information antecedent 'Perceptions of Information Value' of the stakeholders (Figure 7.2)

In summary, the IP (rewards & Penalty) does have some influence on the antecedent 'Perceptions of Information Value'. Depending on the situation, IP (rewards & penalty) may be seen as a driving factor and may also become a restraining force to the stakeholders. Despite the discussions mentioned above, the responses from the stakeholders indicate that the influences of IP (rewards & Penalty) typically have secondary effects on their antecedent 'perception of information value'.

7.2.1.3 IP (Work Context)

Another factor that was frequently referred to during the interviews was 'work context'. Work context is described as the perceived responsibilities that come with the stakeholders' position and job description. For example, user level users (clerks, junior officers, programmer, etc.) assume that information they are handling or dealing with is not so relevant (to the organisation or at least the management) because their contribution to the organisation is minimal. They believe that they are not in the position to be trusted with

highly valuable, sensitive or confidential information. Therefore, because of this, they often believe that information that they handle is of less importance and have a low information value. So assumptions prevail that information as such does not need substantial protection or in some cases may not need any protection at all. This notion, therefore, makes them believe that they don't necessarily need to be compliant with information security countermeasures. The above notions are indicated in the following excerpts:

> **MOFAT-02** *For us we have a unit that takes control of securing our data, they will protect all sensitive data and confidential data from our PC.*
>
> **MOD-01** *I can think of that level may be I have not experienced any security incidents. I guessed when it happened.. my boss will take care of it.*

A stakeholder in a senior position also expresses the same concern in the following excerpts.

MOE-02-01 one *of our problems is to convince our junior staff and clerks that whatever information they are handling is of high value to the organisation. Usually, they leave the security part of their work to the IT/IS department.*

As a result stakeholders with such perceptions may see the process of protecting information is secondary to their daily tasks and many, expect such processes should be handled by the security department or their superior. Most stakeholders (non-IT/IS users) perceived that responsibility to ensure the security of information is the sole responsibility of appointed IS or IT personnel. Some stakeholders view information security as secondary to their primary tasks and, more worryingly, they may believe that information security countermeasures can hinder their duties as indicated by the following excerpt:

> **PMO-22** *The token for the PKI is bulky and we need to enter the code every time we sends e-mail, this becomes an overhead to my work.*

Stakeholders with higher posts see that their appointments come with the responsibility of treating the information appropriately and this behaviour is expected of them. They also believe that their subordinates should also have the same perception towards the same information. This clearly shows that work context of a stakeholder may become a driving factors towards achieving a good value on the information. Unfortunately, this notion is not always in check. It is common to see lower levels staff displays behaviours that are not in line with their superior requirements or intentions.

MID-01 *the higher rank or higher appointment you have, the more.... sensitive document ... as you get higher, you understand ... how important is the information is to be kept or not to give out to anyone....*

MOFAT-01 *I think, regarding personal, like, how you do things and get recognise. Regarding self-satisfaction, you get the job done in the best way that you can do. It's like, okay, this is the best thing I can do, my boss is satisfied with my job*

Upper Management as the owner of the information is always more positive in their expectation that all staff should consider that information they are dealing with has a high value to the organisation. This suggests contrasting perception from some of the user level stakeholders. These perceptions might be the outcome of a few factors;

- Lack of understanding on what information security, actually is.
- Failure to realise or understand the meaning or value of the information they are handling.

Another issue related to work context mentioned by the participants in the interviews was regarding the perception of physical security. The availability of physical security is perceived as overall security for the information. Furthermore, stakeholders are more focused on logical security implementation rather than to understand why is it necessary to implement and to comply with it. Some stakeholders realise that any countermeasures implemented was for a reason but they rarely knows what the reason is. Users are more focus on how information are being used rather than how should it be appropriately protected.

The IP (work related) factor is portrayed in the diagram (figure 7.2) as a primary effect driving force. The IP (work related) factor has the potential to motivate stakeholders to better appreciate the information they handle. For example, convincing the user level stakeholders that the information they are handling is important and has high value to the organisation may help in encouraging a higher valuation of the information by the stakeholders.

7.2.1.4 IP (Instructions)

As evidenced from the analysis of the cultural aspects, it has been found that relying on the judgements of superiors is a common state of affairs. From the data analysis, it becameclear that stakeholders are also basing their information valuations on the nature and type of instructions they receive from their superiors. Despite the existence of information classifications, most of the time subordinates waits for further instructions from their direct superior on the issue of information classification and valuation. These instructions more often are seen as the standard ways of carrying out their tasks and create a *de facto* valuation on the information being handled. Instructions from superiors are therefore an important mechanism for information valuation, as indicated from the excerpts below:

> **MOHA-03** *we don't have any policy, we work according to our superiors instructions or command. So it's up to the person who gave the instructions, it may also change.*
>
> **PMO-17** *I rate the sensitivity of the information that I handle a high nine because my boss, like every document we have other people, cannot see it. If he sees these documents lying around he will tell you off, we have to secure the information from prying eyes*

How superior stakeholders manage their information protection is one of the important factors that was expressed as having a clear influence over stakeholders' value assigning process. Some participants admit that their compliance behaviours, with information security countermeasures, is influenced by how strict or slack their superiors are in managing information security. The above examples also clearly indicate that appropriate instructions from superior may become the driving factor in assigning a good perceptions of information value on the information. They also tend to copy the behaviour displayed by their superior i.e. if their superior are strict on upholding information security then a secure environment will exist and if their superior does not pay much detail on information security issues, then a relaxed environment will be adapted.

On the other side of the coin, some participants believe that information passed down to them does not need much security as they have the idea that if it is confidential or sensitive the information might not reach them.

> **PMO-03** *Classified information does not reach us... whatever our boss gives us... so*

> *far we don't have any classified information.. We don't have anything about financial etc. "I don't handle on the filing of confidential information or papers."*
>
> **MOE-02** *all the confidential stuff is taken care by my boss.*
>
> **PMO-18** *It depends a lot on the HOD, if he is strict then information security is strict.... otherwise people will only take it for granted.*

From the data analysis, it became clear that when the superior had an eye for security and considered to be strict on information security by the stakeholders, an acceptable level of information security is always practised. This is expressed by one of the stakeholders in the excerpt below;

> **MOHA-01** for *me all the confidential information is being handled by my officer, they will know if it is sensitive or confidential. All this information will be dealt with by a designated person so other staff don't know about it."*

Evidence also shows that some leaders (managers or IT specialists) do not provide ample guidance on how to handle information for their subordinates. This may result in confusion amongst user level stakeholders mainly with the misconceptions of the confidentiality, importance and sensitivity of documents and information they are handling.

In many cases, segregation of information is not clearly defined. As user level staff depends on their superior instructions to carry out actions, it is very important that a clear and concise procedure is provided. For example, although there is an official framework on the categorisation of information provided by the Internal Security Agency (ISA) it is only as a general reference. The specific definition of each category is left to the head of the organisations, departments and units. In many cases, these categories are vaguely defined, from one office to another, different assumptions are made and things get complicated especially for the user level stakeholders (the users). Evidence from the interviews also points out that upper management is not properly educated on information security policy; what they are, how they work and how to administrate the policy. Many also believe that their organisation, department or unit requires a different policy from others but there are not sure about it.

It is also noticed that although most IT personal and higher management have ample IT/IS training or background they are still reluctant to introduce security measures in their

respective, organisation, department or division. There were several reasons expressed as to why senior staff may be reluctant to take the lead:

- They believe that to do so must come from a higher authority instruction.
- They don't want to be seen as big-headed
- Does not want to be held responsible if anything goes wrong;

Therefore, it can be highlighted that the value a stakeholder's assigned to the information may be influenced by the instructions they received from their superior. This is supported by the nature of the Bruneian culture which is collective in nature. In this kind of culture respecting superior views and ideas are highly expected. The IP (instructions) may become a restraining force (figure 7.2) if the instructions received are prone to non-compliance nature. In this kind of setting, in which instructions from superior are given priority, it will present an opportunity for the organisation to use this environment to be able to influence better the perceptions of the stakeholders on the importance of information security.

7.2.1.5 IP (AET) Awareness Education & Training

Issues of AET were also a frequently referenced made by the stakeholders during the interviews. Most participants mentioned the importance of awareness towards information security from an education and training initiatives perspective. This strongly indicates that awareness of information security exists amongst stakeholders. Most reported AET done by organisations are informal and it depends a lot on the views of their superior. Most of the time, AET are in the form of a verbal reminder of do's and don'ts. From the perspective of the stakeholders, their needs for training are more towards understanding the "why" elements of information security countermeasures. For example, why do they have to have a strong password and the consequences of sharing of information? Rather than the common training of telling staff what to do and what not to do.

Stakeholders also commonly highlighted that selection for training is usually made by the human resource department and sometimes are not done properly and, as a result, some people that handle information are excluded from the training. Although stakeholders realise the importance of undergoing information security training, most of them have never undergone any AET. Expression from the stakeholders suggests that training

opportunities will instil the notion that they need to be able to provide necessary protection to their information and advocates that the information they are working must be highly valued. Unfortunately, due to the selective nature of the information security AET provision by the organisation, some stakeholders assume that they were not sent for training because what they are doing does not encompass information security matters. This perception thus provides a false attitude towards information security and may result in low compliance towards information security countermeasures.

> **PMO-07** *we are not given any information security training, only the security team goes for security training…. But I think everyone should go*
>
> **PMO-13** *Yes, it is important for our knowledge.... before this I have not been sent..i would love to attend one... it is important for me to gain that knowledge...like what we do... we don't know how the security is no, but I have only gone through end-user training for PC..but, not on security.... not including misuse of data or information and so on..*
>
> **MOHA-01** *Staff should be given ethical training on top of awareness training. More towards work attic. For example, what threat are there out there…what is our weakness and so on.. not just do's and don'ts…..*
>
> **MOH-01** *training was on how to use the system but on the ethical issue... like policy.... not even been taught.... things like that... what... we don't have it all together...*
>
> **PMO-04** *I know that our organisation has conducted training, but I was never included…I was nominated once… but never selected.*
>
> **MOD-01** *I was never sent for any training regarding security… If I'm sent for one, it's not significant to the process of securing information.. I don't think they see our tasks involve important information.*
>
> **PMO-03** *we have installed a PKI for securing e-mail, but we have not been introduced to that and we were not taught how it works. I guess t because we a junior staff and we don't need it.*
>
> **MOE-04** *security training is important for all, but I guess only people who need them the most are sent for training.*

Together, the above responses strongly indicate that from the perspective of the stakeholders the provision of awareness, education and training will improve how they perceived the value of the information they are handling. The positive valuation may arise due to the confidence achieved by the stakeholders in their self-efficacy if they had proper

training. From this perspective, the provision of AET would become a driving factors to the stakeholders. It also shows the commitment and the seriousness of the organisation on the security of their information thus it indirectly espouses the value of the information. Additionaly, the management of AET provision must be taken seriously and carefull management must be done to avoid exclusion of AET to stakeholders. Although, AET is seen as a driving force in influencing stakeholders' value assessment, inappropriate exclusion of awareness, education and training as indicate by the above responds may turn into a restraining force to the stakeholders.

7.2.1.6 IP (Peer Actions and Environments)

Perceptions about the information security behaviour, of peers, is another significant factor that influences a stakeholder's information valuation process. Similarly, perceptions are also based on the surrounding environments e.g. their superior's attitude towards information technology and their behaviour towards information handling and protection. For example, a nurse knows that some information on the patients is confidential and sensitive. However, since they are used to seeing doctors sharing that information freely, it is accepted as a valid action.

> **MOH-02** *It happened, when I was a new nurse, the doctor talk about the patient confidential information with attachment students and others....so some information is considered not that confidential after all....*

A stakeholder surrounded by colleagues that do not appropriately observed the information security policies is exposed to bad influences as illustrated by the following excerpts. The excerpt also suggest that peer actions and environment may become the restricting factors for the stakeholders.

> **MOF-01** *Yes.. I think it'll impact, for example if some staff does not comply and no action is taken they will say what's wrong with me doing it.. they are not going to take action …*
>
> **MOC-08** *the information security atmosphere in our office relates to how our big boss views it. Our boss is quite strict on complying to information security; other sections bosses are not so strict.*

The above quotes suggest that how superiors frame the environment of the department also plays an important role in influencing how stakeholders' value the information they are handling. Indirectly, the appropriate actions by their peer and the environment set due to the actions becomes the driving factor for the stakeholder to better evaluate the value of the information they are handling. Therefore, Peer Action and Environment plays an important role as an influencing factor to stakeholder's antecedent 'Perceptions of Information Value'.

7.3 Factors influencing Workgroup PIV

This section presents a detail discussion on the factors that have been found to have influence over the value element Workgroup 'Perceptions of Information Value'. These are factors expressed by the stakeholders that they thought other stakeholders consider important in encouraging them to exercise appropriate information security behaviour. Discovery of these factors will answer the second sub-objectives of RO3, which is to understand the factors that influence the stakeholders' perceptions of information value from the perspective of a work-group. Since these factors were mainly expressed as a collective perspective within a group and such group may represent a big portion of the people in the organisation so the factors are consolidated under a major theme called 'Organisational priorities (OP)'.

7.3.1 Organisational Priorities (OP).

To the individual stakeholder, the term importance is further classified into sub-variables. At the highest sub-levels, the importance metrics factors are differentiated between their personal perspectives and collective perspectives of the stakeholders as a group within the organisations. The collective views of the group of stakeholders are called the organisational priorities. The information 'value' are mostly assigned to a group of people, for example, a shared value created by clerks of a department on an individual piece of information, a collective value assigned by middle management or value assigned to a group of IT/IS personnel. These valuations may be seen as representing the 'actual value' by a particular group of people but not necessarily agreed upon by other groups of stakeholders in the

organisation. This perspective suggests that a real value may never be accurately quantified and justified. The factors that fall under the OP category are factors that are claimed by the group of stakeholders to be important to the organisation. For example, any information that helps to sustain and develop the core functions of the organisation would be crucial to the organization. Additionally, if the information relates to monetary matters higher value is expected.

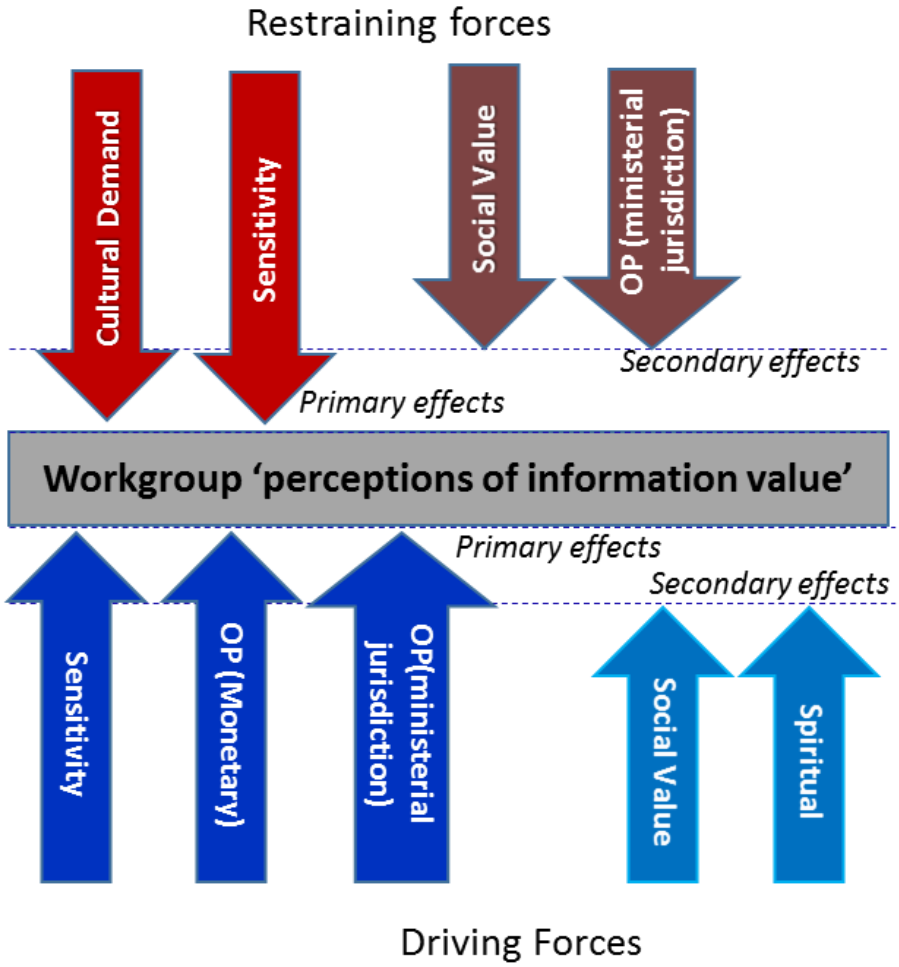


Figure 7.3 *Influencing factors on workgroup 'Perceptions of Information Value'.*

The factors that fall under the 'organisational priorities' are discussed in the following subsections. Figure 7.3 portrays the various factors that are found to have a significant impact on the Workgroup 'Perceptions of Information Value'. Some of the factors are suggested to have primary effects on the value element while others are seen only to have secondary impacts.

7.3.1.1 OP (Monetary Value)

Information that is associated with any monetary value is always seen as important and need to be protected. Examples of such information would be the tender documents, project allocation, budget allocation, staff salaries, etc. Staffs are always reminded by superior to take extra caution when dealing with information that relates to the significant amount of money.

> **MOF-01** *Approved budget and allocation of monies are very sensitive and relevant information. I need to secure them well. I deal with tenders from outside a lot; I need to protect our budget information so the vendors do not take advantage of us.*
>
> **MOE-03** *of all my tasks, I think the most important information that I need to protect is on the department budget.*

The above excerpts indicates that stakeholders assume that IP (monetary) is one of the factor that may encourage their valuation of information. Users that handle information perceived as not having association with any monetary value may observe the information to be not as important with information related to monetary value. Therefore, information that cannot be valued in monetary terms may be assigned a lower value, and therefore a lower level of security and protection might be assigned to it.

7.3.1.2 OP (Ministerial Jurisdiction)

Information handled, differs from one ministry to another which depends on the core function of the department and the organisation's priorities. For example, staff under the ministry of education would manage the information regarding students and teachers whereas the prison staff would have control over information of their prisoners while the military would have critical information on the country's military strength. This resulted in

two different perspectives, one from the general public and another from the stakeholders in different ministries.

From the perspective of the general public, information dealt by certain authorities such as the military and other enforcement agencies such as the police, immigration and customs, as well as the health services, are seen to be more important. The information they handled are considered highly confidential (although it is not known what kind of information) and very sensitive (such as health records held by health services or the whereabouts of military forces) more than the information maintained by the other organisations. Information controlled by other departments may be considered common and therefore deserving of less protection. This view is also shared amongst some stakeholders, particular those who represent organisations such as the military, enforcement agencies and health services. They also perceived the information they are handling is more confidential and more sensitive compared to information managed by other ministries. Due to this, the OP (ministry Jurisdiction) becomes a primary driving force in influencing the Workgroup 'Perceptions of Information Value', which is shown by the upward arrow shown in figure 7.3. This finding, suggest that manipulating stakeholders' perceptions on the importance of information through establishing the importance of the organisation's information in the public eyes may influence the valuation of information of the stakeholders.

Some other stakeholders who are from other organisations other than the military, enforcement agencies or health organisations, believe that although the information they are handling is also important, it is not as highly confidential and sensitive as information handled by the military, enforcement agencies and health services. . The following responses support the validity of such notions:

> ***MID-01*** *we handle information that are more crucial to the country then other ministry… one of the impact if it falls into the wrong hand because the Navy work in secretive, we are protecting the sovereignty of the country.*
>
> **PMO-15** *one department .. consider certain information could be highly classified while the other department might say no.... e.g., student records... we say.... its low in our rank.. we have other records, e.g., financial information government personal records.....high-level government records..... but to that department.... e,g, curriculum department... they will say this is our main information. We'll treat this as*

> *highly valuable... so proper classification of data and information across the government is not there yet.....*

Stakeholders in departments or units that are commonly perceived to handle high 'value' information will see the OP becoming a driving force. The high 'perception of information value' may come as motivation to the stakeholders to provide appropriate relevant protection on the information. Such view has made the perception of the information value of the stakeholders in Ministries (not perceived to handle important information) low despite handling a similar kind of information. These perceptions raised some misunderstanding, confusion and even disagreement amongst different level of people in an organisation and between higher-level officers in different organisations and ministries. Since some public staff works across departments and ministries and a lot of staffs are related (family and friends) this may cause some issue. This issue may come in the form of inconsistency perception of the value of information. For these reasons, the OP (Min Jurisdiction) may also become a secondary restraining force in influencing the Workgroup 'Perceptions of Information Value'. The red downward arrow labelled 'OP (min Jurisdiction) portray this notion in figure 7.3.

7.4 Common influencing factors

During exploration and investigation of the factors, it was found out that some factors impact both individual and group perspectives. This section introduces and discusses the influencing factors that are common to both antecedent 'Perceptions of Information Value' and Workgroup 'Perceptions of Information Value'. There are four categories of factors identified that suggest some influence on the two value elements. These factors are cultural demand, sensitivity, social value and spiritual.

7.4.1 Cultural Demand

The element of culture such that one should respect and follow what has been dictated by culture is another factor that was commonly mentioned during the interviews. Previous studies by Salleh & Clarke (2009) found a similar pattern in which culture plays an important role in shaping the intention and the actual behavior people chose in an organisational setting. As a guide to exploring the impact of culture, fundamental dimensions identified by Hofstede et al. (2010) were adopted, to help explore the influence of national cultural dimensions. Since there were no prior scores for Brunei as there has been no study made on the cultural implications based on the Hofstede dimensions, an alternative way to gauge how Brunei would fare according to the Hofstede's cultural dimensions was made. Average scores by some selective countries that display similar characteristics to Brunei Darussalam were taken instead. Detail discussion on the process of determining the cultural score for Brunei Darussalam and its outcome can be found under Appendix B of this document.

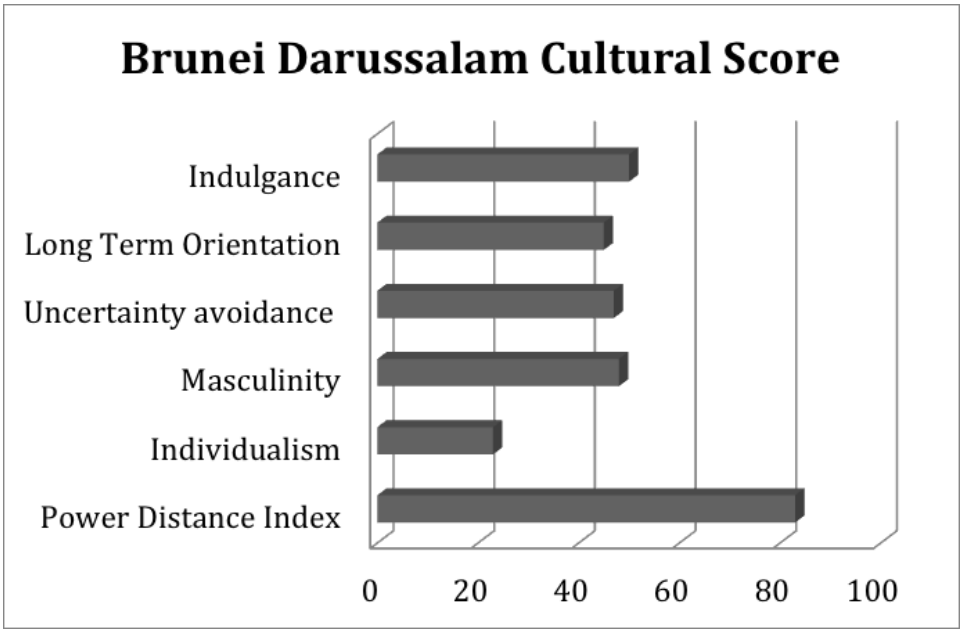


Figure 7.4 Brunei Darussalam's cultural score

Amongst the traits displayed (figure 7.4), two main traits dominated the representations from the respondents. These are power distance index (PDI) and Individualism. Referring to (Hofstede et al., 2010), a high PDI score indicates that hierarchical order is well accepted; everybody has a place and this needs no further justification. Subordinates expect to be told what to do and the Ideal boss is a benevolent autocrat. The analysis of the representation of the stakeholders during the interviews indicate that this cultural trait relates to dimensions of individual priorities; instruction and leadership (discussed under section 7.2.1). In which stakeholders' valuation of their information and how they choose to behave are strongly influenced by their superiors. They accept whatever instruction they received from their superior without questions. In some cases, information is treated as important and an appropriate measure to protect is taken only when they receive direct instructions from the boss. The following responses show that one of the cultural traits i.e. submitting to superior may become a driving factor for appropriate information value assessment and assignment:

> ***MOHA-01*** *My officer handles for me all the confidential information*, they will know if it is sensitive or confidential. All this information will be handled by a designated person so other staff don't know about it."
>
> ***PMO-18*** *It depends on a lot on the HOD, if he is strict then information security is strict.... otherwise people will only take it for granted.*

> ***MOHA-04*** *Behaviours towards information security sometimes depends on a hierarchy of commands... if someone with higher rank ask for information.... it is shared without question.*

Brunei Darussalam national culture is of a collective nature as indicated by the low individualism (IND) trait score (Figure 7.4). According to (Hofstede et al., 2010), such societies foster strong relationships where everyone takes responsibility for fellow members of his or her group to preserve the in-group feelings and commitments. Loyalty in a collectivist culture is paramount and overrides most other societal rules and regulations. Information flow is hierarchical and controlled; subordinates expect to be told what to do and the ideal boss is a benevolent autocrat. Attitude towards managers are formal. Harmony is found when everybody saves face in the sense of dignity, self-respect, and prestige. Social relations should be conducted in such a way that everybody's face is saved. The society fosters strong relationships where everyone takes responsibility for fellow members of his or her group. Society's offence leads to shame and loss of face, employer/employee relationships are perceived in moral terms (like a family link), hiring and promotion decisions take account of the employee's in-group; management is the management of groups.

Analysis of the corresponding representations by the stakeholders reveals that the stakeholders' are leaning towards a collectivistic society. A collective culture in itself may influence how stakeholders make their information security behaviours. The following quotes indicate that the sense of responsibility towards others is strong within the community and in many cases, others interest are given priority over the information security.

> **MOHA-02** *if people know you have access to certain information, "can you check something for me?" these information cannot be shared, but sometimes we are pressured by colleague, friends.. so we must say sure that they can be trusted.....*
>
> **MOH-02** *We don't usually release information on patients but if the family members insist we have to. Sometimes even distance relative and friends want to know and they are persistence, some of them are people we know... so in this case we have to....*
>
> **PMO-05** *if me ... I follow or comply because I'm responsible to the government... if we don't follow... if let's say. I would only disclose my password with my team.... if another team I will not share*

> **MOF-01** *Because sometimes for staff related matters like those who were given disciplinary that one considers like very confidential so we cannot disclose to others. Only to the relevant parties*

Collectivism implies subordinating personal interests to the interests of the group and is based on cooperation and harmony, as well as a concern for the well-being of the group (Pinillos and Reyes, 2009). This indicates that the group behaviour may have influence personal behaviour and this can result in both good and bad. The following excerpts from the interviews indicate how culture, beliefs and custom may influence the perceptions of stakeholders.

> **MCYS-01** *They tend to believe that "it's just Brunei" not like in other countries (UK) more prone to hackers ... they feel that they are safe.... ..why would somebody do that. No awareness of information being attacked*

> **PMO-04** *I know Brunei is considered as a safe place. There is nothing here to be hacked or spied on... I'm thinking on the positive side.*

The above excerpts suggest that there is a collective believe that because the country is small and not a major player in the world, it is safe from crime regarding information. This belief poses some danger to the attitude towards information security. Such notion may result in the stakeholders' to lower their guard and might have a lower perception of the value of the information they are handling.

In some of the reported cases, information security procedures are overlooked or ignored because of the influence of culture and customs. Reporting information security violations are uncommon and in some cases the procedure are missing from the organisational policy. As suggested by the following excerpts, caring for others' feeling and keeping their credibility is seen as a responsibility. To some stakeholders, it is something that has to be done, an obligation to others and respect for customs.

> **MOHA-03** *We have no reporting procedure; we don't want small matters to become big. There is one case, although we know who leaked the information we did not do anything. We don't want to cause chaos and if this comes to the knowledge of our boss, then he will deal with it. Otherwise, we keep quiet; we want don't want to hurt his/her feeling.*

> **PMO-03** *We are not really, we always have pity on people and have mercy and very compassionate especially if it's amongst friends. We usually say it's ok even if it's not.*

We are like "I don't want to disappoint him. We want to protect his feeling.

MOF-03 *I think it has something to do with our culture. Umm usually if there is something that is not so good things happened, we do not reveal it we try not to drop their water face.. something like that.. and its for the department status… we don't want to look bad.*

MOH-01 *Regarding peer reporting.. Maybe its culture..... like sometimes.. I come up with this..... Complaint... we talk within my colleague...then when I say.. we should report this... but the other will say... please remember that... they are also nurses.... it comes back to us..... we just... put it behind us... so its not an issue any more.... but we among nurses we know but we don't story.... it to others....*

It was also reported that in some instances, colleagues or friends and even family may put the stakeholders under pressure or in an uncomfortable situation when they request the stakeholders to share and disclose some information. This information might be confidential and sensitive, but because they are related or know each other it is hard for them to turn down the request.

MOE-01 *Its normal for our people, they want to know what happens to others... busybody sometimes.... even sometimes looking into papers they shouldn't do... but sometimes because they are colleagues or friends we let them go.*

MOHA-02 *Sometimes officers are under stress, so they release confidential information to counter hearsay or incorrect stories told by the public. In one specific situation, an attending officer put confidential information on the social media just to put right stories that were told incorrectly by the media and public.*

Staff relationships are close; many are family tied therefore so it is immoral not to trust others. Rules and regulation are often overridden due to the paramount level of loyalty to the group, friends or family.

MOF-01 *Because sometimes for staff related matters like those who were given disciplinary that one considers like very confidential so we cannot disclose to others but only to the relevant parties.*

People are looking to each other. Password sharing is common because of this close-knit society. Wrongdoing or breaches are seldom reported to save face.

PMO-03 *We are not really, we always have pity on people and have mercy and very compassionate especially if it's amongst friends. We usually say it's ok even if it's not. We are like "I don't want to disappoint him. We want to protect his feeling.*

Normative beliefs play important roles in the context of culture. If the stakeholder is perceived that their significant others (in this case, their peers and superior) expect them to exercise certain action towards any information needs, then this may encourage them actually to display such behaviours. This is particularly valid in the context of culture and customs. It is expected that someone have to respect the traditional and the widely accepted behaviour. Culture in this regard comprises of the national culture and the organisational culture. National culture relates to a held values practised by the community for example what is good and what is bad, normality against abnormality, what is safe and what is considered dangerous. National cultural values are learned early, held deeply and changed slowly over the course of generations (International, 2015). Organisational culture, on the other hand, comprised of guidelines that are rooted in organisational practices that are learned on the job.

Closely related to the Bruneian Culture is the issue of trust. Trust is one of the factors that was frequently mentioned by the stakeholders when discussing why certain information security issues happen. Being trusted and giving trust are some of the sentiment that relate to the security of information. It is gathered that trust in the context of this research findings can be categorised into three meaning. Trust may represent belief, confidence and reliance/dependence. The significant of trust within the information value processes are signifies through the excerpts below;

> **MCYS-01** *back to our culture in Brunei ...we tend to trust each other... we are like family... although sometimes we know that this person can do bad things... we believe that they can change... and by giving him the trust he may change...*

Password sharing and information sharing exists because the person that disclose the information or password has the confidence trust that the other person will not abuse the information and will not perform malicious activities. Many also believe that with the general upbringing of people in Brunei, which relates to the enrichment of one's faith that one need not have a prejudice attitude towards others, one must believe that others act with good intention. Obeying rules and regulation as well as respecting a higher authority is demanded. In order to be trusted, the trustee is expected to have a responsibility, this may

include his or her ability to adhere to rules and regulation and display good ethic and behaviours towards information and its protection.

Trust is also translated in the reliance or dependence of the stakeholders on security personnel to look after all their security issues. When a stakeholder placed total trust on others to maintain the security of the information they are handling this will produce a slack approach towards information security compliance. For example the saying such as "if anything happened, our security personnel are always at hand" and "it's not my problem, the security guys should take care of it" are common.

Another form of trust is based on relationship. Due to the country's small population, it is not uncommon for stakeholders to know each other from outside the organisation boundary and some even have family ties. Common race and religious beliefs strengthen the close-knit community. Due to these factors, trusts between people are strong and many believe that because they are family or close friends, the other person can be trusted.

> **MOE-03** *Sharing password happened when both of them really trust each other. Trusting the person, like trusting the person of not doing anything unnecessary. So meaning that if you trust somebody, u will share your password if you fully trust the person.*
>
> **MCYS-01** *they trust each other I believe so.... when we want to access... they sometimes give their password straight to us,.... without knowing whether we are staff or not ,somebody may come over and act like they are one of the staff....and do bad things and steal information.....*
>
> **MID-02** *I would probably ask another person (person on duty) to secure all the documents and since the person on duty is always young people and new in the army they will lock up and close the light and And get out as soon as possible.*
>
> **PMO-10** *Well as I said Brunei culture, friends and family always share. This is the main issue. For strangers, they will not share, but with family or close friends they do*

The main problem with trust is that attackers or malicious individuals can exploit it. Trust is reported as the main way of access by outside threats (Cisco annual security report, 2014). Therefore, a community that based trust on customs should be concerned on the issues of information security. In the case of the Brunei's Public sector experience it is found out that trust is one of the factors (summarised under Cultural Demand factor) that shows primary

impacts on the antecedent 'Perceptions of Information Value' and the Workgroup 'Perceptions of Information Value'.

In both of the value elements as shown in figure 7.2 and figure 7.3, the impact of culture is seen from the side of restraining forces and is impacting both value elements at the primary level. This is because most of the reporting made by the stakeholders during the interviews, suggests that the cultural demands typically hinder their compliance behaviours. On the contrary, although most of the responses in the context of culture are seen as a restraining factor there are also some aspects of the cultural demand that can be manipulated to become a driving force. For instance, in the following response, although the stakeholder is describing the restraining elements of the cultural demand, at the end he also indicate that because of culture (being polite) people are obliged to comply to an information security countermeasure.

> **MOC-02** *That I mentioned about the cultural issue... implement security like ....we like to be seen as trusting community... in reality, we don't have that kind of trust... we need proof like e.g. ic and so on... giving IC (or providing information) to the bank or organisation is seen as normal to us.... for example being in an organisation building and when ask to surrender some personal information we will be obliged to do so and sometimes done voluntarily ... someone will think not only about its the policy but also rejecting these is seen as being rude*

To summarise the Cultural Demand discussion, it is important for any Information security training to be directed not only towards influencing individuals' IS security behaviour but also changing the work communities' prevailing organisational work practices. Developing the organisation's security culture could minimise risks to information assets and specifically reduce the risk of employee misbehaviour and harmful interaction with information assets (Da Veiga and Eloff, 2010). It is argued that employees' IS security behaviour consists of such shared organisational work practices, which, along with formal IS security policies, depend on organisations' unwritten culture (Dhillon 2007) which defines what kinds of behaviour are seen as acceptable and unacceptable.

7.4.2 Holbrook's Dimension of value

One of the questions that needed to be addressed by the study was to understand how stakeholders perceived the benefits of complying or non-complying from the various dimension of value. Since there is no specific dimension of value described in the information security and information security compliance literatures, the Holbrook Value Dimensions - used to understand customer valuations of product and services - was adopted and adapted.

Initially, the four dimensions of value: the economic value of efficiency and excellence; the social value of status and esteem; the hedonic value, and altruistic value of ethics and spirituality were included in this study. During the pilot study, participants were asked to relate their information valuing processes with respect of Holbrook's four main dimensions of value .Ultimately, based upon the results of the pilot study, only the social value and altruistic value were found to be influential, and therefore addressed in the main study. Although economic value was not explored under the Holbrook's dimension, it was mainly explored and frequently expressed and categorised by the participants under the monetary value under importance matrices. The hedonic value was not mentioned at all during the pilot study and even it was brought up in the main study, none of the participants was able to associate their valuation under such dimension so the hedonic value was dropped from the study. The findings with regard to the social and altruistic dimensions are presented in the following sections.

7.4.2.1 Spiritual

Spiritual is a combination of Holbrook (1996) dimensions of ethics and spirituality. Because the nature of the two dimensions are related and the categories that define them such as justice, virtue, morality, faith, ecstasy and sacredness define similar justifications the two dimensions were combined under the title altruistic (Sánchez et al., 2008).

In this study, the element of Altruistic that commonly appears in the interviews is the element of faith and virtue. Virtue is mainly expressed regarding being nice to people by doing good deeds. Virtue is also defined as being in complying behaviour as an obligation towards their faith.

Brunei Darussalam officially proclaimed that the national philosophy is “Melayu Islam Beraja” (MIB) or Malay Islamic Monarchy. MIB constitutes the blend of the Malay language culture and Malay customs, the teaching of Islamic laws and value under a monarchy system, which must be esteemed and practised by all. Religion is an important element in influencing stakeholders’ behaviour with information security. In Islam information is viewed as very important assets that help in gaining knowledge to maintain an Islamic society which is prosperous (Zulhuda, 2010). Some people’s value of information is greatly influenced by their spiritual beliefs i.e. the charter outlined by their religion. Brunei being an Islamic country and majority claimed to be devoting followers believe actions such as obeying the superior, honesty in every transaction and upholding trust are obligations. Additionally, from an Islamic perspective, both the Qur’an and the prophetic traditions (Hadith) provide an indication on proper handling of valued information to maintain its security. For example, as reported by Zulhuda (2010) one of the elements that are mentioned in the Qur’an is important of information authenticity because the unverified authenticity of the information source may bring about uneasiness, defamation or loss to others.

Confidentiality is regarded as a trust (Amanah) in Islam. It is the obligation for someone intrusted to convey a massage to someone to preserve the confidentiality of such message. Breaching a secret is forbidden if it involves harm or lost. Therefore, it is also an obligation for them to comply with any rules, regulations and policies implemented thus evidenced in their actions towards compliance with information security countermeasures. The following responses suggest that spiritual aspects may become driving factors towards appropriate valuation of information:

> **MOC-02** - *the altruistic value of religion.. Especially in this country it's a key role to help the development of I think security measures online and how you treat information online because... if we do show the desire to help other people ... we wouldn’t spread information that is fake. We would check it first.... if it's true before I send it out.. and if we really do leave up to expectation....that our... spiritual expectation then we really wouldn’t be selfish in doing so…*
>
> **MOE-01** *We want the sustenance from our work is blessed. The important thing is we need, to be honest in our work; we will fill blessed with satisfaction. We put our trust*

in Allah (SWT).

A practitioner of religion will see complying with information security countermeasures as a ritual demand and as an obligation to be fulfilled. According to (Rokhman,2010) Islamic work ethics, an orientation towards work and approaches work as a virtue in human lives significantly and positively affect job satisfaction and organisational commitment. Among the items measured and believed to be an Islamic work ethic are that one should constantly work hard to meet responsibilities and the willingness of an employee to put in a great deal of efforts beyond that normally expected to help their organisation to be successful. The following excerpt strongly suggest that religion or spiritual can become the driving factor behind appropriate valuation of information and the adoption of good information security behaviour:

> **PMO-04** *in Islam we must base our behaviour on submission to Allah (tawakal), this include abiding by rules and regulation.*

Muslims believe that the value of work does not merely depend on the results but rather more on the accompanying intention of doing the work. Under the Islamic work ethic, for example, laziness is seen as a vice, dedication to work is a virtue and good work benefits both one's self and others. From the Islamic point of view good ethic (akhlaq mulia) must be incorporated at every point and dimensions, including the security of information. This is embraced from the tradition of the prophet Muhammad that a Muslim should possess a magnificence akhlaq (ethic) towards anything. This also indicates that moral values and ethics are very much central to the Muslim life. These beliefs were reflected in the interviews with the stakeholders. Therefore, if one has good intentions such as being committed to the organisations and abiding by all rules and regulation, then improvements in compliance are expected.

Therefore, due to the notions and the reasons mentioned above, spiritual as a factor is seen as a secondary influence on both the value elements as shown in figure 7.2 and figure 7.3. It is also concluded that the spiritual is considered as a driving forces, which encourage stakeholders to perform better towards information security compliance. This finding opens

up the opportunity for management to take advantage of manipulating or using 'spiritual' as a selling factor to improve information security compliance behaviours.

7.4.2.2 Social Value

Originally, Social Value was described by (Holbrook, 1996) as two separate value dimension of status and esteem. Holbrook (1996) list success, impression and management to be underlying status while reputation, materialism and possession make up the esteem value. Later status and esteem dimensions have been combined under the heading 'social value' (Sánchez et al., 2008) because the two categories are closely related and overlap each other dimensions.

Social is all about how a person perceives significant others, and ultimately evaluates them. The social norm is described as the acceptable behaviour or cues amongst a group of people or society. This includes de facto on rules of what is appropriate and inappropriate, beliefs, attitude and behaviours. Social value is also about esteem, which is defined with the words respect and admiration. Esteem is also associated with approval, popularity, honour recognition and praise. All these nouns represent the view of other people expressed their admiration, recognition and the praise they offer to someone because of certain action or behaviour. For example, if a stakeholder cares about self-esteem he or she would display the appropriate behaviour to get approval from others.

The social value may have both good and bad impacts on how stakeholders assign a value to their information. A positive influence may come from the needs of getting approval, praised and respected from others and copying appropriate or acceptable behaviours displayed by others. Unfortunately, if the social norm of the organisation is not in favour of good behaviour, this may influence the stakeholders 'Perceptions of Information Value' thus determine his or her choice of behaviour.

The social value as an influencing factor is what is called a double blade sword; it can be either a driving factor or it can also become a restraining factor. As shown in figure 7.2 and figure 7.3 the Social Value impacts both the value elements from both sides (driving and restraining). Although in both value elements, the Social Value influences are seen as secondary but nevertheless, they are playing important roles in manipulating and

influencing the decision-making process of the stakeholders. The following excerpt suggests that Social Value could create both good and bad influence. Therefore, it is important for management to monitor the social norms of the organisation so that they can use this factor as a driving force.

> **MOE-02** *In my previous office compliance to security procedures are high, everyone looks after each other, they will tell you off if you don't do it right. Here it is different compliance lacking, being compliance is out of the norm, others will see you differently if you follow the book.*

There is always a tension between the choice of information protection and information disclosure when faced with pressure. The concept of public good comes into the picture, the tension between disclosing something and creating panic and failing to protect people because they could have known about it or accused not being transparent if something believes to be of public interest.

In some instances, stakeholders reports of having to resort to behaviour that could compromise the security of their information due to being pressured by their superior and peer. There are some cases where public persistence pestering could result in the stakeholders succumbing to their request to share classified information. Pressure comes in two forms:

- **Pressure from superior**: although most request comes in from direct superior in some cases request for information also comes from higher-level authority that does not directly concern the stakeholders. User level staff have the beliefs of a request from higher authorities should be attended without questions.
- **Pressure from peers**: This form of pressure are more common an example would be colleagues want to know about specific situations and insist on some information although he or she knows that it is confidential.

The following excerpt from the interviews indicates the impact of social obligation in the form of public, peer and superior pressure. Most of the time stakeholders are aware of the information security issue but due to what they perceived as their social obligation inappropriate actions were taken.

> **MOHA-01** *you cannot say no. People will hate you. Why do I have to share, this is not*

right… so people will hate you for that. So, in a way, in the person mentality, "oh no.. this can't be it… people will dislike me. I don't want that… So, that's in the mindset of Bruneian.

PMO-14 *recently my head of unit... texted me to borrow my PC I cannot give you my password... because it's also linked to my e-mail... she can also access to my shared network.....she wanted to use application on my PC.... I never share my password, but she is my boss.*

MOHA-04 *Behaviour towards information security sometimes depends on hierarchy of commands... if someone with higher rank ask for information.... it is shared without question*

MOHA-06 *"sharing confidential information cannot be done... it considered confidential.... but if the officer… wants to read them then we have to give it to them.....*

PMO-07 *I will share (password)… With him (colleague) if it's necessary... let say if he uses my e-mail to email someone else.... we have PKI (public key infrastructure) I will e-mail the people and tell them that it was not from me....*

MOE-02 *one thought... we will be more careful and secondly be more organised... then people will not be hesitance in working with us… excellence and it gives motivation to us....*

7.4.3 Sensitivity of information

In some instances, the valuation of information was based on the perceived sensitivity of the information. Sensitivity becomes one of the factors that were mentioned to have significant impacts on the stakeholders' valuation of information. Sensitivity here is defined, as the tendency of the information if misused or leaked will cause other people to be upset, particularly if it is associated with their dignity. This dimension derives from the users' awareness and understanding of the feelings of other people. For example not disclosing penalties carried out on breaches to avoid shaming the perpetrator. In other cases, information is secured to protect the victims and their family honour of certain tragedy, for examples in rape cases and health conditions.

The sensitivity of information varies according to the context in which it is used. Sensitivity in this context is defined as the process in which a stakeholder evaluate whether the information he or she possessed or handled, if not appropriately will;-

- Have consequences on his or her job.

  MOD-01 *it is my responsibility to protect the information I deal with, if I don't there must be some consequences, it's a way to secure my job.*

- The misuse of the information creates unwanted consequences to the public**.**

  MOHA-02 *Cases of rapes are seen as very sensitive as this may raise anxiety amongst the population but on top of that, it was to avoid shaming the victims. Example, in the case of rape cases... sometimes... the family of the victims "humiliated" ... a lot of them, the family does not want other people to know....*

- Will have an impact on other people, especially people close to them i.e. family, colleagues and friends.

  MOF-01 *Cases disciplinary actions taken on staff are considered very confidential, this we cannot disclose to others. Only known to relevant parties, this is to avoid defaming the staff and their relatives.*

- Will have an unwanted impact on their department, organisation and even the country.

  PMO-18 *Staff salary information is very sensitive, people should not have access to other people salary information... some people may questions if their peer salary is higher than them.*

The above points and the responses associated with them show that sensitivity of information does play a great role as a driving factor towards appropriate information value assignment amongst stakeholders. Users are more willing to comply with information security countermeasures to protect information if they think that the consequences of a "breach'' or misuse of the information can affect someone, especially peers, co-workers, friends and family. On the other hand, if they think that the information is less sensitive they tend to apply a less strict security measures on it. This notion is suggested in the response below:

> **MOHA-01** about *my work, I believe the information is not really, not have to be secretive (this person is working with inmates information). So I can be relaxed with the security.*

It is also noticed that if according to the perception of the stakeholder the sensitivity of information is high and the information is significant to the well-being or safety of their

family, extended family and friends they will have the impulse to share the information with them. An example of this is stakeholders in the enforcement agency that have information on increasing crimes that are not publicly announced would have the urge to share them with their family due to his or her concern for their wellbeing. The above notion is evidenced by some of the excerpts from the second phase of data collected;

> **MID-2-01** *Some people are only concern about their family, they text their location so their family will know their whereabouts without realising this might compromise their location (Military personnel during training).*
>
> **MOHA-2-01** *personal take pictures of incidents and send them to their family with the intention to inform and warn their family although some information is sensitive.*

The Brunei Darussalam Penal Code (1998) and the Protective Security Manual (PSM)(2009) outline four main classifications of information. These are Big Secret, Secret, Confidential and Restricted. The PSM clearly defines that information must carefully and clearly be identified according to their appropriate classification. Applying too high or too low a classification would result in a dangerous situation. This for instance creates the false perception of some stakeholders. The perception is that information that does not fall into the four categories of classification is considered as unclassified information. It is also perceived that once the information reaches the user level of organisations, it has lost its classification and it may be held as unclassified.

> **MOHA-03** *for me all the confidential information, will be handled by my office, they will know if it is sensitive or confidential. All this information will be handled by a designated person so other staff don't know about it.*
>
> **PMO-13** *classified information... will be a marked on the letter.... they will put it in a plain envelope address to this department with only their department stamp on it but inside sometimes I will find letters marked confidential... then I will open the letter.*
>
> **MOE-02** *This is one of the problems in our organisations in Brunei... we are 'sharing and caring' the info are not really labelled top secret... especially all the information that we get from the teachers.., we need to evaluate the information from the teachers for our national curriculum,.... supposedly some of the data should be restricted....*

The problem with these perceptions is that when users are assured that the classification of information has been sorted out, they think the information they have is not important and confidential. This may lead to the perception that information they are handling needs less, or no protection at all.

7.5 Concluding Remarks

In conclusion, this chapter outlined and presented factors that were found to have a significant influence over a stakeholder's value assigning process. The presentation of the analysis of the factors is critical to this study, as it has provided many useful insights into the various factors that can indeed be beneficial to organisations. Organisation can learn from the findings which factors exist within their organisation and may use these factors to enhance their stakeholders' information valuation processes.

This chapter through its analysis of the factors has provided insights on ways the factors could impact the stakeholders' value assigning processes both from an individual perspective as well as from the perspective of a group of stakeholders. Therefore, it can be concluded that the third research objectives have been reached through the realisation of the two sub-objectives mentioned earlier.

The presentation also provided insights into how these factors could be manipulated to encourage stakeholders to assign an appropriate value to the information they are handling. More importantly, this chapter has provided empirical evidence that the mentioned factors are indeed significant in influencing the value assignment processes.

8. Conclusions

8.1 Introduction

The overall aim of this research was to explore the potential of ‘‘perceptions of information value’’ as an alternative to understanding and consequently improving information security compliance behaviours, particularly in Brunei’s public organisations. The research was initially motivated by the use of ‘‘perceived value” on objects such as product or services in the business field, which when properly manipulated can improve the perceptions of value on the goods or services (Huang and Cheng, 2013; Liu and Yang, 2014).

The objectives which contribute to the fulfilment of this aim have been achieved firstly through a review of the literature. Subsequently, an intensive, qualitative approach based upon an interpretative-constructivist philosophy has been successfully used to undertake a set of exploratory and explanatory interviews with various stakeholders in the information security setting. These provided a broad overview of processes in information value assignment, building on the issues found in the extensive review of the literature and identifying influential factors. Further interviews with stakeholders from various public organisations built upon the findings from the previous stages by examining the views of those directly involved in information security. The philosophy of interpretativism-constructivistism that underpins this research focuses the researcher on uncovering unseen structures and mechanisms that influence behaviour (Gary, 2009; Thomas, 2006). This emphasis has been usefully applied in this research, resulting in an analysis of the data gathered which enabled key factors underpinning selection of information security compliance behaviour to be identified and a conceptual model of these factors to be developed.

This final chapter of the thesis will present a summarised narrative of the analysis and the contributions that have been derived from this study. This chapter will start with the conclusion on the general findings of the research followed by a conclusion discussion of the key findings in relation to the initial research objectives (outlined in chapter 3).

The contributions of the research will be highlighted followed by the presentation of the implications of the research acknowledging its limitations and highlighting opportunities for

future and further research related to this one. Recommendations based on the findings and analysis will also be presented as in the final section before the chapter is ended with the concluding remarks section.

8.2 The Information Security Landscape

This section reports on the current situation and setting of the information security landscape of the Bruneian Public Sector as being reported by the stakeholders. This is also a presentation of some general findings that are significant to the issues of information security particularly the issues of compliance behaviour.

8.2.1 Respondents' Background

In order to maximise the possibility of learning and to understand the issues of information security compliance behaviour, different levels of stakeholders were selected as respondents. Ultimately, the stakeholders represented three distinct levels, namely: the management or owner of the information; Information Technology or information security related stakeholders (IT/IS personnel); and general stakeholders (information users). The recruitment of the three different levels has given the research more perspectives and has enriched the data collected. From the multilevel perspectives, it was possible to create a comprehensive understanding of the issues under study. Particularly the views of the different stakeholders have created gaps in current understanding of issues such as on awareness, education and training, policies, procedures in dealing with information and how best to protect the information.

Generally, all the participants of the research are involved in dealing with some kind of information in their work. Although referral to the terms such as 'information security', information protection and 'perceptions of information value' were not commonly made, from the what the stakeholders said, they have make implicit use of, and act upon, such terms. One of the most important processes identified in the research is the process of assigning a value to information. Subconsciously all the stakeholders go through very similar processes when deciding the course of action when it comes to the security and protection of information. Due to the rich experiences of the stakeholders, it was possible to have a

comprehensive view of the how stakeholders develop their perceptions of information value.

8.2.2 Attitudes towards information security

It has been found that the current situation and attitudes towards information security are sporadic. The term sporadic has been used in the sense that there are a very wide variety of views and perceptions about information security, expressed either directly or indirectly by stakeholders. For example, the stakeholders possess different levels of awareness depending on their fundamental training and education. Stakeholders that were exposed to more training or have been educated on issues of information security will generally have more positive attitudes towards information security. Although the importance of training and education, about information security, has been underlined by many stakeholders, at all the three levels, unfortunately, the provision for training and education are not particularly well developed. Many stakeholders expressed their concern because no training or education was provided where they need it the most. This condition has created diversity in the stakeholders' perceptions of the value of information. Notably, stakeholders that have not been sent for training and their work involves information that they think is important may have a divided perception. Although they perceived that the information they handle is important, yet they were not given any proper training on how to manage them.

Another realisation on the stakeholders is that their normative belief is quite strong. Generally, stakeholders try to behave consistently with the prescriptions of significant others. Two important issues arise from this situation. Firstly, misinterpretation of important others perceptions on the value of information or on how better to handle the information may occur. Even on a clear term of information can be misinterpreted (Cherdantseva and Hilton, 2012) let alone the subjective important others perception. A false impression on the significant others' perceptions on the value of information may result in the stakeholder adapting the same poor perception the significant others have. Consequently, this may result in the adoption of an inappropriate set of behaviours.

Secondly, even if the interpretation of the significant others' perception is made correctly; they still may have a bad perception after all. This again may result in the stakeholder

adopting the wrong perception and may lead to undesirable consequences. This situation is heightened if the stakeholder's sole reference to information value perception is based on his or her normative beliefs. This is why it is important that the stakeholder base their valuation on the value of information based on several sources. An especially important source would be the value espoused by the management. The issues surrounding espoused value on information is discussed in the following section.

8.2.3 Awareness, education and training (AET)

It was found that AET has a significant impact on the perceptions of information value. Stakeholders that have undergone awareness programme and some amount of education and training on information issues (security) shows that they are more knowledgeable on the issues discussed in the interviews. This supports the suggestion by (Jenkins et al., 2012; Puhakainen and Siponen, 2010) that having sufficient level of AET will provide a stakeholder with self-efficacy in terms of protecting information. It is also realised that stakeholders deprived of any awareness programme, training or education initiatives may have false perceptions about the reason they were not given an opportunity for training. One of the impacts of not being invited to participate in training might be to adopt an inappropriate inference about the importance of information. Stakeholders felt that the reason they were excluded from any training or awareness programme is that they don't need it as the information they are handling needs moderate protection or no protection at all. They also believe that people sent for training deals with important, confidential or sensitive information and this is the reason they were sent for training.

The current landscape of AET from the perspective of information security indicates two main issues. Firstly, there are insufficient training opportunities and more often that there is a mismatch of training to the needs of stakeholders. Therefore, it is important to provide AET for all level of stakeholders as to avoid misconception and information security AET should be seen from various angles, mainly how stakeholders view them. Secondly, failure to understand the needs of the different stakeholders on the kind of AET are common. More often, training is standard and not tailored to the specific requirements of the

stakeholders. Therefore, the needs of AET of stakeholders from all level should be clearly identified and understood in order to provide for a more efficient AET.

8.2.4 Policy, rules and regulation

Brunei Darussalam a developing country can be considered at the early stage of the development of its information security policies, infrastructures and behaviours. Generally, the awareness on information security is at an acceptable level but there are a few issues that may cause confusion amongst stakeholders. As mentioned in previous chapters (chapter 2 and chapter 5) the availability of policies or any sorts of guides is essential in order to guide the stakeholders in the correct direction (Doherty and Fulford, 2006; Herath, 2009; Ifinedo, 2012; Stahl et al., 2012). From the perspectives of the stakeholders, the provision of proper policy and rules on information security and information protection are necessary. These documents are part of their reference to realise their responsibility towards these issues. This is also echoed in the findings by (Rees et al., 2003). More importantly, the appropriate form of regulation must be available to support the mandated policies and rules. If necessary management of standards and procedures were not in place, the effectiveness of such documents will diminish. Stakeholders will not believe in the information security policy if they do not see the commitment from the organisation to carry out the punishment accordingly. This notion is supported by the research by (Höne and Eloff, 2002). Moreover, documents such as policies, rules and regulations are medium which enable organisations to communicate the 'espoused' value of the information they are handling. With such documents, stakeholders are able to gauge the importance of the information according to the sets of expected behaviour stated in the documents (Alnatheer and Nelson, 2009).

Despite acknowledging the importance of documents such as the information security policy, it is found out that organisations in Brunei Darussalam are behind in rolling out such documents to be referenced by their stakeholders. Even worse in some situation the organisation believe that by solely providing high-ends technical countermeasures they are already well protected despite lacking or missing proper policies. Moreover, the organisation found that through the installation of such protection, stakeholders would

spontaneously comply and they will have the correct perception towards information security. These beliefs have created a gap in perceptions between the organisation and their stakeholders (D'Arcy et al., 2009). Where organisations failed to provide appropriate policies or rules on information security, they often also failed to espouse accurately a suitable value on the information they have. From the perspective of a stakeholder, the missing policy may indicate the triviality perception of the organisation over the protection of their information. Some stakeholders have also expressed their concern over the vague or unclear content of policy. For example, confusion arises when labelling information stakeholders are often in dilemma under which label their information should be categorised under and as a result the wrong level of protection is assign to it.

8.2.5 Cultural aspects

One of the important factors that are highly significant to the formation of information value in the context of Brunei Darussalam's information Security landscape is the element of culture. The etiquette and attitude are deeply rooted in the culture of the country. Customs and beliefs are also moulded around the concept of culture that has been inherited from the previous generation. The culture here consolidates the national customs and beliefs as well as the public organisations' customary ways of doing things. One important inference that can be made from the data collected is that the organisation's culture is built on the shared customs and beliefs of the community (nation). It is believed that a contributor to this issue might be the domination of locals compared to expatriates working in the public sector. Therefore, the national culture was managed to be preserved and in line with previous research, particularly by (Salleh and Clarke, 2009) the impact of culture plays a major role in Bruneian workforce decision making.

8.3 Key Findings

This section presents a summary of the key findings in relation to the three research objectives that have guided this research. The research objectives are outlined in section 3.3 in chapter 3 of this thesis. This approach, by bringing together all the research findings into single section will help in centring the whole discussion into perspective from the overall context of the research.

8.3.1 First Research Objective.

To understand the extent to which stakeholders develop clear 'perceptions of information value', and the processes by which they assign value to the information that they handle.

The first research objective comprises of three sub-objectives (goals) with the main aim to explore the role of 'perceptions of information value' in the context of information security. The investigation of the concept of 'perceptions of information value' and its roles was presented in chapter 5. The first part of the objective is to explore the concept of 'value' in the context of information handling and information security, to understand how meaningful this concept is from the perspective of stakeholders. The second part of the objective is to explore whether 'perceptions of information value' vary from the perspective of different groups of stakeholders. The third part of the objective was aimed at understanding the overall approaches by which stakeholders assign a value to information, particular in relation to its protection and security.

The term ''perceptions of information value'' was derived from it's used in the marketing and object evaluation process. In the marketing area, the 'perceptions of information value' of an object (including services) significantly drive the price of the object and influences the willingness of customers to purchase the object or subscribe to the service. Although no reference was directly made to the term ''perceptions of information value'', in the context of information security within the literature, quite a number of references were made to users' perceptions on other security issues. For example, perceptions about the severity of penalties by (Kankanhalli et al., 2003; Li and Chen, 2010); perceived costs (efforts) (Beautement et al., 2008) and intrinsic motivations (Herath and Rao, 2009). Clearly, the

issues perceived by the users are more external to the users, more on the mechanism or subject that are imposed on them rather than their personal internal feeling towards the subject or object.

With particular reference to the first part of this research objective, clear evidence was found that stakeholders assign a value to the information they are handling, which is their ‘‘perceptions of information value’’. The process in which the stakeholders’ ‘perceptions of information value’ is conceived is labelled as the information value assignment process.

Meanwhile, in relation to the second part of the first research objective, it is interesting to note that different stakeholders have different ways to express the ‘perceptions of information value’ of the information they are handling. As a matter of fact, different stakeholders (more obvious from different categories of stakeholders) relate their Information Value assignment processes based on different factors. These factors are deemed by the stakeholders to have significant impacts on their information ‘perceptions of information value’ assignment. A discussion of these factors is presented in detail in chapter 7 of this thesis.

In relation to understanding and appreciating instances of value creating process and value creation activities that might significantly Influence ‘perceptions of information value’, they were derived from the key themes detected from the analysis of interview data as well as the insights made from a comprehensive review of associated literature on the issue. There is clear evidence to suggest that there are various stages in the development of ‘perceptions of information value’. There is also ample evidence to show that these stages arise from the different lenses adopted by the stakeholders, as presented in detail in chapter 6.

8.3.2 Second Research Objective

To explore and understand the relationship between stakeholders' 'perceptions of 'information value' and their resultant 'information security behaviours'.

- To explore whether there is relationship between stakeholders' *'perceptions of 'information value'* and their resultant 'information security behaviours, and the extent to which this is mediated through 'intention to comply'';
- To explore and understand how a stakeholders' *'perceptions of 'information value' is affected* by other stakeholders' existing information security behaviours.
- To explore and understand how a stakeholder' 'perceptions of information value' is influenced by the results of their own 'information security behaviours.

This section will present the discussion on the second key finding, i.e. the process of information value assignments. The broad aim of the second research objective was to explore and understand the processes by which stakeholders assign a value to the information they are handling.

Therefore, in relation to discovering the second research objectives, the analysis of the interview data; provided clear evidence to confirm the existence of a comprehensive process of assigning a value to information. The result of such a value assigning process is the creation of a 'perceptions of information value'. The findings under this objective are manifested in the form of a model (Figure 5.3). It is important to highlight that although it is found that stakeholders manifested the processes of value assessment and assignment to the Information they are handling, these are mainly done sub-consciously without them consciously understanding the potential of this process. Therefore, it is suggested that this process should be exploited and manipulated to help in developing better information security compliance. It is also believed that if a stakeholder is conscious of the process and understands how the process works they would yield better PIV towards the information they are handling.

8.3.3 Third Research Objectives

To understand the factors that influence the stakeholders' 'perceptions of information value', which in turn affect their resultant 'information security behaviours.'

- To understand the factors that influence the stakeholders' perceptions of information value from an individual perspective.
- To understand the factors that influence the stakeholders' perceptions of information value from the perspective of a workgroup.

Under this objective, a number of interesting findings were made. As a result of the analysis of the research, validation on one of the assumptions made earlier in the research (section 3.5) which in part state that several influencing factors have influence over the value that is assigned to a specific information asset by the stakeholders. The impacts from these factors are from the perspective of the stakeholders. Initially, there were few pre-determined factors that were brought into the studies. Additionally, throughout the studies, it was found out that other factors are significant in influencing the information behaviour of the stakeholders. A total of nine main factors were ultimately discovered through this study. From the initial four main dimensions from the initial interpretive model (figure 3.4), based on the findings from the interview data the factors evolves into nine factors.

The significance of these factors was discussed in chapter 7. Various perspectives such as how a factor might become significant, the relative strengths of different factors and the extent to which factors either encouraged or constrain appropriate behaviours were all studied. Among the findings, it is found that different type of stakeholders might be affected by various factors and the intensity of the effect of a factor differs for a different type of stakeholders. There are also factors that have a common influence on both individual stakeholders and a group of stakeholders.

One factor that was found to have a particularly strong influence upon the stakeholders' Information Value assignment process is culture. Culture in this context is a mixture of the nation's perspective as well as the culture that belongs to a public organisation. Since locals dominate most of the public organisations in Brunei, it is no surprise that the organisational

culture is similar to the national culture all along. The culture at the Organisational level in Brunei Darussalam is adopted or largely influenced by what is experienced by its national culture, customs and beliefs. In most places in the public organisations, ways of doing work are not exposed to other than Bruneian culture as a number of foreign workers or expats are very minimal. Although from the perspective of education, most staff are overseas trained, it might be anticipated that such external influences might affect behaviours. In reality, due to the strong influence of the 'Malay Islamic Monarchy' philosophical doctrine, the adherence to local customs, culture and beliefs dominates.

8.3.4 Validation of Assumptions

There were a few assumptions made at the early stages of the research. The assumptions act as support for the objectives of the research. These assumptions support the research in terms of interpreting the issues surrounding the area of research. One problem with the assumptions is that as they are part of an implicit belief system, they may be difficult to verify. However, to be able to make inferences about any assumption, it is still important to attempt to validate and proof that the assumptions are valid and supported.

Initially, there were five assumptions made as listed below. All of the assumptions were made base on the validity that of the existence of 'perceptions of information value'. Results obtained from the analysis of the data collected for studies suggest that there is a substantial ground to accept the assumptions as accurate and valid statements.

Assumption 1: The intention to exercise appropriate behaviour is influenced by the variation of perspectives of stakeholders on their 'perceptions of information value' of the information they are handling.

The existence of 'perceptions of information value' is reported under objective one in Chapter 5 of this document and the above assumption is profoundly related to the first objective of the research. With ample evidence from the data collected, it is suggested that the above assumption i.e. intention to exercise or adopt a behaviour is strongly influenced on how they perceived the value of the information.

The next assumption is also related to the first objective of this research. This research also claims the validation of this assumption in which the value perceived by the stakeholder is strongly influenced by factors that are seen as important or significant to the value of the information.

Assumption 2*: The Value placed on information assets is dependent on the personal assumptions on several influencing factors (for example importance of information, and the sensitivity of the information)).*

Several factors were found to have significant or strong influence over the stakeholders, some of the factors were deduced from the literature and some of them have been induced from the analysis of the data collected. The findings of these factors and their relation to information security behaviours are presented in chapter 7 of this document.

Assumption 3*: The higher the value placed on the information assets (by the stakeholder), the higher will be the need to protect it, and the more willing the stakeholders will be to comply with security measures.*

The assumption above, which states that the strength of protection and the seriousness given to protecting the information depends a lot on its value, as perceived by the stakeholders. Therefore, this suggests an opportunity to manipulate the ‘‘perceptions of information value’’ so that stakeholders may be able to appreciate the protection need of the information they are handling.

Assumption 4: *The behaviours enacted by stakeholders will have an impact on the value of the information.*

The above assumption was able to be empirically proven to be valid and can be held as a true statement. This explicit assumption was discussed in detail in chapter 6 of this thesis. In a vice versa impacts of the stakeholders’ information behaviour and the value that they assigned on information, the impact or the outcome of behaviour does play a significant impact on how they align the value they perceived on the information and the behaviour associated with the information. For example, a stakeholder that perceived that particular information is important and needs a good level of protection may reassess his or her perception if he or she observes that his or her colleagues do exercise the appropriate

behaviour towards the information. Additionally, if the misbehaving colleague gets away with it, this will tarnish the initial value that the stakeholder had on the information.

Assumption 5: ***Organisational and national culture have a significant impact on how the stakeholders' approach the process of assigning value.***

Amongst the five mentioned assumptions, assumption 5 has perhaps provided the most empirical evidence, in support of its validity. The discussion of assumption 5 is presented in chapter 7. Strong evidence is provided that culture is one of the primary issues that has a substantial impact on the value assignment process of the stakeholders. For example, how information is value depends on a lot on how their predecessor deals with the information. A good illustration would be sharing of classified information; the Bruneian culture highlights the gesture of sharing of information, particularly with family and close friends. Keeping secrets is seen as a discourteous gesture, therefore sharing of information although it is classified is commonly seen as normal. Understanding the cultural issues of the country and the culture of the organisation provide alternative ways to explain the issues of information security compliance.

8.3.5 Summary of Key Findings

From an overall perspective, it is important to reflect further on the above findings and contrast these with the relationships that had been assumed in the conceptual research framework [see section 3.5]. In this regard, it can be confirmed that the predicted relationships [see figure 3.3] could be validated by the research.

Additionally, the research has managed to develop an interpretive model of how information 'perceptions of information value' works in the context of Brunei's public organisations. This is based on the stakeholders' Information Value Assignment process [see figure 5.3 and section 5.3]. Therefore, it is also possible to adequately substantiate the model to be valid and proposed by the research as an alternative reference to the formation of information security behaviour.

The model is also a valid alternative reference for the organisation to understand the mechanics of the formation of information security behaviour. For example, the model

should be able to assist in determining why some users adopt compliance behaviour and why certain users are reluctant to comply with information security countermeasures. Moreover, understanding the contributing factors of non-compliance behaviours would provide the opportunity for the organisation to focus on the root problem and provide a solution to it.

8.4 Contributions

In relation to the research contributions, the knowledge that this study is offering can broadly be divided into two key areas. The first area of contribution is regarded as directly arising from the various insights obtained from the exploration of the study's research objectives. The second area of contribution is in the form of a revised model that the study is proposing, which has been crafted mainly from the overall understanding and general appreciation of the research findings.

8.4.1 Contribution Arising from Research Findings.

This thesis has explicitly outlined an alternative way to understand the processes that are significant to information security compliance behaviour. This novel lens provides an alternative perspective on how to handle and manage information security compliance. Whilst prior studies may have suggested a number of other factors and different perspectives about how to improve information security behaviours and the more general improvements to information security, this research presents the stakeholders' ''perceptions of information value'' as an alternative way in which to interpret and ultimately manage security issues.

This research specifically contributes to the knowledge of information security and information security compliance through the notion that the information security actions or behaviours, displayed by stakeholders, typically result from a rationalised assessment of the value of the information they are dealing with. Moreover, the thesis has provided a richer understanding on how information is being appreciated by stakeholders who belongs to different levels in their public organisations setting. It is well evidenced that there are gaps in the understanding of the different level of stakeholders on issues of information security.

For example, the various stakeholders have a different understanding on which information need to be secure and how to best secure them. Gaps are also found in the needs and requirements of different level of stakeholders in order for them to be able to protect information as well as for them to be able to sustain their information security compliance behaviour. This is marked as another contribution of the research, in which the perspective or demand from the information owner (stakeholders) was explored, understood and presented. These findings were contrasted with information security from the viewpoint of lower level stakeholders who only work with the information but do not own it. It is clear that there is a gap between these two levels of stakeholders in terms of understanding of their responsibility for information protection and security. The gap also indicates that the expectations of the stakeholders on each other are also more often misinterpreted and misaligned, in that it creates inconsistency in the management of information security issues.

The findings of this research also present important insights into the valuations made by the stakeholders. The base has been developed into several categories, which are made up of several significant influential factors. The research also provides empirical evidence that indicates the significant impact of the explored factors on the stakeholders' valuation of the information.

This research also found that cultural elements are a widespread influence on the way people choose to behave or at least plan to act. Understanding the impact of culture, customs and norms on the way Bruneian in the public organisation will benefit policymakers, security analysts and the management of the institution itself.

8.4.2 Contribution in the Form of a Revised Model

Another novel contribution of the research has to be the introduction of a revised model. It is important to note that the revised model was not based solely on the appreciation and understanding obtained through the analysis of research data. It was also effectively based on a complementary review of the associated literature arising from the new information gathered by the research. Therefore, this particular model can be further regarded as having emerged from the appreciation of empirical data, as well as be based on insights obtained from the existing knowledge particularly pertaining to the related areas of interest

(information protection, information security compliance and information security behaviour).

The aim of the research was to explore alternative ways, to understand information security and the issues surrounding it. Moreover, it is postulated that through this improved understanding of the issues of information security compliance, it should be possible to improve stakeholders' compliance with information security countermeasures. Therefore, understandings learned in this research are consolidated in a form of model that was discussed in detail in chapter 5 of this thesis (figure 5.3).

The model provides an alternative perspective from which information security compliance behaviour can be understood. The model consists of information security behaviour variables and several elements that present different lenses of information 'perceptions of information value'. The model also provides important insights into the complex relationships between the 'perceptions of information value' elements. It is the product of these relationships that ultimately deliver the stakeholder's 'perceptions of information value'. Furthermore, the model also describes the relationship of the various value elements with the information security behaviours' variables.

Another important contribution of the research has been delivered through the exploration and refinement of factors that proved to have a significant impact on the Information Value Assignment. These factors make up the fundamental building blocks of information value assignment and where necessary manipulation of these factors may provide an alternative way to develop healthy compliance intention and healthy compliance behaviour towards information security countermeasures can be achieved. Another opportunity brought by the development of the model is that it may become a very useful tool for an organisation to better understand how their stakeholders choose their information security behaviours. This model provides a structured and systematic approach to determining the possibility and the feasibility of using ''perceptions of information value'' as an alternative to understanding information security compliance behaviour.

In addition, considering this revised model as one of the research contributions, matches with the theoretical foundation that have been adopted by this research. This research has

taken partly inductive perspective and at the same time leans towards two key concepts from the grounded theory for its approach to data analysis. One of the key concepts is in effect highlighting the motivation and intention to develop a theory out of the data. These activities so far are in line with the qualitative nature of the research.

8.5 Limitations of Present Research and Future Research

Inevitably any research would face issues that might contribute to some restriction on the research. This research, in particular, is not immune to a similar thing. This section presents some of the issues of limitation experienced during the research. Solutions and remedies taken to address the issues are also presented but for those issues that were not resolved in this research are proposed to be considered to be studied in future research.

i. Some of the interviewees were not very open to the idea of sharing their concern on the issues under study. They were quite reserved when answering the questions, and many offer a typical “I don’t know” as the answer. In most of the interviews, interviewees have to be coaxed into providing answering the questions. One way to persuade them to provide a reply is to provide them with leads to possible solutions.

ii. The terms used in this research such as information security perceived value, value assignment and valuation of information was not familiar to the stakeholders. Although they actually engage with such processes they usually don’t have any specific or standard terms to describe them. It was a tall task for the researcher carefully to align the terms with the actual experience of the stakeholders in order to define each term correctly.

iii. A big portion of the data was collected from interviews with stakeholders and is primarily based on the interpretative ability of the researcher. Research that involves human being is not freed from bias although steps such as triangulation and respondent validation were taken to reduce the bias.

iv. The data collected for this research are mainly based on the cases reported by the stakeholders in the interviews, focus group and the workshops carried out. It is thought that the use of participant observation might provide additional

perspectives to the research findings. For instance, researchers could collect data through observing participants' behaviour over a prolonged period of time by engaging in their activities.

v. There remains some data gathered from the two data collection phases that were not used in this research, for example, the background information about the research participants. This data could be utilised in the future research to understand the characteristics of stakeholders and the relation to their information value assignment process.

vi. The findings in this research are based on qualitative measures. Despite the validity of the results, it is thought that statistical measures on the level of significance of each of the factors identified in this research on the stakeholders' information value assignment might add a different dimension on the research findings. Therefore, this notion warrants a quantitative study as one of the future research.

8.6 Recommendations

Based on the findings and the key contributions made by the research there are a number of important recommendations that may act as guidelines for information security stakeholders in their struggle to achieve better information security compliance or at least triggers some thinking over the matters. The recommendations are listed below.

8.6.1 Understanding stakeholders' perceptions, needs and wants

In every system, the stakeholders are the major players that help to determine the success and unfortunately the causes of failure of the scheme as well. In the context of information security, despite well-managed technology and processes, it is the stakeholders' actions that are contributing to the successfulness of the system. In this thesis, it has been established that there are gaps or discrepancies in the perspectives of different level of stakeholders of information security. Therefore, it is crucial to learn and understand the issues of information security from the various perspectives. In this study, these views have been expressed in term of the different factors, which are deemed to be important by the stakeholders. Through learning and understanding of these concerns, needs and wants of the stakeholders, possible solutions can be provided to address them. For example, different level of stakeholders will need different kind or content of information security training.

As the stakeholders are at the centre of an information security process, it is important to adopt to a "stakeholder centred" approach towards the provision of training, awareness as well as the design and setting of the security environment.

8.6.2 Learning and understanding culture and customs

Another point that has been established in by this research is that there is a significant impact of culture (both national and cultural) towards information security compliance behaviour processes. Evidently, the culture of the country has some significant influence on how organisations operate. Therefore, it is important to understand the national culture as well as the acceptable customs in the organisation.

- **Understand the culture**

Culture, traditions and beliefs shape how people manage and take action on most of the issues they faced. Mostly culture is learned from others; from observing others and inherited in some cases. Therefore, it is imperative to identify those customs and beliefs that may promote bad influence or has a severe impact on the organisation's information security culture. For example, the custom that adheres to the notion of "caring is sharing" must be referenced to cautiously, particularly when the sharing concern confidential and sensitive information. For example exchange of account, password and controlled information should not fall under the caring gesture.

- **Work with the community**

In order to build a secure organisational community, the larger community must not be ignored. Evidently much of the pressure experienced by stakeholders on issues of information security for example information sharing comes from the community or their links outside the organisation. It needs to be understood that the blame of a breach shouldn't be directed towards stakeholders totally. Many of data or information breaches are fuelled by pressure by outsiders. Particularly, in a public domain where authority and hierarchal structure are observed it is not uncommon for stakeholders at a lower level to be pressured in a way that may end up for them to impropriate behaviours, for example, the disclosure of classified information.

8.6.3 Effectively and efficiently espousing value of information

Organisations typically provide a set of acceptable or expected norms or bounds of information security behaviour for the individual members of the organisation. This expectation is channelled through the stakeholders by making known how much the organisation value the information, for example, what and how the information can benefit the organisation. Without such process of the espousing value of information, stakeholders will, by default, follow their individual value systems. These may or may not promote behaviour that the organisation finds desirable. Therefore, it is important for the organisations to consider the following.

- **Transparency**

More often, stakeholders complained that they were 'kept in the dark' on issues regarding the importance of information to the organisation. These may include, improper documentation on how the organisation value the information they have as well as how should members of the organisation deal with the information. The provision of standard policy lacks in most public organisation. Although there is a standard manual on information security the reference to it was not straightforward. The manual was not freely accessible and it is deemed confidential. Many stakeholders have no knowledge of the existence of such standard and have never seen it. Therefore, it is important for organisation to ensure that all members of the organisations are aware of any information security documentation as well as ensuring that they understand what it contained.

- **Clear and comprehensive instructions**

Where policies are present (not many in the case of Bruneian's public sector), statements are commonly not clear and it is left for the stakeholders to make their own interpretation. More worryingly, the superiors that make the translations themselves are sometimes not well verse or re not sure on what the policy actually denotes.

What is more important is that language in which the policies or guidelines are written, is expressed in a clear manner, and is easily understood by all level of stakeholders. It is also necessary to highlight that the policy is directed to all level of stakeholders and all

stakeholders are informed of the policy; this step may be useful to remove the notion of "I'm nobody in the organisations".

8.6.4 Factors influencing information value

One of the important findings made in this research would be the identification of factors or variables that were found to be significant to the processes of value assignment by the stakeholders. These factors influence stakeholders' decision on the value of information and help in forming the stakeholders' intention. Subsequently, these factors indirectly determine the information security behaviours adopted by the stakeholders.

By identifying the factors that are most significant to their organisations, information security officers could develop an in-depth understanding of the behaviours displayed by their stakeholders. Consequently, these factors may be manipulated or be addressed in order to promote change stakeholders' behaviour intention and subsequently will determine the sort of behaviour they will adopt.

Therefore, it is necessary for organisations to investigate and explore what factors are significant, in the context of their own organisations, and use such findings to understand and improve the effectiveness of information security in their own organisations.

8.6.5 Accountability is the key

Another important finding made in this research is that the lack of responsibility amongst stakeholders. Statements such as '*this is not my responsibility, because…..*', '*it is someone else duty to do this*' and '*my work is not really significant*' are common amongst stakeholders. These statements lead mindset such as, *'I don't have to learn about security', 'security is not my responsibility', etc.* The prevailing mindsets such as these are not healthy for the organisations' information security as it may encourage stakeholders to undermine the importance of information securing. Therefore, it is important for organisations to highlight the importance of each and one of the stakeholders (including the importance of their work contributions) so that devotion and loyalty to the organisations can be developed. It is believed that a higher level of commitment will yield, the better chances for employee

engagement which results in increased teamwork, better performance and reduced turnover (Ibrahim and Al Falasi, 2014).

8.6.6 Application of the Model

The central theoretical contribution of this research is a model that explicates the role of information value in the processes by which computer users decide whether or not to comply with their host organisation's information security policies. Broadly, in Gregor's [2006; 611] terms, this primary contribution is a '*theory for explaining*', in that it seeks to expound the relationship between information value and security compliance behaviour, but it does not provide any predicative capabilities, nor does it deliver testable propositions.

The model explains how different components work with information value assessment and assignment processes, a concept that has never been used before. It is about how a manager for example can work on the 'process of information value assessment and assignment so people (staff) will recognise the value of all type of information so that they can develop a compliance behaviour.

Most notably, it has been demonstrated that an individual's perception of information value may change over time, and it can be affected by the immediate workgroup and wider organisational interpretations of value, as well as by a range of cultural, educational and ethical factors. This reinforces the notion that information security is primarily a social, rather than a technical, problem, which will require people-oriented solutions (D'Arcy et al., 2009). This research has also demonstrates that the outcome of users' security behaviours sends out a very strong message about the extent to which their host organisation values its information. Furthermore, this study is unique in its treatment of common information security factors, such as: education (Pahnila et al., 2007a; Puhakainen and Siponen, 2010) and (Chan et al, 2005; Hu et al, 201); and ethics (Williams, 2008), in that it highlights their influence on information value, as well as attitudes towards security compliance.

These findings offer a number of important implications for practitioners and managers seeking to both encourage colleagues to perceive and treat their information as a valuable resource, and in so doing, improve their organisations' compliance with information security protocols. Organisations can use the model to realise their needs to address and state their

espoused value. Generating information security culture of the organisation so that individual and people in workgroups have the same 'perception of information value'. Taking advantage of the highlighted variables/factors that encourage better information values assessment so that better 'perception of information value' can be achieved.

Specifically, researchers should consider users' perceptions of information value, when conducting future studies of information security compliance. Perhaps the most important, practical implication to emerge from this study is that rather than simply exhorting employees to comply with information security policies, managers should also focus on educating colleagues on the value of information that they're handling, so that they will be far more ready and willing to take the necessary steps to protect it.

At its heart, this model focuses upon human factors and demonstrates that the behaviour of the human agent is central to the effective enforcement of information security policies. Whilst the findings of this study may primarily be of relevance to public sector organisations, in developing economies, because of its strong focus upon human behaviour, it is envisaged that its findings should have some currency or legitimacy in a wide variety of alternative contexts.

8.8 Concluding Remarks

The research aim and objectives (see Section 3.3) were achieved in this thesis through an in-depth qualitative approach. The research followed a carefully planned progression through the intended objectives which built on each other, coming finally to fulfilling them by proving the existence of 'information perceived value' The potential roles of information 'perceptions of information value' as an alternative way to understand users or stakeholders' information security behaviour was also presented. Furthermore, this thesis also provides a model on how information security behaviours are formed in the organisation and more importantly this thesis presents the factors which may help in the formation of these behaviours. In-depth understanding of these factors is imperative as to explain why stakeholders choose to behave in a certain way.

Bruneians live in a conservative society committed to its culture and, as a result, their response information security countermeasures compliance behaviour has been found to be affected by the culture of Brunei Darussalam, which is influenced by the customs, traditions and religion which play a significant role in people's life.

In conclusion, it is found that Bruneian public stakeholders' behaviour toward information is formed based on the complicated process of building value and assigning a value to the information. The intention of the stakeholder is then matched with how they value the information and subsequently their choice of behaviours are modelled from this intention. Influencing factors such as individual priorities, organisational priorities, religion and culture play a significant role in shaping the value perceived by the stakeholders. Since Brunei has a collective society, others' opinion (for example the value derived by significant others or group of people working together) are critical. More often, these collective views are readily accepted and used although an individual stakeholder may have a different perspective on the same issue or matter.

Bibliography

Ackerman, M.S., Cranor, L.F., Park, F. and Reagle, J. (1999), “Privacy in E-Commerce : Examining User Scenarios and Privacy Preferences”, *E-Commerce*, pp. 1–8.

Ackoff, R. (1989), “Ackoff, R. L., "From Data to Wisdom”, *Journal of Applies Systems Analysis*, Vol. 16, pp. 3–9.

Adams, A. and Sasse, A. (1999), “User are not the enemy”, *Communications of the ACM*, Vol. 42 No. 12, pp. 41–46.

AITI. (2010), “Brunei darussalam household ict survey report 2010”.

Albrecht, G. and Hoogstraten, J. (1998), “Satisfaction as a determinant of compliance.”, *Community Dentistry and Oral Epidemiology*, Vol. 26 No. 2, pp. 139–46.

Albrechtsen, E. (2007), “A qualitative study of users’ view on information security”, *Computers & Security*, Vol. 26 No. 4, pp. 276–289.

Albrechtsen, E. and Hovden, J. (2010), “Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study”, *Computers & Security*, Elsevier Ltd, Vol. 29 No. 4, pp. 432–445.

Alfawaz, S., Nelson, K. and Mohannak, K. (2010), “Information security culture: a behaviour compliance conceptual framework”, *8th Australasian Information Security Conference (AISC 2010)*, Vol. 105, pp. 47–55.

Al-Hamdani, W. a. (2009), “Non risk assessment information security assurance model”, *2009 Information Security Curriculum Development Conference on - InfoSecCD ’09*, ACM Press, New York, New York, USA, p. 84.

Alnatheer, M. and Nelson, K. (2009), “Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context”, *Australian Information Security Management Conferences*.

Anderson, J.M. (2003), “Why we need a new definition of information security”, *Computers & Security*, Vol. 22 No. 4, pp. 308–313.

Aytes, K. and Conolly, T. (2003), “A Research Model for Investigating Human Behavior Related to Computer Security”, *AMCIS 2003 Proceedings*.

Ayuso, P.N., Gasca, R.M. and Lefevre, L. (2012), “FT-FW: A cluster-based fault-tolerant architecture for stateful firewalls”, *Computers & Security*, Vol. 31 No. 4, pp. 524–539.

Babin, B.J. and Attaway, J.S. (2000), “Value and Gaining Share of Customer”, *Journal of Business Research*, Vol. 2963 No. 99.

Bansal, G., Zahedi, F. “Mariam” and Gefen, D. (2010), “The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online”, *Decision Support Systems*, Elsevier B.V., Vol. 49 No. 2, pp. 138–150.

Beautement, A., Sasse, M.A. and Wonham, M. (2008), “The Compliance Budget : Managing Security Behaviour in Organisations”, *Security*.

Bélanger, F. and Crossler, R.E. (2011), “Privacy in the digital age: A review of Information Privacy Research in Information Systems”, *MIS Quarterly*, Vol. 35 No. 4, pp. 1017–1041.

Bell, W.F. (1999), “The Impact of Policies on Organizational Values and Culture”, *The Joint Services Conference in Professional Ethics*, available at: <http:www.usafa.af.mil/jscope/JSCOPE99/ Bell99.html>.

Bersz, F.P. (2004), “People often the weakest link in security, but one of the best places to start”, *Journal of Health Care Compliance*, Vol. 6 No. 4, pp. 57–60.

Bowen, G. a. (2005), “Preparing a qualitative research-based dissertation: Lessons learned”, *The Qualitative Report*, Vol. 10 No. 2, pp. 208–222.

Britten, N. (1995), “Qualitative Research: Qualitative interviews in medical research”, available at: http://www.bmj.com/content/311/6999/251.short (accessed 20 December 2014).

Brostoff, S. and Sasse, M.A. (2003), “‘Ten strikes and you’re out’: Increasing the number of login attempts can imporve password usability”, *Workshop on Human-Computer Interaction and Security Systems*, pp. 1–4.

Bryman, A. (2011), “Triangulation”, *Encyclopedia of Social Science Research Methods*, No. 1966, pp. 1–5.

Bryman, A. (2012), *Social Research Methods*, 4th ed., Oxford University Press, Oxford.

Bulgurcu, B., Hasan, C. and Benbasat, I. (2010), “Information security policy compliance: an empirical study of rationaly based beliefs and information security awareness”, *MIS Quarterly Executive*, Vol. 34 No. 3, pp. 523–548.

Bullot, M., Dixon, T., Tomes, G. and Henderson, J. (1997), *Scenario-Based Evaluation of Existing Data Collections*, available at: http://www.aihw.gov.au/WorkArea/DownloadAsset.aspx?id=6442458110.

Cabinet Office. (2008), *Data Handling Procedures in Government: Final Report*, London, available at: https://www.gov.uk/government/publications/data-handling-procedures-in-government.

Castano, S., Fugini, M., Martella, G. and Samarati, P. (1994), *Database Secuirty*.

Chan, M., Woon, I. and Kankanhalli, A. (2005), “Perceptions of Information Security at the Workplace : Linking Information Security Climate to Compliant Behavior Mark Chan National University of Singapore Irene Woon School of Computing , National University of Singapore Atreyi Kankanhalli School of Com”, *Journal of Information Privacy and Security*, Citeseer, Vol. 1 No. 3, pp. 18–41.

Charmaz, K. (2006), *Constructing Grounded Theory*, SAGE Publications, Ltd., California.

Chen, C., Shaw, R.S. and Yang, S. (1992), “Mitigating Information Security Risks by Increasing User Security Awareness : A Case Study of an Information Security Awareness System”, *Information Security*, Vol. 24 No. 1, pp. 1–14.

Cherdantseva, Y. (2011), *Information Security*.

Cherdantseva, Y. and Hilton, J. (2012), “Information Security and Information Assurance .

The Discussion about the Meaning , Scope and Goals ."

Christofides, E., Muise, A. and Desmarais, S. (2009), "Information disclosure and control on Facebook: are they two sides of the same coin or two different processes?", *Cyberpsychology & Behavior : The Impact of the Internet, Multimedia and Virtual Reality on Behavior and Society*, Vol. 12 No. 3, pp. 341–5.

Clark, D.D. and Wilson, D.R. (1987), "A comparison of Commercial and Military Computer Security Policies", *IEEE Symposium on Security and Privacy*.

Council National Research. (2007), *Engaging Privacy and Information Technology in a Digital Age*, The National Academies Press, available at: Http://www.nap.edu.

Cox, A., Connolly, S. and Currall, J. (2001), "Raising information security awareness in the academic setting", *Vine*, Vol. 31 No. 2, pp. 11–16.

Cranor, L.F., Reagle, J. and Ackerman, M.S. (1999), *Beyond Concern: Understanding Net Users' Attitudes About Online Privacy*.

Creswell, J.W. (2003), *Research Design Qualitative Quantative and Mixed Methods Approaches*, Second Edi., SAGE Publications, Ltd., London.

Creswell, J.W. (2009), *Research Design Qualitative, Quantitative, and Mixed Methods Approaches*, 3rd Editio., SAGE Publications, Ltd.

Creswell, J.W. (2012), *Qualitative Inquiry and Research Design: Choosing Among Five Approaches*, SAGE.

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M. and Baskerville, R. (2013), "Future directions for behavioral information security research", *Computers & Security*, Elsevier Ltd, Vol. 32, pp. 90–101.

Crotty, M. (1998), *The Foundation of Social Research*, SAGE Publications, Ltd.

CSI. (2011), *Computer CrIme and SeCurIty Survey*.

D'Arcy, J., Hovav, A. and Galletta, D. (2009), "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach", *Information Systems Research*, INFORMS: Institute for Operations Research, Vol. 20 No. 1, pp. 79–98.

Danaher, P.J. and Mattsson, J. (1994), "Customer Satisfaction during the Service Delivery Process", *European Journal of Marketing*, Vol. 28 No. 5, pp. 5–16.

Davenport, T.H. and Prusak, La. (2000), *Working Knowledge, How Organizations Mange What They Know*, Harvard Business School Press, USA.

Dewa, Z. and Maglaras, L.A. (2013), "Data Mining and Intrusion Detection", *Network*, Vol. 2 No. 04329022, pp. 200–203.

Dhillon, G. and Backhouse, J. (2001), "Current directions in IS security research: towards socio-organizational perspectives", *Information Systems Journal*, Vol. 11 No. 2, pp. 127–153.

Dick, A. and Basu, K. (1994), "Customer Loyalty; toward an integrated conceptual

framework", *Journal of the Academy of Marketing Science*, Vol. 22 No. 2, pp. 99–13.

Doherty, N.F., Anastasakis, L. and Fulford, H. (2009), "The information security policy unpacked: A critical study of the content of university policies", *International Journal of Information Management*, Vol. 29 No. 6, pp. 449–457.

Doherty, N.F., Coombs, C.R. and Loan, C.J. (2012), "Factors affecting the successful ralisation of benefits from systems development projects: findings from three case studies", *Journal of Information Technology*, No. 27, pp. 1–16.

Doherty, N.F. and Fulford, H. (2005), "Do Information Security Policies Reduce the Incidence of Security Breaches", *Information Resources Management Journal*, Vol. 18 No. 4, pp. 21–39.

Doherty, N.F. and Fulford, H. (2006), "Aligning the information security policy with the strategic information systems plan", *Computers & Security*, Vol. 25 No. 1, pp. 55–63.

DTI. (2006), *Department of Trade and Industry Departmental Report 2006*, London, available at: http://www.berr.gov.uk/files/file28518.pdf.

Easley, D. and O'hara, M. (2004), "Information and the Cost of Capital", *The Journal of Finance*, Vol. 59 No. 4, pp. 1553–1583.

EBLF. (2009), *E-Business Interim Comittee Report*, available at: www.eblf.gov.bn.

Edgar H. Schein. (2010), *Organizational Culture and Leadership*, 4th Editio., jossey-Bass.

Eggert, A. and Ulaga, W. (2002), "Customer perceived value: a substitute for satisfaction in business markets?", *Journal of Business & Industrial Marketing*, Vol. 17 No. 2/3, pp. 107–118.

Eid, R. and El-gohary, H. (2015), "The role of Islamic religiosity on the relationship between perceived value and tourist satisfaction", *Tourism Management*, Elsevier Ltd, Vol. 46, pp. 477–488.

Eller, L.S., Lev, E.L. and Feurer, A. (2014), "Key components of an effective mentoring relationship: A qualitative study", *Nurse Education Today*, Elsevier Ltd, Vol. 34 No. 5, pp. 815–820.

ENISA. (2010), "The new users' guide: How to raise information security awareness (EN) — ENISA", available at: http://www.enisa.europa.eu/activities/cert/security-month/deliverables/2010/new-users-guide (accessed 26 February 2013).

Eric Savitz. (2011), "Humans: The Weakest Link In Information Security - Forbes", pp. 11–13.

Fereday, J. and Muir-Cochrane, E. (2006), "Demonstrating Rigor Using Thematic Analysis : A Hybrid Approach of Inductive and Deductive Coding and Theme Development", *International Journal of Qualitative Methods*, pp. 80–92.

Fielden, K. (2010), "Information Security Framework", pp. 38–43.

Fishbein, M. and Ajzen, Ic. (2011), *Predicting and Changing Behaviour: The Reasoned Action Approach*, Tylor & Francis.

Forget, A., Chiasson, S., Oorschot, P.C. Van and Biddle, R. (2008a), "Improving Text

Passwords Through Persuasion Categories and Subject Descriptors", *Perception*.

Forget, A., Chiasson, S., Oorschot, P.C. Van and Biddle, R. (2008b), "Persuasion for Stronger Passwords : Motivation and Pilot Study", pp. 140–150.

Furnell, S. and Rajendran, A. (2012), "Understanding the influences on information security behaviour", *Computer Fraud & Security*, Vol. 2012 No. 3, pp. 12–15.

Furnell, S., Tsaganidi, V. and Phippen, A. (2008), "Security beliefs and barriers for novice Internet users", *Computers & Security*, Elsevier Ltd, Vol. 27 No. 7-8, pp. 235–240.

Furnell, S.M., Gennatou, M. and Dowland, P.S. (2002), "A prototype tool for information security awareness and training", *Logistics Information Management*, MCB UP Ltd, Vol. 15 No. 5/6, pp. 352–357.

Gallarza, M.G., Gil-saura, I., Holbrook, M.B., Valencia, U. De and Naranjos, A.D.L. (2011), "The value of value : Further excursions on the meaning and role of customer value", Vol. 191, pp. 179–191.

Gallarza, M.G. and Saura, I.G. (2006), "Value dimension, percieved value, satisfaction and loyalty: an investigation of university students' travel behaviour", *Tourism Management*, Vol. 27, pp. 437–452.

Garrison, C.P. and Ncube, M. (2011), "A longitudinal analysis of data breaches", *Information Management & Computer Security*, Vol. 19 No. 4, pp. 216–230.

Gary, T. (2009), *How to Do Your Research Project*, Sage, London.

Gerber, M. and Solms, R. Von. (2005), "Management of risk in the information age", *Computers & Security*, Vol. 24 No. 1, pp. 16–30.

Gill, P., Stewart, K., Treasure, E. and Chadwick, B. (2008), "Methods of data collection in qualitative research: interviews and focus groups.", *British Dental Journal*, Vol. 204 No. 6, pp. 291–295.

Glanz, K. and Bishop, D.B. (2010), "The Role of Behavioral Science Theory in Development and Implementation of Public Health Interventions", available at:http://doi.org/10.1146/annurev.publhealth.012809.103604.

Gov.bn. (2016), "Brunei e-governement", available at: www.brunei.gov.bn.

Grace, D. and O'Cass, A. (2005), "An examination of the antecedents of re-patronage intentions across different retail store formats.", *Journal of Retailing and Consumer Services*, Vol. 12, pp. 227–243.

Grossklags, J., Hall, S. and Acquisti, A. (2007), "When 25 Cents is too much : An Experiment on Willingness-To-Sell and Willingness-To- Protect Personal Information".

Groups Miniwatts Marketing. (2012), "Internet World Stats", available at: http://www.internetworldstats.com/stats.htm (accessed 30 August 2012).

GSA. (2010), *U.S General Services Administration*, *GSA Mobility and Telework Policy*.

Guba, E.G. (1990), "The alternative paradigm dialog", *The Paradigm Dialog*, Newbury PArk , CA, pp. 17–30.

Guba, E.G. and Lincoln, Y.S. (1994), “Competing Paradigms in Qualitative Research”, *Handbook of Qualitative Research*, SAGE Publications, Ltd., Thousand Oaks, CA, pp. 105–117.

Guo, K.H. (2013), “Security-related behavior in using information systems in the workplace: A review and synthesis”, *Computers & Security*, Elsevier Ltd, Vol. 32 No. 1, pp. 242–251.

Guo, K.H., Yuan, Y., Archer, N.P. and Connelly, C.E. (2011), “Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model”, *Journal of Management Information Systems*, Vol. 28 No. 2, pp. 203–236.

Hammersley, M. (2007), “The issue of quality in qualitative research”, *International Journal of Research & Method in Education*, Vol. 30 No. 3, pp. 287–305.

Hansche, S. (2001), “Designing a Security Awareness Program: Part 1”, *Information Systems Security*, Vol. 9 No. 6, pp. 1–9.

Hansen, J. V, Lowry, P.B., Meservy, R.D. and McDonald, D.M. (2007), “Genetic programming for prevention of cyberterrorism through dynamic and evolving intrusion detection”, *Decision Support Systems*, Vol. 43 No. 4, pp. 1362–1374.

Harris, L. and Westin, A.F. (1995), *Equifax-Harris Mid-Decade Consumer Privacy Survey*, Atlanta, GA.

Harrison, J.V. (2005), “Enhancing network security by preventing user-initiated malware execution”, *International Conference on Information Technology: Coding and Computing (ITCC’05) - Volume II*, Ieee, pp. 597–602 Vol. 2.

Henninger, M. (2013), “The Value and Challenges of Public Sector Information”, *Cosmopolitan Civil Societies Journal*, Vol. 5 No. 3, pp. 75–95.

Herath, T. (2009), “Protection motivation and deterrence: a framework for security policy compliance in organisations”, *Europe Journal Information System*, Vol. 18 No. 2, pp. 106–125.

Herath, T. and Rao, H.R. (2009), “Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness”, *Decision Support Systems*, Elsevier B.V., Vol. 47 No. 2, pp. 154–165.

Hesket, L.J., Sasser, W.E. and Schlesinger, L.A. (1997), *The Service Profit Chain: How Leading Companies :ink Profit to Loyalty, Satisfaction, and Value,* Free Press.

Hofstede, G., Hofstede, G.J. and Minkov, M. (2010), *Cultures and Organizations*, Third., McGraqHill.

Holbrook, M. (1994), “The Nature of Customer Value: An Axiology of Services in the Consumption Experience.”, in Rust, R. and Oliver, R. (Eds.), *Service Quality: New Directions in Theory and Practice.*, Thousand Oaks, CA, pp. 21–72.

Holbrook, M.B. (1996), “Customer Value — A Framework For Analysis and Research”, *Advances in Consumer Research*, Vol. 23 No. 1, pp. 138–142.

Home Civil Service. (2012), “Making government work better, HMG Security Policy Framework”, No. April, pp. 1–51.

Höne, K. and Eloff, J.H.. (2002), “What Makes an Effective Information Security Policy?”, *Network Security*, Vol. 2002 No. 6, pp. 14–16.

Hu, Q., Hart, P. and Cooke, D. (2007), “The role of external and internal influences on information systems security - a neo-institutional perspective”, *Journal of Strategic Information Systems*, Vol. 16 No. 2, pp. 153–172.

Huang, Y.T. and Cheng, F.F. (2013), “The effect of online sales promotion strategies on consumers’ perceived quality and purchase intention: A moderating effect of brand awareness”, *Proceedings - 2013 5th International Conference on Service Science and Innovation, ICSSI 2013*, pp. 91–95.

Hwang, C. and Yoon, K. (1981), *Multiple Attribute Decision Making, Methods and Applications*, Springer-Verlag.

IBM Security Services, I.B.M.S. (2015), *IBM X-Force Threat Intelligence Quarterly ,*.

Ibrahim, M. and Al Falasi, S. (2014), “Employee loyalty and engagement in UAE public sector”, *Employee Relations*, Vol. 36 No. 5, pp. 562 – 582.

ICO. (2010), *The Guide to Data Protection*, available at: http://ico.org.uk/for_organisations/data_protection/the_guide.

Ifinedo, P. (2012), “Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory”, *Computers & Security*, Elsevier Ltd, Vol. 31 No. 1, pp. 83–95.

International, I. (2015), “Organizational Culture and National Culture : What ’ s the Difference and Why does it Matter ?”, available at: http://www.itapintl.com/index.php/about-us/latest-news/57-organizational-culture-and-national-culture-what-s-the-difference-and-why-does-it-matter (accessed 1 January 2015).

isaca. (2009), “An Introduction to the Business Model for Information Security”, available at: http://www.isaca.org/Knowledge-Center/Research/Documents/Intro-Bus-Model-InfoSec-22Jan09-Research.pdf.

Itami, H. and Roehl, T.W. (1991), *Mobilizing Invisible Assets*, HArvard University Press.

Ives, B., Olson, M.H. and Baroudi, J.J. (1983), “The measurement of user information satisfaction”, *Communications of the ACM*, Vol. 26 No. 10, pp. 785–793.

Jagatic, T.N., Johnson, N.A., Jakobsson, M. and Menczer, F. (2007), “Social Phishing”, *Communication of the ACM*, Vol. 10 No. 50, pp. 94–100.

Jansen, H. (2010), *The Logic of Qualitative Survey Research and Its Position in the Field of Social Research Methods*, *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research*, Vol. 11.

Jenkins, J.L., Durcikova, A. and Burns, M.B. (2012), “Forget the Fluff: Examining How Media Richness Influences the Impact of Information Security Training on Secure Behavior”, *2012 45th Hawaii International Conference on System Sciences*, Ieee, pp. 3288–3296.

Juned, A. (2013), “Inaugural lecture by State Mufti”, pp. 1–7.

Kankanhalli, A., Teo, H.-H., Tan, B.C.Y. and Wei, K.-K. (2003), "An integrative study of information systems security effectiveness", *International Journal of Information Management*, Vol. 23 No. 2, pp. 139–154.

Kayworth, T. and Whitten, D. (2010), "Effective information security requires a balance of social and technological factors", *MIS Quarterly Executive*, Vol. 9 No. 3, pp. 303–315.

Khalifa, A.S. (2004), "Customer value: a review of recent literature and an integrative configuration", *Management Decision*, Vol. 42 No. 5, pp. 645–666.

Khan, R.L. and Cannell, C.F. (1957), *The Dynamics of Interviewing*, John Wiley & Sons Inc, USA.

Khun, T.S. (1996), *The Structure of Scientific Revolutions*, third., The University of Chicago Press.

Kim, Y., Park, G., Kim, T. and Lee, S. (2007), "Security Evaluation for Information Assurance", *2007 International Conference on Computational Science and Its Applications (ICCSA 2007)*, Ieee, pp. 227–230.

Kraemer, S., Carayon, P. and Clem, J. (2009), "Human and organizational factors in computer and information security: Pathways to vulnerabilities", *Computers & Security*, Elsevier Ltd, Vol. 28 No. 7, pp. 509–520.

Kral, D. (2001), "Information Security in small and medium-sized companies", *ACTA VSFS*, Vol. 5 No. 1, pp. 61–74.

Lazarus, R.S. and Folkman, S. (1984), *Stress, Appraisal and Coping*, Springer Publishing Company.

Leach, J. (2003), "Improving user security behaviour", *Computers & Security*, Vol. 22 No. 8, pp. 685–692.

Lebek, B., Uffen, J., Breitner, M.H., Neumann, M. and Hohler, B. (2013), "Employees' Information Security Awareness and Behavior: A Literature Review", *2013 46th Hawaii International Conference on System Sciences*, Ieee, pp. 2978–2987.

Lee, E. and Overby, J.W. (2004), "Creating value for onlinf, shoppers: iimiplicat'ions for satisfaction", *Journal of Consuner Satisfaction, Dissatisfaction and Complaining Behaviour*.

Leidner, D.E. (2010), "Globalization, culture, and information: Towards global knowledge transparency", *The Journal of Strategic Information Systems*, Vol. 19 No. 2, pp. 69–77.

Li, X. and Chen, X. (2010), "Factors Affecting Privacy Disclosure on Social Network Sites: An Integrated Model", *2010 International Conference on Multimedia Information Networking and Security*, Ieee, pp. 315–319.

Liang, H. and Xue, Y. (2009), "Avoidance of Information Technology Threats: A theoretical perspective", *MIS Quarterly*, Vol. 33 No. 1, pp. 71–90.

Liginlal, D., Sim, I. and Khansa, L. (2009), "How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management", *Computers & Security*, Vol. 28 No. 3-4, pp. 215–228.

Lincoln, Y. and Guba, E.G. (1995), *Naturalistic Inquiry*, SAGE Publications, Ltd., Newbury PArk , CA.

Liu, H. and Yang, L. (2014), "Influence of Marketing Strategy on NPD Performance : Role of Customer Perceived Value and Product Characteristics", *Open Journal of Social Science*, Vol. 2 No. March, pp. 34–38.

Malheiros, M., Brostoff, S., Jennett, C. and Sasse, M.A. (2011), "Would You Sell Your Mother ' s Data ? Personal Data Disclosure in a Simulated Credit Card Application".

Mathiesen, K. (2004), "What is information ethics?", *Computers and Society*, Vol. 32 No. 8, pp. 1–11.

Mcconnell, M. and Hamilton, B.A. (2002), "Information Assurance in the Twenty-First Century", *Security and Privacy*.

McIlwraith, A. (2006), *Information Security and Employee Behaviour*, 1st ed., Gower, London.

Mell, P. and Grance, T. (2011), *The NIST Definition of Cloud Computing (Draft) Recommendations of the National Institute of Standards and Technology*, Vol. 145.

Mertens, D.M. (1998), *Research Methods in Education and Psychology: Integrating Diversity with Quantative & Qulaitative Approaches*, Thousand Oaks, USA Carlifonia.

Milberg, S.J., Burke, S.J., Jeff, H. and Kallman, E.A. (1995), "values, personal information privacy and regulatory approaches", *Communication of the ACM*, Vol. 38 No. 12, pp. 65–74.

Miles, M.B. and Huberman, A.M. (1994), "Qualitative Data Analysis: An Expanded Source book", SAGE Publications, Ltd.

Milfelner, B., Snoj, B. and Pisnik Korda, A. (2011), "Measurement of Perceived Quality, Perceived Value, Image, and Satisfaction Interrelations of Hotel Services: Comparison of Tourists From Slovenia and Italy", *Drustvena Istrazivanja*, Vol. 20 No. 3 (113), pp. 602–624.

Mohamed, N. and Ahmad, I.H. (2012), "Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia", *Computers in Human Behavior*, Elsevier Ltd, Vol. 28 No. 6, pp. 2366–2375.

Morris B. Holbrook. (1996), "CUSTOMER VALUE C A FRAMEWORK FOR ANALYSIS AND RESEARCH", in P.Corfman, K. and Jr., J.G.L. (Eds.), *Advances in Consumer Research*, Vol. 23, pp. 138–142.

Mothersbaugh, D.L., Foxx, W.K., Beatty, S.E. and Wang, S. (2011), "Disclosure Antecedents in an Online Service Context: The Role of Sensitivity of Information", *Journal of Service Research*, Vol. 15 No. 1, pp. 76–98.

Mowshowitz, A. (1992), "On the market value of information commodities. I. The nature of information and information commodities", *Journal of the American Society for Information Science*, Vol. 43 No. 3, pp. 225–232.

Muniandy, L. and Muniandy, B. (2012), "State of Cyber Security and the Factors Governing its Protection in Malaysia", *International Journal of Applied Science and Technology*, Vol.

2 No. 4, pp. 106–112.

Nehf, J.P. (2012), *OPEN BOOK the Failed Promise of Informaiton Privacy in America*, available at: http://ssrn.com/abstract=2192471 ii.

Ng, B.-Y., Kankanhalli, A. and Xu, Y. (Calvin). (2009), "Studying users' computer security behavior: A health belief perspective", *Decision Support Systems*, Vol. 46 No. 4, pp. 815–825.

Van Niekerk, J.F. and Von Solms, R. (2010), "Information security culture: A management perspective", *Computers & Security*, Elsevier Ltd, Vol. 29 No. 4, pp. 476–486.

Notoatmodjo, G. (2007), "Exploring the 'Weakest Link': A Study of Personal Password Security", No. December, available at: http://130.203.133.150/viewdoc/summary?doi=10.1.1.122.1794 (accessed 28 November 2012).

Oh, H. (2003), "Price fairness and its asymmetric effects on overall price, quality, and value judgements: the case of an upscale hotel.", *Tourism Management*, Vol. 24, pp. 397–399.

Orna, E. (2004), *Information Strategy in Practice*, Gower Publishing Limited.

Orna, E. (2005), *Making Knowledge Visible*, Gower Publishing Limited, London.

"Oxford Dictionary". (2015), .

Pahnila, S., Siponen, M. and Mahmood, A. (2007a), "Employees ' Behavior towar ds IS Secur ity Policy Compliance", *40th Hawaii International Conference on System Sciences*.

Pahnila, S., Siponen, M. and Mahmood, A. (2007b), "Which Factors Explain Employees ' Adherence to Information Security Policies ? An Empirical Study", *Pacific Asia Conference on Information System*.

Parsons, K., Mccormac, A., Butavicius, M. and Ferguson, L. (2010), "Human Factors and Information Security : Individual , Culture and Security Environment".

Pascarella, P. (1997), "Harnessing Knowledge", *Management Review*, pp. 37–40.

Petrick, J. (2003), "Measuring cruise passengers' perceived value", *Tourism Analysis*, Vol. 7, pp. 251–258.

Pfost, J., Soriano, R. and FOx, S.F. (2012), "The current landscape of information security", available at: https://www.brighttalk.com/webcast/7521/42171?utm_campaign=webcasts-search-results-feed&utm_content=Security+Architecture+and+Engineering+advisor+of+the+U.S&utm_source=brighttalk-portal&utm_medium=web&utm_term= (accessed 18 February 2013).

Pinillos, M.-J. and Reyes, L. (2009), "Relationship between individualist–collectivist culture and entrepreneurial activity: evidence from Global Entrepreneurship Monitor data", *Small Business Economics*, Vol. 37 No. 1, pp. 23–37.

Post, G. and Kagan, A. (2007), "Evaluating information security tradeoffs, restricting access can interfere with user tasks", *Computers & Security*, Vol. 26 No. 3.

Power, E.M. (2007), *Developing a Culture of Privacy: A Case Study*, *IEEE Security Privacy Magazine*, Vol. 5, IEEE Computer Society, pp. 58–60.

Power, R. and Forte, D. (2006), "Case Study: a bold new approach to awareness and education, and how it met an ignoble fate", *Computer Fraud & Security*, Vol. 2006 No. 5, pp. 7–10.

Prins, C. (2006), "When personal data, behavior and virtual identities become a commodity: Would a property rights approach matter?", *SCRIPT-Ed*, Vol. 3 No. 4, pp. 270–303.

Puhakainen, P. and Siponen, M. (2010), "Imporving employees compliance through information system security training: an action research study", *MIS Quarterly*, Vol. 34 No. 4, pp. 757–778.

Pura, M. (2005), "Linking perceived value and loyalty in location based mobile services", *Managing Service Quality*, Vol. 15 No. 6, pp. 509–538.

PWC. (2012), *UK Information Security Breaches Survey - Technical Report*, available at: http://www.pwc.co.uk/en_UK/uk/assets/pdf/olpapp/uk-information-security-breaches-survey-technical-report.pdf.

Rad, B.B., Masrom, M. and Ibrahim, S. (2011), "Evolution of Computer Virus Concealment and Anti-Virus Techniques : A Short Survey", *IJCSI International Journal of Computer Science*, Vol. 8 No. 1, pp. 113–121.

Rainer, R.K., Marshall, T.E., Knapp, K.J. and Montgomery, G.H. (2007), "Do Information Security Professionals and Business Managers View Information Security Issues Differently?", *Information Systems Security*, Vol. 16 No. 2, pp. 100–108.

Raiu, C. (2012), "Cyber-threat evolution: the past year", *Computer Fraud & Security*, Elsevier Ltd, Vol. 2012 No. 3, pp. 5–8.

Rajh, S.P. (2012), "Comparison of perceived value structural models", *Market, Scientific Journal of Crotia*, Vol. 24 No. 1, pp. 117–133.

Ratner, C. (2012), "Ratner Forum Qualitative Sozialforschung / Forum : Qualitative Social Subjectivity and Objectivity in Qualitative Methodology Ratner", Vol. 3 No. 3, pp. 1–6.

Rees, J., Opadhyay, S.B. and Spafford, E.H. (2003), "PFIRES: a policy framework for information security", *Communications of the ACM*, Vol. 46 No. 7, pp. 101–106.

Rhee, H.-S., Kim, C. and Ryu, Y.U. (2009), "Self-efficacy in information security: Its influence on end users' information security practice behavior", *Computers & Security*, Elsevier Ltd, Vol. 28 No. 8, pp. 816–826.

Richardson, R. (2008), "CSI Computer Crime & Security Survey", *Computer Security Institute*, No. 1, pp. 1–30.

Rifon, N.J. and Choi, S.M. (2005), "Your Privacy Is Sealed : Effects of Web Privacy Seals on Trust and Personal Disclosures", Vol. 39 No. 2, pp. 339–362.

Robinson, D. (2013), "Cybercrime wave gathers force", *Financial Times*.

Rossouw von solms. (1998), "Information Management & Computer Security Information security management (1): why information security is so important", *Information*

Management & Computer Security, Vol. 6 No. 4, pp. 174–177.

Russell, C. (2002), *Security Awareness - Implementing an Effective Strategy*, available at: http://www.sans.org/reading_room/whitepapers/awareness/security-awareness-implementing-effective-strategy_418.

Salleh, N.M. and Clarke, N. (2009), "emotions and their management during a merger in Brunei: The Impact of National Culture", pp. 1–45.

Sánchez, F.R., Iniesta-Bonillo, M.Á. and Holbrook, M.B. (2008), "The conceptualisation and measurement of consumer value in services", *International Journal of Market Research*, Vol. 51 No. 1, p. 93.

Sanchez-fernandez, R. and Iniesta-Bonillo, M. a. (2007), "The concept of perceived value: a systematic review of the research", *Marketing Theory*, Vol. 7 No. 4, pp. 427–451.

Santander. (2016), *You Make Us Who We Are Employee Handbook*.

Sasse, M.A., Brostoff, S. and Weirich, D. (2001), "Transforming the 'weakest link' — a human/computer interaction approach to usable and effective security", *BT Technology Journal*, Vol. 19 No. 3, p. 122.

Saul McLeod. (2016), "What is conformity?", available at: http://www.simplypsychology.org/conformity.html (accessed 12 January 2016).

Saunders, B.M. and Tosey, P. (2013), "The Layers of research design", *Rapport*, Vol. 14 No. 4, pp. 58–59.

Saunders, M., Lewis, P. and Thornhill, A. (2003), *Research Methods for Business Students*, Third., Prentice Hall, Essex, available at: www.booksites.net.

Seyal, A.H. and Rahim, M. (2011), "Customer Satisfaction with Internet Banking in Brunei Darussalam ":, *E-Service Journal*, Vol. 7 No. 3, pp. 47–69.

Sheth, J.N., Newman, B.I. and Gross, B.L. (1991), "Why We Buy What We Buy : A Theory of Consumption Values", *Journal of Business Research*, Vol. 170, pp. 159–170.

Shropshire, J., Johnston, A., Schmidt, M. and Johnston, A.C. (2006), "Personality and IT security : An application of the five-factor model Personality and IT security : An application of the five-factor model", *AMCIS 2006 Proceedings*.

Siponen, M., Pahnila, S. and Mahmood, A. (2007), "New Approaches for Security, Privacy and Trust in Complex Environments", *IFIP International Federation for Information Processing*, Vol. 232, pp. 133–144.

Siponen, M., Pahnila, S. and Mahmood, M.A. (2010), "Compliance with Information Security Policies ":, *IEE Computer Society*, Vol. 43 No. 2, pp. 64–71.

Siponen, M. and Vance, A. (2010), "Neutralization: New insights into the problem of employee information systems security policy violations", *MIS Quarterly*, MIS Quarterly & The Society for Information Management, Vol. 34 No. 3, pp. 487–502.

Smith, E. a. (2001), "The role of tacit and explicit knowledge in the workplace", *Journal of Knowledge Management*, Vol. 5 No. 4, pp. 311–321.

Smith, N. a, Ley, P., Seale, J.P. and Shaw, J. (1987), “Health beliefs, satisfaction and compliance.”, *Patient Education and Counseling*, Vol. 10 No. 3, pp. 279–86.

Soomro, Z.A., Shah, M.H. and Ahmed, J. (2016), “Information security management needs more holistic approach: A literature review”, *International Journal of Information Management*, Elsevier Ltd, Vol. 36 No. 2, pp. 215–225.

Stahl, B.C., Doherty, N.F. and Shaw, M. (2012), “Information security policies in the UK healthcare sector: a critical evaluation”, *Information Systems Journal*, Vol. 22 No. 1, pp. 77–94.

Stanton, J.M., Stam, K.R., Mastrangelo, P. and Jolton, J. (2005), “Analysis of end user security behaviors”, *Computers & Security*, Vol. 24 No. 2, pp. 124–133.

Stanton, J.M., Stam, K.R., Mastrangelo, P.R. and Jolton, J. (2004), “Behavioral Information Security : Two End User Survey Studies of Motivation and Security Practices”, *Proceeding of the Tenth Americas Conference of Information System, New York*, No. August, pp. 2–8.

Stone, E.F., Gardner, D.G., Guetal, H.G. and McClure, S.A. (1983), “A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organisations”, *Appllied Psychology*, Vol. 63 No. 3, pp. 459–468.

Strand, D. (2013), “Applying the 20-60-20 rule to leadership & change Management”.

Straub, D.W. (1990), “Effective IS Security: An Empirical Study”, *Information Systems Research*, Vol. 1 No. 3, pp. 255–276.

Sutcliffe, a. G., Maiden, N. a. M., Minocha, S. and Manuel, D. (1998), “Supporting scenario-based requirements engineering”, *IEEE Transactions on Software Engineering*, Vol. 24 No. 12, pp. 1072–1088.

Sweeney, J., Soutar, G., Whiteley, A. and Johnson, L. (1996), “Generating Consumption Value Items : a Parallel Interviewing Process Approach”, *Asia Pacific Advances in Consumer Research Volume 2*.

Sweeney, J.C. and Soutar, G.N. (2001), “Consumer perceived value : The development of a multiple item scale”, *Journal of Retailing*, Vol. 77, pp. 203–220.

Swire, P.P. and Steinfeld, L.B. (2002), “Security and privacy after September 11: the health care example.”, *Minnesota Law Review*, Vol. 86 No. 6, pp. 1515–40.

Tahir, M., Mahmood, K. and Shafique, F. (2008), “Information Needs and Information-Seeking Behavior of Arts and Humanities Teachers : A Survey of the University of the Punjab , International College of Engineering & Management Muscat , Oman Khalid Mahmood Professor and Chairman Department of Library and”, *Library Philosophy and Pratice*, Vol. 2008 No. 1997, pp. 1–11.

Tajuddin, S. (2010), *Informaiton Security Awareness Feasibility Study in Brunei Darussalam*.

Thaler, R. (1985), “Mental Accounting and Consumer Choice”, *Marketing Science*, Vol. 4 No. 3, pp. 199–214.

Thaler, R.H. and Sunstein, C.R. (2008), *Nudge: Improving Decisions Anbout Health, Wealth,*

and Happiness, Yale University Press, New HAven.

Thiyagarajan, P., V, P.V. and Aghila, G. (2010), "Anti-Phishing Technique using Automated Challenge Response Method", *Proceedings of the International Conference on Communication and Computational Intelligence*, pp. 585–590.

Thomas, D.R. (2006), "A General Inductive Approach for Analyzing Qualitative Evaluation Data", *American Journal of Evaluation*, Vol. 27 No. 2, pp. 237–246.

Tsai, J.Y., Egelman, S., Cranor, L. and Acquisti, a. (2010), "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study", *Information Systems Research*, Vol. 22 No. 2, pp. 254–268.

Vance, A., Siponen, M. and Pahnila, S. (2012), "Motivating IS security compliance: Insights from Habit and Protection Motivation Theory", *Information & Management*, Elsevier B.V., Vol. 49 No. 3-4, pp. 190–198.

Da Veiga, A. and Eloff, J.H.P. (2010), "A framework and assessment instrument for information security culture", *Computers & Security*, Elsevier Ltd, Vol. 29 No. 2, pp. 196–207.

Venter, H.. and Eloff, J.H.. (2003), "A taxonomy for information security technologies", *Computers & Security*, Vol. 22 No. 4, pp. 299–307.

Verizon. (2012), *2012 Data Breach Investigations Report*, available at: http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf.

Wang, J. (2015), "R ESEARCH A RTICLE I NSIDER T HREATS IN A F INANCIAL I NSTITUTION : A NALYSIS OF A TTACK -P RONENESS OF I NFORMATION S YSTEMS A PPLICATIONS 1", Vol. 39 No. 1, pp. 91–112.

Weirich, D. (2005), *Persuasive Password Security*, *Discourse*, available at: http://hornbeam.cs.ucl.ac.uk/hcs/publications/Weirich_Thesis_final.pdf.

Weirich, D. and Sasse, M.A. (2001), "Pretty good persuasion: a first step towards effective password security in the real world", *New Security Paradigms Workshop*, ACM Press, New York, New York, USA, No. October, p. 137.

Wenger, E. (2009), "Communities of practice a brief introduction", pp. 1–5.

Werelds, S.L. and Sandra streukens. (2011), *Customer Value Measurement*.

Westhoek, H.J., van den Berg, M. and Bakkes, J. a. (2006), "Scenario development to explore the future of Europe's rural areas", *Agriculture, Ecosystems & Environment*, Vol. 114 No. 1, pp. 7–20.

Westin, A.F. (2003), "Social and Political Dimensions of Privacy", *Journal of Social Issues*, Vol. 59 No. 2, pp. 431–453.

Wiant, T.L. (2005), "Information security policy's impact on reporting security incidents", *Computers & Security*, Vol. 24 No. 6, pp. 448–459.

Widman, J. (2011), "10 Massive Security Breaches", *Information Week Security*, available at: http://www.informationweek.co.uk/security/attacks/10-massive-security-

breaches/229300675?pgno=8.

Williams, P. and Soutar, G.N. (2000), “Dimensions of Customer Value and the Tourism Experience : An Exploratory Study Faculty of Business and Public Management”, *ANZMAC 2000 Visionary Marketing for the 21 Century: Facing the Challenge*, pp. 1415–1421.

Wilson, K.S., John, W. and Freeway, C. (2012), “Conflicts Among the Pillars of Information Assurance”.

Woodruff, R.B. and Gardial, S. (1996), *Know Your Customer: New Approaches to Customer Value and Satisfaction*.

Yapa, P.W.S. (2014), “Critical Perspectives on Accounting In whose interest ? An examination of public sector governance in Brunei Darussalam”, Vol. 25, pp. 803–818.

Yeo, A.C., Rahim, M. and Ren, Y.Y. (2009), “Use of Persuasive Technology to Change End-Users ’ IT Security Aware Behaviour : A Pilot Study”, *International Journal of Human and Social Science*, Vol. 4 No. 9, pp. 673–679.

Zeithaml, V.A. (1988), “Consumer Perceptions Of Price , Quality , And Value : A Means-”, *Journal of Marketing*, No. 52, p. 2.

Zulhuda, S. (2010), “Information security in the Islamic perspective: The principles and practices”, *Proceeding of the 3rd International Conference on Information and Communication Technology for the Moslem World (ICT4M) 2010*, p. H–33–H–39.

Appendix A. Scenario Based Questions

Clear Desk Policy

You are driving home after a long day in the office and suddenly remembered that you left your workstation in the office unlock and it is still switched on and an important report is still lying on your desk. What will you do?

Typical answers

- Call into office and ask a colleague to lock your workstation and store away the important document
- Immediately goes back to the office to lock or switched on and store the document away.
- It does not matter, as it is a common practice to leave workstation unlock and leaving documents lying around is not an offence
- Since only authorised personnel are allowed into the office it is safe to leave it as it is.
- I believe that my colleague will not snoop around

Questions

- If the answer is nothing, why?
- It is highlighted that there is an "important report" visible to prying eyes, discuss the term 'important' to the participant as well as the organisation.
- If the document is a personal document, how differently will the participant react?
- If any different reaction, why?

Password Disclosure

While you are away for a holiday, you received an e-mail or short message service (SMS) on your phone from a colleague at work requesting for your password and username. He needs to access your system to extract some information for a report he or she is compiling. What will you do?

Typical answer for scenario two will be;

- Send him the password and the username in an encrypted e-mail
- Send him the password and the username in an e-mail
- Send him the password and the username in separate e-mails
- Send him the password and the username in separate encrypted e-mails
- Tell him the password on the phone
- Sent him an SMS containing the password and the username
- Send him the password and the username in two separate SMS
- Give him instruction to where, you hide the piece of paper containing your password

and your username
- Never share the password

Questions

- If answer falls into category A-H, ask the participant because his willingness to share the credentials?
- Ask what might he store in the computer or system?
- How important are the documents stored in his or her system to the organisation?
- How important are the documents stored in his or her system personally?
- If the document is a personal document, how differently will the participant react?
- If any different reaction, why?

Usage of Portable Storage Device

You need to take some 'classified' information with you to a meeting held outside your organisation. What will you do?

Common or expected answers for Scenario 3;

- Copy the information onto your personal portable storage drive
- Copy the information onto your personal portable storage drive after scanning the device for any viruses.
- Encrypt the information and then copy the information onto your personal portable storage drive after scanning the device for any viruses.
- Copy the information onto a verified portable storage drive issued by your organisation
- Copy the information onto a verified portable storage drive issued by your organisation after scanning the device for any viruses
- Encrypt the information before copying onto a verified portable storage drive issued by your organisation after scanning the device for any viruses

Questions

- If answer falls into category A-C, ask the participant to justify his action of using his device?
- How important are the documents stored in his or her device to the organisation?
- How important are the documents stored in his or her device personally?
- If the document is a personal document, how differently will the participant react?
- If any different reaction, why?

Software Infringement

You need a specific application for an important project you are working on, you have a copy of the software that has not been verified for its copyright and have not passed through your organisation's quality assurance process. What will you do?

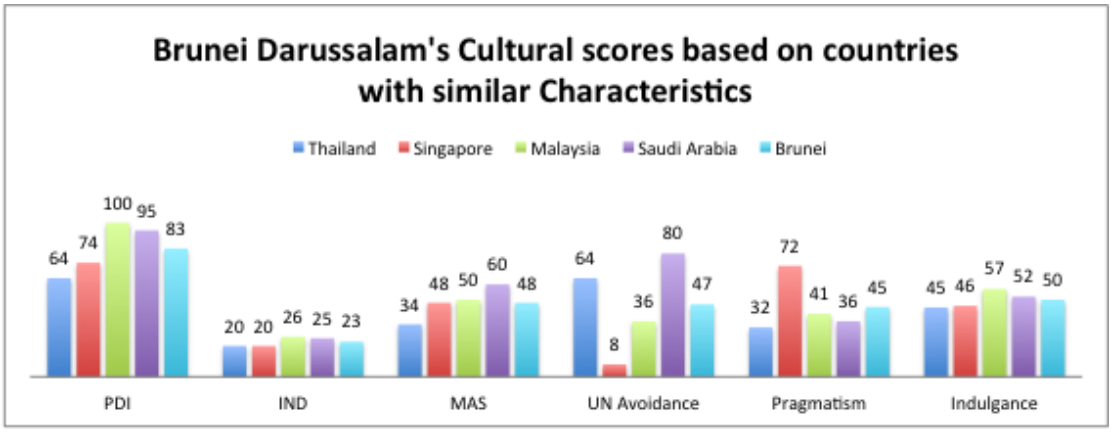
Common or expected answers for Scenario 4 will be,

- This is a situation that requires an exception; it is ok to install the application.
- Install the software on a personally owned system and run the application from there.
- Look for a similar freeware on the internet to finish the work
- This is too much of a hassle; security is a hindrance to my work
- Wait until the software is verified and passed by QA

Questions?

- Ask Participants to justify their answer?
- What do you think are the risk that may arise if you install the unverified software?
- If the answer falls within category B, ask participants to justify why it is ok to install it on a personal machine then instaling in on a machine belonging to the organisation?

Appendix B. Brunei National cultural dimensions according to hofstede's 6D model



	Thailand	Singapore	Malaysia	Saudi Arabia	Brunei Darussalam
PDI	64	74	100	95	83
IND	20	20	26	25	23
MAS	34	48	50	60	48
UN Avoidance	64	8	36	80	47
Pragmatism	32	72	41	36	45
Indulgence	45	46	57	52	50

PDI (83%)

The extent to which the less powerful members of institutions and organisations within a country accept that power is distributed unequally.

Hierarchical order is well accepted – everybody has a place, which needs no further justification. Subordinates expect to be told what to do. Ideal boss is a benevolent autocrat

Individualism (23%)

The degree of interdependence a society maintains among its members

Harmony is found when everybody saves face in the sense of dignity, self-respect, and prestige. Social relations should be conducted in such a way that everybody's face is saved.

The society fosters strong relationships where everyone takes responsibility for fellow members of their group.

Societies offence leads to shame and loss of face, employer/employee relationships are perceived in moral terms (like a family link), hiring and promotion decisions take account of the employee's in-group, management is the management of groups.

Masculinity (48%)

The fundamental issue here is what motivates people, wanting to be the best (masculine) or liking what you do (feminine).

Being modest and humble is seen as very important; thus showing that one knows it all and therefore has come to educate the counterparts is not liked.

During discussions being cautious is important, not to being too persistent.

Assertiveness and competitiveness is less

Uncertainty Avoidance (47%)

The extent to which the members of a culture feel threatened by ambiguous or unknown situations and have created beliefs and institutions that tries to avoid these.

Countries exhibiting high uncertainty avoidance maintain rigid codes of belief and behaviour and are intolerant of unorthodox behaviour and ideas.

There is an emotional need for rules (even if the rules never seem to work) time is money, people have an inner urge to be busy and work hard, precision.

Punctuality are the norm, innovation may be resisted, security is an important element in individual motivation.

Low UAI societies maintain a more relaxed attitude in which practice counts more than principles and deviance from the norm is more easily tolerated. In societies exhibiting low UAI, people believe there should be no more rules than are necessary and if they are ambiguous or do not work, they should be abolished or changed. Schedules are flexible, hard work is undertaken when necessary but not for its own sake. Precision and punctuality do not come naturally, innovation is not seen as threatening.

Countries exhibiting high uncertainty avoidance maintain rigid codes of belief and behaviour and are intolerant of unorthodox behaviour and ideas. In these cultures there is an emotional need for rules (even if the rules never seem to work) time is money, people have an inner urge to be busy and work hard, precision and punctuality are the norm, innovation may be resisted, security is an important element in individual motivation.

Pragmatism (45%) - normative

How people in the past as well as today relate to the fact that so much that happens around us cannot be explained.

Culture is more normative than pragmatic. People in such societies have a strong concern with establishing the absolute Truth; they are normative in their thinking. They exhibit great respect for traditions, a relatively small propensity to save for the future, and a focus on achieving quick results.

Indulgence (50%) – a bit restrained

The extent to which people try to control their desires and impulses, based on the way they were raised.

Societies that score low on this dimension suggests a more restrained societies that do not put much emphasis on leisure time and control the gratification of their desires. People with this orientation have the perception that their actions are restrained by social norms and feel the indulging themselves is somewhat wrong. While a higher score would suggest that generally exhibit a willingness to realise their impulses and desires with regard to enjoying life and having fun. They possess a positive attitude and have a tendency towards optimism. In addition, they place a higher degree of importance on leisure time, act as they please and spend money as they wish.

Appendix C. Participant Information Sheet

INFORMATION SECURITY BEHAVIOUR IN ORGANISATION

(BRUNEI DARUSSALAM)

Participant Information Sheet

Name (Main Investigator): Sharul Tajuddin (s.t.haji-tajuddin@lboro.ac.uk)

Supervisors: Dr. Wendy Olphert (C.W.Olphert@lboro.ac.uk) and Professor Neil Doherty (N.F.Doherty@lboro.ac.uk)

What is the purpose of the study?

The main aim of this research is to contribute to the improvement of information security through its human aspect, in the specific context of Brunei Darussalam. It is argued that by recognising and facilitating the necessary conditions that promote user involvement, particularly compliance, improvements are likely to succeed.

Therefore, the main purpose of this study is to understand stakeholders (users, owners and information security personal) appreciation and expression of issues regarding information security behaviour. This study will also explore the elements considered importance by user in their process of deciding how to react to an information security incident.

Who is doing this research and why?

The research is being done by the main investigator as named in the above section and will be supervised by two supervisors also named above from Loughborough University. This study is part of a Student research project supported by Loughborough University in part for completion of a PhD in Information Security under the Centre for Information Management, School of Business and Economic.

Once I take part, can I change my mind?

Yes! After you have read this information and asked any questions you may have we will ask you to complete an Informed Consent Form, however if at any time, before, during or after the sessions you wish to withdraw from the study please just contact the main investigator. You can withdraw at any time, for any reason and you will not be asked to explain your reasons for withdrawing.

Will I be required to attend any sessions and where will these be?

Yes! You will be required to attend a session of one to one interview with the main investigator. This is either done face-to-face or using online tools such as Skype. The interview session will be audio recorded for transcription purpose. You will be inform on the venue for the interview at a later stage.

How long will it take? *Each Interview session will take up to 1 hour.*

Is there anything I need to do before the sessions?

A short document on various information security critical 'case' incidents will be e-mailed to you. You are expected to read these document before the interview.

Is there anything I need to bring with me? *No*

What personal information will be required from me?

You will only be asked some common demographic information such as age, length of services, level of education etc.

Are they any risks in participating? *No*

Will my taking part in this study be kept confidential?

The data we collect do not contain any personal information about you except for the nature of your work and the duration you have been in your current position. It is practically impossible to identify individuals from the data collected. The information collected will only be accessible to the investigator and supervisors of this research.

What will happen to the results of the study?

The data collected in this study may be used in presentation at conferences and may be published in journals for the academic audience. Individual participants will not be identifiable in what way so ever.

What do I get for participating?

Your participation in this study will contribute to a significant research on how to improve information security compliance in government organisation in Brunei Darussalam. This indirectly will contribute to the betterment and stability of our government organisations.

I have some more questions who should I contact?

Please do not hesitate to contact the main investigator or any of the supervisors listed above if you have any other questions on this study.

What if I am not happy with how the research was conducted?

If you are not happy with how the research was conducted, please contact the Mrs Zoe Stockdale, the Secretary for the University's Ethics Approvals (Human Participants) Sub-Committee:

Mrs Z Stockdale, Research Office, Rutland Building, Loughborough University, Epinal Way, Loughborough, LE11 3TU. Tel: 01509 222423. Email: Z.C.Stockdale@lboro.ac.uk

The University also has a policy relating to Research Misconduct and Whistle Blowing which is available online at http://www.lboro.ac.uk/admin/committees/ethical/Whistleblowing(2).htm.

Appendix D. Informed Consent Form

INFORMATION SECURITY BEHAVIOUR IN ORGANISATION (BRUNEI DARUSSALAM)

INFORMED CONSENT FORM

(to be completed after Participant Information Sheet has been read)

The purpose and details of this study have been explained to me. I understand that this study is designed to further scientific knowledge and that all procedures have been approved by the Loughborough University Ethical Approvals (Human Participants) Sub-Committee.

I have read and understood the information sheet and this consent form.

I have had an opportunity to ask questions about my participation.

I understand that I am under no obligation to take part in the study.

I understand that I have the right to withdraw from this study at any stage for any reason, and that I will not be required to explain my reasons for withdrawing.

I understand that all the information I provide will be treated in strict confidence and will be kept anonymous and confidential to the researchers unless (under the statutory obligations of the agencies which the researchers are working with), it is judged that confidentiality will have to be breached for the safety of the participant or others.

I agree to participate in this study.

Your name _____

Your signature _____

Signature of investigator _____

Date _____

Appendix E. Pilot Interviews Schedule

Introduction (Interviewer)

- On the research objectives
- Structure of the interview

Introduction (Interviewee)

- Demographic details
- Work Details
- Experience
- Nature of responsibilities
- Nature of Data/information handled and processes
- View on Data/information importance to their organisation/development
- View on Data/information importance to their own tasks/development
- Existing protection for information (sufficient/efficiency)
- Personal information security hygiene? Does it correspond to organisation's Information security hygiene?

Introduction to Case Base – Critical incidents

- Introduction of incident 1-4 (discuss with participants the nature and how the incidents unfold)

Discussion of Critical incidents

- If experienced, what was their reaction, if not what would they have done
- Justification of their action and decision
- What do they think, significant others will react
- Justification of their "perceived action" by their significant others

Appendix F. Other Theories

THEORY	MAIN POSITIONS	SIGNIFICANT POINT(S)
SOCIAL LEARNING THEORY **ALBERT BANDURA**	People are motivated by a) how they value and need a goal b) their expectation of achieving the goal. One's judgments, beliefs, and expectations predict behaviour more than anything	People learn through observing others' behaviour, attitudes, and outcomes of those behaviours. "Most human behaviour is learned observationally through modelling: from observing others, one forms an idea of how new behaviours are performed, and on later occasions this coded information serves as a guide for action." (Bandura)
THE TRANSTHEORETICAL MODEL AND STAGES OF CHANGE (TTM) **PROCHASKA & DICLEMENTE, 1983; PROCHASKA, DICLEMENTE, & NORCROSS, 1992**	The notion of readiness to change, or stage of change, has been useful in explaining and predicting changes for a variety of behaviours including smoking, physical activity, and eating habits Stages of change is a heuristic model that describes a sequence of steps in successful behaviour change: pre-contemplation (no recognition of need for or interest in change), contemplation (thinking about changing), preparation (planning for change), action (adopting new habits), and maintenance (ongoing practice of new, healthier behaviour)	Changes to behaviour does not always happen in a linear manner they often recycle and repeat stages (e.g., individuals may relapse and go back to an earlier stage depending on their levels of motivation and self-efficacy).

EXPECTANCY VALUE MODEL **MARTIN FISHBEIN**	According to expectancy-value theory, behaviour is a function of the expectancies one has and the value of the goal toward which one is working. Such an approach predicts that, when more than one behaviour is possible, the behaviour chosen will be the one with the largest combination of expected success and value. Expectancy-value theories hold that people are goal-oriented beings. The behaviors they perform in response to their beliefs and values are undertaken to achieve some end.	Expectancy-value theory suggests that "people orient themselves to the world according to their expectations (beliefs) and evaluations". Utilising this approach, behaviour, behavioural intentions, or attitudes are seen as a function of • expectancy (or belief) – the perceived probability that an object possesses a particular attribute or that a behavior will have a particular consequence; and • Evaluation – the degree of affect, positive or negative, toward an attribute or behavioral outcome" (Palmgreen, 1984).