Information security culture: A Behaviour Compliance Conceptual Framework

Salahuddin Alfawaz[1] **Karen Nelson**[1] **Kavoos Mohannak**[2]

[1] Faculty of Science and Technology, Queensland University of Technology
Brisbane, Australia
Email: s.alfawaz@isi.qut.edu.au
Email: kj.nelson@qut.edu.au

[2] School of Management, Queensland University of Technology
Brisbane, Australia
Email k.mohannak@qut.edu.au

Abstract

Understanding the complex dynamic and uncertain characteristics of organisational employees who perform authorised or unauthorised information security activities is deemed to be a very important and challenging task. This paper presents a conceptual framework for classifying and organising the characteristics of organisational subjects involved in these information security practices. Our framework expands the traditional Human Behaviour and the Social Environment perspectives used in social work by identifying how knowledge, skills and individual preferences work to influence individual and group practices with respect to information security management. The classification of concepts and characteristics in the framework arises from a review of recent literature and is underpinned by theoretical models that explain these concepts and characteristics. Further, based upon an exploratory study of three case organisations in Saudi Arabia involving extensive interviews with senior managers, department managers, IT managers, information security officers, and IT staff; this article describes observed information security practices and identifies several factors which appear to be particularly important in influencing information security behaviour. These factors include values associated with national and organisational culture and how they manifest in practice, and activities related to information security management.

Keywords: information security management, conceptual framework, information security culture, information security behaviour and compliance.

1 Introduction

Studies have shown that non-technical issues are at least as important as technical issues in safeguarding an organisation's sensitive information (Dhillon and Torkzadeh, 2006; Siponen and Oinas-Kukkonen, 2007). The importance of non-technical issues related to security management, however, has been deemphasised in many studies by virtue of their quantitative nature (Siponen and Oinas-Kukkonen, 2007). As a result, little attention has been paid to the role of human factors (e.g. individual choice and behaviour) or to organisational factors such as national and organisational culture, environment, and levels of information security awareness, and how these factors relate to attitudes about information security and its management. However, studies have shown that these factors are crucial to successfully of safeguarding organisational information assets and that user input is imperative in addressing information security management strategies or issues (Vroom and von Solms, 2004).

There is general consensus that the purpose of information systems security is to ensure business continuity and minimise damage by preventing and /or minimising the business impact of security incidents. Dhillon et al. (2007) argue that "computer crime committed by internal employees is essentially a rational act" that may result from internal or external factors (e.g personal factors, work situation and available opportunities). These authors assert that behavioural security holds the key to successful information system security management (Dhillon et al., 2007).

Information security compromised by organisational insiders (employees and other stakeholders who have physical and/or logical access to organisational assets) can pose an enormous threat to an organisation's information systems. The risk posed to data by insiders needs to be closely monitored and managed. This risk can takes two forms. The first form of risk is that posed by malicious insiders who deliberately leak sensitive data for personal financial gain or other criminal purposes. The second form of risk is from insiders who unintentionally exposure data. Both these forms can result from carelessness or attempts to work around security measures. Information security management theorists assert that the behaviour of users needs to be directed and monitored to ensure compliance with security requirements (Vroom and von Solms, 2004; Dhillon et al., 2007; von Solms and von Solms, 2004). This view suggests that the success of an information security program depends on users' behaviour related to information security. Therefore, we contend that a better understanding of the characteristics of users' information security behaviours, will assist in assessing, improving and auditing individual information security behaviours, particularly in dynamic security environments.

Fishbein and Ajzen (1975) present the theory of reasoned action (TRA). TRA seeks to explain that an individual's behaviour or action is determined by his or her intention to perform such behaviour. Thus,

TRA considers that behaviour is determined by intention - which is in turn influenced by the individual's attitude towards performing that behaviour, and subjective norms (social pressures to perform the behaviour). The theory of reasoned action and its extension the Theory of Planned Behaviour (TPB) (Ajzen, 1985) have been applied in several studies relating to information security issues. More specifically, in risk perception, and security-related behaviour, both theories suggest that "ease of use" is an important factor affecting human behaviours. Siponen (2000) finds that the issues associated with "ease of use" of security solutions (e.g. techniques and adherence to procedures) has not been well addressed in the security literature. He suggests that a qualitative research approach would be appropriate to investigate this topic.

Earlier research has suggested several factors are crucial to information security policy adherence and user awareness. For example, Straub et al. (1993) applied the deterrence argument that information security actions will deter users from committing unauthorised acts. The deterrence argument has also been applied to improving the quality of information security policies (von Solms and von Solms, 2004), promoting security awareness (Straub and Nance, 1990), developing structures of responsibility (Dhillon et al., 2007) and protecting assets by motivation (Workman et al., 2008). Each of these studies provides important insights into specific issues relating to users adherence with security policies. To some extent, these studies all draw on the theory of reasoned action (TRA) and the theory of planned behaviour (TPB) (Fishbein and Ajzen, 1975; Ajzen, 1985), to understand and test constructs related to individuals' information security behaviours.

However, most of these studies, have paid little attention to the influence of national and /or organisational culture on employees attitudes, beliefs, and behaviours, or to the interactions between the individuals and their context. These interactions, may also contribute to an individual's beliefs and values about information security and its management.

2 The Analytic Framework

While there are some normative models for information security behaviour which are reported to work for one or two firms, there is little in the way of general guidance. The research reported here thus represents a preliminary attempt to identify a descriptive measure of information security related behaviours that are applicable for different types of organisations.

Classification theory suggests that classifying perceptions is crucial to human survival and adaptation, and attempts to explain the nature of concepts (categories/ classes) and why humans classify things (Smith and Medin, 1981; Parsons, 1996). Stanton et al. (2005) suggest that it is important to have a systematic view of end users security behaviour to facilitate accurate auditing and assessment of this behaviour. Therefore a classification that emphasises the characteristics of the organisational subjects who may perform authorised or unauthorised actions is proposed as helpful to understanding individual information security behaviour. Such a classification may serve two purposes for an organisation. Firstly, categorising a phenomenon makes systematic studies possible, and secondly, classification may assist organisations prioritise their information security efforts.

The term "knowing-doing gap" refers to people who have knowledge but do not take action or behaviour consistent with that knowledge (Pfeffer and Sutton, 2000). Workman et al. (2008) used this concept to investigate people's security behaviour referring to "people who have been trained but then do not use their new knowledge or skills as management expects". Following this analogy, we propose other possible patterns of an individual's behaviour with respect to information security practices. We choose to call these patterns modes (where mode means a "manner or way of acting, doing, or being; method or form") (Webster's New World Dictionary).

Based on an individual's acknowledgment of the security rules and possession of the essential skills for performing certain actions, we identify four modes to categorise individual security behaviours: Knowing-Doing mode, Knowing-Not doing mode, Not knowing-Doing mode and Not knowing-Not doing mode. Table 1 summarises the four modes. Figure 1 depicts these modes and their inter-relationships. The arrow lines connecting each mode represent the dynamic movement of each mode, which draws influences from individual's skills, knowledge and values based on change across the internal and external environment. Each mode is defined, theoretically justified and supported with relevant example/s as follows.

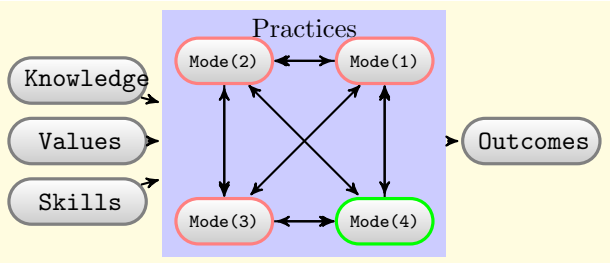

Figure 1: Information Security Behaviour Modes

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

An example is a user who is not aware of the existence of organisational information security policies; he/she cannot be expected to follow them. Regardless of the presence of the necessary resources and the motivation to succeed, he/she can still fail to comply because they lack the knowledge of requirements/rules. An employee who has just joined the organisation or a manger who just been promoted to a new position may belong to this mode. This mode is a type of cognitive failure. Cognitive failures include issues such as: misunderstanding the security policy, missing an update of the policy, and poor decision-making.

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

Table 1: Information Security Behaviour Modes

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

A subject who is not aware of organisation information security policies, but asks supervisors or coworkers before taking certain actions, is an example of this mode. Some people may exercise more caution than others when they are uncertain how to act. This prudent behaviour demonstrates the conventional economic concept of being risk averse. The concept of risk being averse suggests that, when facing choices with the same outcomes, subjects tend to choose the less-risky one (Friedman and Savage, 1948). To some extent, this mode is also traceable to the self-regulatory model, which identifies rule-following as "originating within an individual's intrinsic desire to follow organisational rules" (Tyler et al., 2007).

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

Given their knowledge, skills and sometimes authority over others, it seems reasonable to expect that employees will comply with the requirements/rules. However, this is sometimes not the case. An example of this mode is a person who has been trained but then does not use his new knowledge or skills as management expects (Workman et al., 2008) or a top manager or IT staff member who takes advantage of his position to compromise the rules (Dhillon, 2001). This mode suggests that while knowledge and skills are a key contributor to users behavioural output they are not the only ones. Theories of cognitive psychology explain why people may irrationally behave. One explanation is that a person's set of beliefs, or culture, may influence their actions. This suggests that if a person has a tendency to perform an authorised act and this tendency needs to be influenced, one has to focus on changing their primary belief system (Dhillon, 2001). In this regard, Dhillon suggests that exposing employees to information about the consequences of their action may produce a change in their behaviour.

Mode(4): Knowing- Doing: In this mode, which takes the lower right corner of the model, the subject Knows the rules of behaviour and has the knowledge/skills and they are Doing the right behaviour (following the rules - security is not compromised).

This mode is based on the assumption that employees are rational actors who will comply with requirements because they have the necessary knowledge and skills. This mode is based on the view that people follow rules as a function of cost-benefit analyses (Stout et al., 2001). As in the case of mode 2, mode 4 is also linked to the self-regulatory model.

While mode 4 appears to be the *"perfect mode"* for management to target, there are at least two reasons why it is risky to rely on this mode alone. The first reason is that the information system security discipline is rapidly evolving as is the threat environment, and the required level of knowledge and skills. Yet, Mode 4 assumes that actors are able to keep their knowledge and skills current. This has always been a major challenging and costly task. The second reason is that it is not enough to secure the system by relying on those subjects who have the knowledge/skills and are Doing the right behaviours. Mode 4 requires the same level of planning, monitoring and managing as the previous modes. Furthermore an employee's behaviour may change from one mode to another, depending on their organisational role, the state of technology development, and the status and availability of security training.

3 Method

This article presents the findings from three exploratory case studies conducted in organisations in Saudi Arabia. Three methods were used to collect qualitative case data: semi-structured interviews, field notes and document analysis. For the purposes of this study, efforts were made to select diverse case organisations to allow for different of business, organisational size and approaches to information systems security management. The organisations selected for the study are Case A - a private organisation in the over 5000 employees category, Case B - represent participants from public organisations and Case C - a non-profit organisation which employs approximately 3,600 people, organisations in Saudi Arabia. The research was conducted in three phases over three years (January 2007-December 2009). This paper presents the preliminary result of this study. The first phase involved gathering data on the case organisations information security management approaches and practices to establish a baseline for later research. The sources of data for the interviews were senior managers, information security managers, functional managers, IT specialists, and IT users in each of the case study organisations.

In total, 13 interviews were conducted in case A, 16 in case B and 11 in case C with a further 7 interviews being carried out with Saudi PhD students who hold a related IT position in their work. Each interview lasted on average one and a half hours. The interview data was supplemented by a range of documentary evidence. This evidence was acquired from sources such as field notes, annual reports, organisational charts, official policy statements, and corporate Web sites.

4 Analysis and Findings

In all three cases, participants were asked to identify three main causes of security incidents as well as the obstacles to achieving improved information security compliance in their organisation. The interview data from the three cases revealed that behavioural issues associated with users' security compliance behaviour were the most common concern. These issues include password sharing, using shortcuts, downloading Internet software, surfing potentially harmful content, ignoring relevant procedures, not sharing information and knowledge relevant to information security practices, not reporting security violations, and not enforcing security-related rules.

The first main cause of security incident was cited as users' errors or non-compliance. One IT manager pointed out that user error was the main cause of many of the information security incidents.

> *"all of the analyses we conducted on the various aspects of security incidents have identified careless and violation of policy rules as the main causes of accidents."*

The second cause identified in all three cases may arise from first and was identified as attacks from viruses and malicious software. In Cases A and C, the third factor identified was hardware failure, while in Case B the third factor was system administrator errors or non-compliance. This variation may reflect that both Cases A and C had issues relating to budget constraints. In other words, these case organisations cannot afford to implement effective security mechanisms and procedures to protect themselves or they have other more important budgetary priorities. Another possible explanation is that both Cases were lacking information security staff or their current staff did not have the required level of skills. Whereas in Case B the issue seems to be more related to IT staff not following the right procedures and using shortcuts rather than lacking the required skills.

In terms of the obstacles to achieving improved security compliance, the cross-case analysis presented in Table 2 indicates that the participants in Case B and C saw the lack of clear direction in security procedures and roles as the major obstacle. In Case A, the lack of awareness and training programs was identified as the first obstacle, while the lack of clear direction in security procedures and roles came as a second. This is followed by the lack of motivation programs as the third obstacle in all three cases.

The variation between the cases appears to indicate existence and implementation of an organisation-wide information security policy in Case A. Whereas in both cases B and C information security procedures and rules were embedded in other organisational polices. Nevertheless, in Case A, participants identified "lack of awareness" as the second obstacle which indicates that that communicating the information security policy to the users is an issue of concern of Case A. Table 2 shows the main causes of security incidents and obstacles to achieving improved security compliance in the three cases.

Table 2: The main causes of security incidents and obstacles to achieving improved security compliance in the three cases

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

In order to build in-depth inferences from the case studies, further data analysis was conducted to visualise and identify patterns and relationships between individuals' information security related behaviours. The aim was to determine whether or not the conceptual model (illustrated in figure 1) and four modes comprehensively describe individuals' information security behaviours that occur in the course of conducting their daily work.

The results presented in Table 3 seem to suggest the plausibility of the four modes, for Cases A, B, and C. While there were similarities in terms of all

four modes of information security behaviour being present in the three cases, variations were found in the behaviours related to each of the modes. Based on our findings from three case studies we placed each case on a grid chart (see Figure 2), as red, green and blue circles representing Case A, Case B and Case C respectively. The case study findings are reported below through an exploration of the framework's four modes as follows.

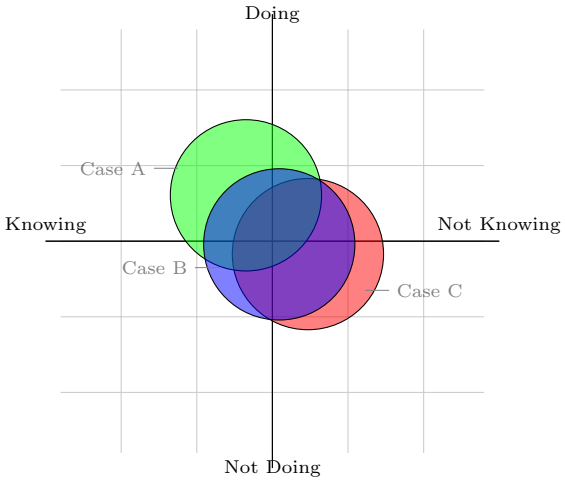

Figure 2: Information Security Behaviour Modes at the three cases

Mode(1):Not Knowing-Not Doing mode:

In Cases B and C, individuals were not aware of their organisations' information security policies; hence, they could not be expected to act to follow them. As noted earlier, regardless of having the necessary resources and the motivation to do so, if an individual lacks knowledge of the requirements or rules he/she may not exhibit appropriate information security behaviours. This is a type of of cognitive failure that also includes issues such as misunderstanding the security policy or missing an update of the policy. In Cases B and C there was no evidence to show that unified and / or clearly articulated information security policies had been communicated to users. The lack of understanding about policy appeared to be the main contributor to most of the non-compliance issues reported by Case B and C.

For instance, respondents from both Cases B and C raised the importance of organisational policies to the development of information security (e.g. policy that seeks to standardize managerial procedure). It also appeared that the lack of clarity about what kind of procedures needed to be followed and enforced contributed to the lack of information security compliance in Case Organisation C.

One IT staff member explained:

> *" mostly individuals are taken for granted to do the right thing [following information security rules and procedures] but, unfortunately, individuals in most cases doing the wrong things"*

Managers from different departments also supported IT staff views that the absence of clear information security procedures and directions had contributed considerably to information security system incidents. All the interviewees in Case C, indicated that they were not familiar with the information security policy, although the IT manager made the following observation:

> *"It [the information security related procedures] has provided us with some guidance in different cases,initially. Now whether all departments would have followed and enforced them is another question"*

Mode(2): Not Knowing-Doing mode:

The data collected from the case the interviews showed that most of the participants in three Cases were risk averse which although they do not know predisposes them to act conservatively. This aversion was mainly attributed to the belief that taking risks could affect their organisation's information assets. In Case A, and to a some extent, in Case B, a combination of self-consciousness as a member of the organisation and a willingness to abide by the organisation's rules indicated two aspects of both Case's organisational cultures. The first aspect was a sensitivity to losing information, knowing that they will be questioned about. The other was the hope for a reward, through the KPIs systems, as well as group bonus schemes, which were linked to organisational performance in the case of case A.

In a similar vein, all participants pointed out that cultural values can influence employees' information security related behaviours. For example one participant noted:

> *"certain cultural values could make people do the right thing but other values may not"*

One can infer from the last part of this statement that certain individual cultural values may have a positive or negative influence on employees' security behaviour. Most of the case data appears to support this claim, for instance respondents indicated that there is a cultural influence on individuals' security-related behaviour which poses challenges, although managers may overcome these challenges by extended exposure to managerial activities such as training and/or awareness. However, some respondents did not see all personal cultural values as having a negative influence, especially in the context of individual security related behaviour. One manager summarised his thoughts:

> *"There are different components of the personal culture. Some of these values are good in promoting good behaviour"*

He went on to illustrate his point using an example showing that some cultural values are useful in positively influencing individual security behaviour:

> *" in some cases religion values dictate where one is going. These religion values may hold one from visiting prohibited sites which usually have some viruses or spywares that could cause security related problems."*

Table 3: Modes of individuals' behaviour of information security culture in the three Cases

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

This data indicates that some cultural values may impact on an individuals security-related behaviour and ultimately influence information security culture in a positive way.

This last point can be further examined by understanding aspects of the relationship between managers and employees. As is common for national cultures that score high on Hofstede's (1984) Power Distance dimension such as Saudi Arabia, executives and managers at upper-levels are sought out for advice and guidance (Hofstede, 1984). In a high Power Distance culture, employees usually rely on managers to solve work issues, because managers often attain the role of problem-solver. The impact of the Power Distance dimension is reflected in some of the information security managers' comments:

> *" When they [employees] face problem they come to me and I do my best.."*

> *"We direct them [employees]."*

In these cultures IT staff report issues to the IT Manager, who provides guidance and directives, which are then actioned by the IT department staff. As one IT staff member commented:

> *"We follow the organisation's procedures by getting the decision from high management."*

These comments suggest that people may lack the experience to resolve problems since managers deal with issues in the absence of explicit procedures. Under these conditions, undesirable employee information security behaviour and actions may be minimised as most activities have to be approved by immediate managers or work supervisors.

Although negatively affected by the lack of sharing and motivation mechanisms, some employees have adopted informal means for sharing information and knowledge related to information security systems. Members of Case A, for example, meet after work and the conversation usually turns to something that happened during their work hours. Whenever the group are together they discuss issues and problems encounter in their daily work. As one participant explained:

> *"Yes, we discuss some [ISM]issues in our lunch brakes or at the informal meetings. It is a good opportunity to ask for opinions or share some experience with colleagues.... Not only with IT people but with others as well, such as HR people.."*

Mode(3):Knowing-Not Doing mode:

The data revealed that there was careless risk taking by individuals who used shortcuts, downloaded internet software, and surfed harmful internet content. These practices, as noted, varied between the three cases. In Cases B and C these behaviours can be mostly attributed, to the lack of and poor clarity about the rules and consequences of taking information security risks. Whereas in Case A, the data indicated intentional incidents relating to non-compliant behaviour. For example, Case A's Intranet

sites are updated regularly with security information, and employees are encouraged to access these sites on a regular basis. However, there was a perception that many of the organisation's members did not take these routine information security awareness programs seriously. One participant commented on security warning e-mails:

> *"the IT department sends a lot of warning e-mails related to security issues...almost every day...but I'm sure not every one takes them seriously."*

Another participant admitted that:

> *"Because some people do not have enough time they delete warning e-mails without even bothering to look at them..."*

Mode(4):Knowing-Doing mode:

The level of information security culture in all three cases indicted that majority of information security related behaviours fit into this mode. Data showed that members in all three cases believed that the organisation's dependence on information systems is "very high and security is an integral part of this equation". Most participants indicated that there was a certain level of comfort with the progress that their IT department was making in information security related areas. For example, in all cases, the data showed that top management commitment to information security was exemplified by allocating the necessary resources and adopting technical solutions to enhance information security programs.

The influence of national culture traits (for example, Hofstede's Power Distance dimension) may be seen in the practices associated with this mode. Saudi Arabia is a high Power Distance society, and data from all three cases indicated that individuals intended to follow the expectations of management and they are more likely to approve actions that they perceive to be supported by functional managers and work supervisors. These traits appear to be having a substantial influence on individuals' information security related behaviour in all three case studies.

Furthermore, the data indicated that a combination of self-consciousness as a member of the organisation and a willingness to abide by the organisation's rules was present in the organisational culture of the three cases. The sensitivity of losing information, knowing that they will be questioned about and the hope for rewards for reporting security incidents were also key factors in individuals' compliance with information security requirements.

However, as previously discussed, we should expect organisations' actors to keep their knowledge and skills current and it is not enough to secure the system by addressing the concern of those who have the knowledge/skills to do the right things alone. Organisations are going through a rapid and costly change as they seek to adjust and perform in the changing environment (e.g. new regulations, new technology and new threats). Therefore, mode 4 requires the same level of planning, monitoring and managing as the previous modes. An employee's behaviour may alter from one mode to another, depending on the organisational role the subject happens to be in, the state of technology deployment, and the relevance and availability of the suitable training.

5 Discussion and Next Steps

The findings supported the proposed model of the four modes of information security behaviour. A number of factors appeared to be interrelated. These inter-related factors included organisational cultural values manifest in practices and activities related to information security management, and factors related to the national culture, particularly the influence of power-distance on individual. The most important factors identified in this study were top management commitment, the level of training and IT skills, security awareness programs, organisational IT structures, the appointment of information security managers, type of motivation system utilised, existence of information security policy, and adoption of information security standards. Other factors were related to the influence of national culture on values in decision making, compliance, risk taking, sharing culture, collaboration, enforcement, reporting, and communication. Hence, these findings are consistent with the view that an individual actor's decision to comply with security requirements is not only a function of the their knowledge and skills or the perceived cost-benefit of the behaviour as described in economic theories, but also, a function of the factors arising from the users' psychology and the social setting in which the actor is situated. Therefore it is crucial to understand how aspects of organisational and national culture inform employees' practices in order to achieve a high level of information security culture.

The complexity inherent in contemporary organisations suggests that organisations will have individuals who do not share a view of information security, and yet are expected to participate in the information security culture of that organisation. These disparate views may be attributed to the different assumptions, attitudes and values towards the information system implementation and use processes held by each of employee. Variation may also be related to, rapid technological advances bringing about an increase in the range of tools used for conducting unauthorised behaviours. Another noteworthy point, is that most employees assume the security of their organisation is not their responsibility and that only IT staff are responsible. Therefore, it is important to understand, what underlying principle values, beliefs and assumptions drive users behaviour. This is further complicated by the rate of change in the information systems environment with respect to security threats, which makes it unwise to assume that individual knowledge/skills will be current and that individual behaviour will remain as expected.

The challenge is now to determine the parts of an organisation's environment that facilitate and enable sustainable approaches to information security adherence. This is a complex issue with no easy answers. One aspect emphasised in the literature is the notion of creating a security culture, which is emerging as a goal for governments and corporations in their attempts to safeguard their information assets. We contend that a culture that encourages ethical conduct and commitment to compliance with information security requirements is a desirable organisational attribute. Many researchers have addressed the importance and the need for an information security culture in organisations (Chia et al., 2002; Ruighaver et al., 2007; Schlienger and Teufel, 2002, 2003; Zakaria and Gani, 2003; Zakaria, 2004). They all suggest that organisations must take affirmative steps to create an environment where security is "everyone's responsibility" and doing the right thing is the norm.

These observations provide a basis for us to propose *"the information security culture mode"*. In this mode organisations would work towards developing an information security culture where all employees adhere to its information security policy and rules even when no one is around and when their behaviour is not being monitored. Practices in mode 5 would also include cooperative information security, such as taking action against acts that would jeopardise the information security system for example, reporting unauthorised acts, and sharing security-related information and knowledge through the appropriate formal and informal channels.

In order to achieve the mode of information security culture, two things will need to occur. Firstly, the environmental factors that influence behaviour and encourage or inhibit individual employees and managers from doing the right thing, even when they know what the policy says, should be identified. Secondly, an effective management strategy that handles both internal and external factors critical to information security should be implemented.

This paper provides some insights but, clearly, additional investigations are required. Hence, we propose that a multi-methodological approach will be required to capture the richness of the information security management systems (ISMS) implementation processes in developing countries and the influence of both organisational and national culture values on information security culture development. More specifically, this second phase will explore information security management related activities within organisations in the Saudi Arabia context and how individual manager and employee personal values may affect the transition towards an information security culture. The study will use an integrated framework that incorporating information security culture into existing cultural models. Further, the study will adopt change management as an effective management strategy that manages both internal and external changes.

6 Conclusion

Based on evidence from three exploratory case studies, we populated a framework of information security practices that could contribute to information security management by identifying behaviours related to four modes of information security practice. The aim was to classify individual information security behaviours in organisations to ensure the development of high quality information security cultures. The information security modes described in this paper provide a sound basis that can be used to evaluate individual organisational members' behaviour and the adequateness of existing security measures.

Although this approach does not deliver completely new measures, it leads to a more consistent set of security parameters which aim to protect against individuals non-compliant behaviour. The main strength of our approach is that it takes into account the complexity of human behaviour and their corresponding actions.

We conclude this paper with three remarks. First, although individual knowledge and skills are important, they alone are not enough to assure a positive contribution towards information security culture reliant on employee behaviours. Second, a person's set of beliefs, or personal culture, plays a major role in influencing their personal attitude towards their security behaviour. Hence, understanding their underling beliefs is crucial in the process of behavioural change. Third, the influence of technology, social environment, regulation and self-interest all contribute to employees security-related behaviours. As a result members of an organisation will could exhibit behaviours from different modes at different points in time. This continuous movement makes it hard to secure an organisation's information system by addressing a single mode in isolation. Hence, future research efforts should concentrate on investigations of these factors. The research findings and the model described in this paper may serve as resources for further investigating the human, (organisational and individual) aspects of effective information security systems.

References

Ajzen, I. (1985). *From Intentions to Actions: A Theory of Planned Behavior*. Springer, Heidelberg, Germany.

Chia, A., Ruighaver, B., and Maynard, B. (2002). Understanding organizational security culture. *Proc. of PACIS2002, Japan*.

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

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

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

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

Friedman, M. and Savage, L. (1948). The utility analysis of choices involving risk. *Journal of Political Economy*, 56:279–304.

Hofstede, G. (1984). *Cultures consequences: International differences in work-related values*. Beverly Hills, CA: Sage Publications.

Parsons, J. (1996). An information model based on classification theory. *Management Science*, 42(10):1437–1453.

Pfeffer and Sutton (2000). *How Smart Companies Turn Knowledge into Action*. Harvard Business Press.

Ruighaver, A., Maynard, S., and Chang, S. (2007). Organisational security culture: Extending the end-user perspective. *Computers & Security*, 26(1):56–62.

Schlienger, T. and Teufel, S. (2002.). Information security culture the socio-cultural dimension in information security management. *FIP TC11 international conference on information security, Cairo, Egypt; 7-9 May 2002.*

Schlienger, T. and Teufel, S. (2003). Analyzing information security culture: increased trust by an appropriate information security culture. *Database and Expert Systems Applications, 2003. Proceedings. 14th International Workshop on*, pages 405–409.

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

Siponen, M. and Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *SIGMIS Database*, 38(1):60–80.

Smith, E. and Medin, D. (1981). *Categoriesa nd Concepts*. Harvard University Press, Cambridge, MA.

Stanton, M., Stam, R., Mastrangelo, P., and Jolton, J. (2005). Analysis of end user security behaviors. *Journal of Computers and Security*, 24:124–133.

Stout, L., Blair, and Margaret, M. (2001). Trust, trustworthiness, and the behavioral foundations of corporate law. *SSRN eLibrary*.

Straub, D. W., Carlson, P. J., and Jones, E. H. (1993). Deterring cheating by student programmers: A field experiment in computer security. *Journal of Management Systems*, 5:33–48.

Straub, D. W. and Nance, W. D. (1990). Discovering and disciplining computer abuse in organizations: A field study. *MIS Quarterly*, 14:45–62.

Tyler, T., Patrick, C., and Jeffrey, F. (2007). Armed, and dangerous (?): Motivating rule adherence among agents of social control. *Law & Society Review*.

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

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

Workman, M., Bommer, W. H., and Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, 24:2799–2816.

Zakaria (2004). Understanding challenges of information security culture: a methodological issue. In *the second Australian information security management conference, Perth, Australia; 26 November 2004*.

Zakaria, O. and Gani, A. (2003). A conceptual checklist of information security culture. In *in 2nd European Conference on Information Warfare and Security, Reading, UK*.