Information Security and People: A Conundrum for Compliance

Hiep Cong Pham
RMIT University Vietnam
hiep.pham@rmit.edu.vn

Duy Dang Pham
RMIT University Vietnam

Linda Brennan
RMIT University

Joan Richardson
RMIT University

Abstract

This evaluation of end-users and IT experts/managers' attitudes towards performing IT security tasks indicates important differences between their perspectives on what is and is not necessary to establish a secure corporate IT environment. Through a series of case studies, this research illustrates that making it easier for end-users to comply does not necessarily equate to enhanced implementation of security measures. End-users want to be autonomous, competent, self-motivated and active participants in the development of secure environments. However, managers and experts want to limit autonomy to ensure that procedures are followed closely, rather than permitting flexibility. This results in the creation of environments that are intrinsically de-motivating rather than motivating end-users to become self-determined and self-regulating co-creators of a secure IT environment. The paper also discusses alternative approaches to developing a human system that works for end-users and experts.

Keywords: security compliance; security management; end user security behaviour

1 Introduction

Information security management is designed to address four phases of organisational security risk management: deterrence, prevention, detection, and recovery (Warkentin and Willison 2009). End-user compliance plays a key role in ensuring the effectiveness of the "prevention" phase by avoiding risky practice. A majority of prior researches in the field have explored the motivation for security compliance, which consists of a wide range of internal and external factors to an individual. Internal factors can be for example, self-efficacy (Dang-Pham and Pittayachawan 2015, Johnston and Warkentin 2010, Rhee et al. 2009) or security goal orientations (Pham and Nkhoma 2015), while external factors come from sanctions and rewards (D'Arcy et al. 2014, Herath and Rao 2009a) , security culture (Ruighaver et al. 2007) and climate (Goo et al. 2014, Dang-Pham et al. 2015), as well as security demands and resources (Pham et al. 2015, Pham et al. 2016).

Security compliance researchers have conducted quantitative studies to evaluate the impact of specified factors on compliance (Crossler et al. 2013, Sommestad et al. 2014). However, there has been a paucity of qualitative studies designed to increase understanding of how users experience security-related issues. Qualitative studies can yield rich perspectives in settings where human factors may intervene in planned outcomes. Recent studies employing qualitative approaches have provided further insights into how the users experience security practices (Albrechtsen and Hovden 2009, Pham et al. 2015, Pham et al. 2016, Dourish et al. 2004), and compared security perspectives between general users and security experts (Albrechtsen and Hovden 2009, Posey et al. 2014). These studies have been useful in establishing that there are gaps between intentions and behaviours in security compliance contexts. However, it is not known if these gaps are because of (lack of) expertise or knowledge,

or if something more calculated or deliberate is at the root of breaches in security. Further, it is not known if end-users, experts or otherwise, share the concerns of IT security managers when it comes to security compliance. A gap between manager expectations and end-user performance is unlikely to be conducive to a secure environment.

Our study takes a qualitative approach and explores the perceptions between average end-users and security experts/managers on five factors; namely risk evaluation, cost of compliance, formal compliance evaluation, self-efficacy, and social influences. The five studied factors were based on established behavioural theories including protection motivation theory (Rogers 1975), the theory of planned behaviour (Ajzen 1991) and rational choice theory (Becker 1968). A number of previous studies have provided empirical evidence that the listed factors influenced security compliance (Dang-Pham and Pittayachawan 2015, Guo and Yuan 2012, Siponen et al. 2014, Vance et al. 2012, Ifinedo 2011). However, little research appears to have compared how end-users and security experts/managers perceive the impact of these factors on security compliance. Understanding such diverse perspectives from both end-users and security managers can facilitate development of security programs that align with users' expectations and improve end-users' security compliance.

2 Literature Review

Earlier quantitative studies often employed well-founded behavioural theories to explain security compliance (Sommestad et al. 2014). Behavioural theories are widely applied to the information security context. Factors that influence security compliance include security risk evaluation and cost of compliance from protection motivation theory (Vance et al. 2012, Ifinedo 2011, Herath and Rao 2009b), security compliance evaluation (sanctions and rewards) from rational choice theory (Vance and Siponen 2012, Bulgurcu et al. 2010, Li et al. 2010), self-efficacy and social influences from planned behaviour theories (Ifinedo 2011). These theories have been found to affect security compliance to some extent in the aggregate. However, most quantitative studies did not examine whether average end-users and security experts/managers complied differently (Sommestad et al. 2014). In this case aggregate data cannot adequately inform management decision making because the aggregate user is a non-existent artefact of statistics, such as is derived when gender results are averaged to produce a mean that is neither male nor female.

It is not uncommon for information security stakeholders to hold different perspectives about security issues. Several studies have explored such perspectives. For instance, different perceptions of ownership over security issues amongst staff and managers were found to result in end-users' rejection of security controls by forcefully breaking into the computer room (Adams and Blandford 2005). Disagreements on the effectiveness of security controls and preferences between management and technical staff were also noted in Mouratidis et al. (2008) where the management staff had doubts about the organisation's network security system in spite of the security team's confidence in the system's effectiveness. In addition, Albrechtsen and Hovden (2009) found that security managers perceived end-users to be a major threat to security effectiveness, whereas the users were actually interested in contributing towards organisational security protection. Security professionals and regular end-users were also found to evaluate security threats and coping measures differently in their workplaces (Posey et al. 2014). For example, the managers saw the users as potential security threats whereas the users perceived security threats as external agents such as hackers and Internet viruses. While these qualitative studies revealed the gap between different stakeholders, especially between end-users and security experts/managers' perceptions of various information security issues, only Posey et al. (2014) adopted protection motivation theory as a theoretical framework to guide their qualitative research.

We contend that there has been a gap between the quantitative and qualitative studies of security compliance. Quantitative studies have not addressed the different perceptions towards security factors among business roles of the stakeholders, while there is a paucity of established theories employed in qualitative studies and they sometimes fall into the category

of description rather than theoretically founded research. Hence, positing alternative strategies is problematic.

This study aims to fill the gap by qualitatively examining how end-users and security experts/managers perceive five common factors that have been found to influence security compliance from several behavioural theories. The findings of the study would shed further insight into whether the two groups of users equally view these factors as effective in promoting security compliance. Each of the five factors is now discussed the following sections.

Factor 1: Security risk evaluation

Protection motivation theory (PMT) has been employed widely to explain how compliance could be motivated by fear of security threats (Dang-Pham and Pittayachawan 2015, Vance et al. 2012, Ifinedo 2011, Herath and Rao 2009b). One of PMT's main hypotheses is that adoption of protective measures is motivated by the cognitive process that evaluates the threats in terms of the degree of likelihood of an occurrence and the perceived severity of consequences (Rogers 1975). In fact, this hypothesis has been supported by a number of information security studies (Dang-Pham and Pittayachawan 2015, Ifinedo 2011, Vance et al. 2012). End-users would be motivated to respond to a security threat when it is evident and personally relevant to them. Furthermore, end-users and security experts had different perceptions of security threats (Posey et al. 2014, Albrechtsen and Hovden 2009). As a result, understanding how these stakeholders perceive security threats is important for security training and achieving compliance.

Factor 2: Cost of security compliance

The other main hypothesis based on PMT postulates that the end-user's cognitive evaluations of protective security measures' effectiveness and cost could impact on their adoption of the security compliance. Employees often perceive performing security practices as an adjunct task, which is secondary to their primary work duties. Hence, when there is a conflict between the need to perform security measures and primary tasks, end-users may ignore security requirements (Adams and Blandford 2005). The cost of compliance imposed on end-users has been identified as one of the key factors leading to non-compliance (Furnell and Rajendran 2012, Leach 2003). Furthermore, the complexity, vagueness, and overload of security tasks were found to negatively affect security compliance by causing stress and increasing moral disengagement with security programs (D'Arcy et al. 2014). In other words, security compliance depends on the extent of the effort that an end-user is required to exercise and their effort depends their engagement with the requirements (e.g. moral, emotional, psychological, or behavioural).

Factor 3: Formal security compliance evaluation

General deterrence theory has been used to explain why users comply with information security policies (Herath and Rao 2009a). Communicating the certainty and severity of sanctions for security non-compliance has been considered as an effective management strategy to prevent security non-compliance. However, inconsistent findings of the impact of sanctions have been reported (Sommestad et al. 2014). For example, fear of penalties for non-compliance has been found to have a significant impact on security behaviour (Herath and Rao 2009a, Kankanhalli et al. 2003). These studies found that if employees perceive high certainties of being caught for violating security policies, they were more likely to comply; moreover the certainty of being caught outweighs fear of the punishment severity. On the contrary, other studies found that sanctions did not have a significant impact on actual compliance (Herath and Rao 2009b, Hu et al. 2011, Pahnila et al. 2007).

Security compliance can also be motivated by external rewards (Bulgurcu et al. 2010, Padayachee 2012, Ruighaver et al. 2007). There have also been inconsistent results regarding the effect of rewards on compliance. Rewards were not considered a good predictor of intention to comply (Sommestad et al. 2014). For instance, Bulgurcu et al. (2010) found rewards, as a part of compliance's benefits, could influence employees' intention to comply. In contrast, Pahnila et al. (2007) did not detect significant effects of rewards on actual compliance.

Factor 4: Security self-efficacy

The concept of self-efficacy is described in social cognitive theory (Bandura 1977), and the theory of planned behaviour (Ajzen 1991) as a component of perceived behavioural control. This construct refers to one's self-confidence in their ability to mobilise motivation, cognitive resources, and actions needed to successfully complete a specific task within a given context. Self-efficacy has been recognised as a key factor that positively influences security compliance (Johnston and Warkentin 2010, Rhee et al. 2009). Self-efficacy is also included in the PMT model and is hypothesised to affect motivation to take security actions (Dang-Pham and Pittayachawan 2015, Vance et al. 2012), and especially that knowledgeable and skilful employees are more amenable to take protective security tasks. Self-efficacy is also strongly related to problem solving or solution seeking behaviours and therefore the development of competency. Acquiring competency is a goal for self-determination alongside autonomy and relatedness (Deci and Ryan 2000). However much automation in security systems is extant in the design, at some point, human factors will intervene. Consequently, a security system must be prepared for outcomes to be co-created between humans and the system that may not have been predicted at the outset, especially in a fast-paced changing environment. Therefore, the design and creation of human systems to support the IT system is also necessary for a secure environment.

Factor 5: Social influences

The impact of social influences on individual's behaviours and beliefs have been widely acknowledged (Cialdini and Goldstein 2004, Leenders 2002). Social influences are often referred to as subjective norms (Ajzen 1991) and can take the form of introjection motivation (Gagné and Deci 2005). For instance, subjective norms refer to the end-users' beliefs about the normative expectations and social pressure that drive people's intention to perform security behaviours, as posited in the theory of planned behaviour (Ajzen 1991). Similarly, self-determination theory (SDT) suggests that people complying with security requirements under introjection processes need to perform actions to maintain their ego which is associated with the surrounding social climate (Gagné and Deci 2005). The spectrum of motivating forces from amotivation through extrinsic, externally applied motivation, and then to self-motivating or intrinsic motivation (Ryan and Deci 2000) shifts the responsibility for compliance from 'other' to 'self'. SDT argues that people can become self-motivating via a series of regulatory processes from non-regulation through external regulation and incrementally internalising the requirements of the task until they become self-motivated. In compliance, self-motivation is the ideal where people can be trusted to work within relevant parameters without surveillance, thereby decreasing costs of security. In the absence of self-motivation, extrinsic factors and other people (social influences and relatedness) motivate people.

Social influences can have normative and informative effects while taking forms of direct persuasions or indirect comparisons (Brennan et al. 2014). It has been argued that people receive normative influence when they want to reduce ambiguity, whereas informative influence helps to clarify uncertainty (Ashforth 1985). Moreover, these influences can be achieved as people engage in direct communication, or indirectly compare their actions and beliefs with the others' perspectives as they establish a social identity (Leenders 2002). In an information security context, subjective norms have frequently been found to influence intention to comply with security policies and actual compliance (Herath and Rao 2009a). Padayachee (2012) discussed that introjection could be created and maintained by an information security climate, which subsequently affected compliance.

3 Research Method

3.1 Research design

The main research question of this study was how average end-users and security experts in organisations perceive the impact of the following factors on end-user security compliance.

1. Security risk evaluation

2. Cost of security compliance
3. Formal security compliance evaluation
4. Security self-efficacy
5. Social influences

A case study method was employed to investigate this question. The case study method is commonly described as an empirical enquiry suitable for investigating phenomena in their natural context, especially when the research topics are new and changing fast (Dubé and Paré 2003, Yin 2009). This research investigated the management of information security as an important topic in the information systems research domain which has been evolving rapidly over past decades (Dubé and Paré 2003). Moreover, the study involves the investigation of the complex relationship between multiple organisational stakeholders with different skills and knowledge. As a result, the case study method is appropriate for our research objective, which aims to examine in-depth the different perspectives towards security compliance between end-users and security experts/managers. Our case study's nature is descriptive and consists of multiple cases including two distinctive groups of end-users and security experts. Rather than aiming at interpreting the phenomena, descriptive case studies present the phenomena as they are in an objective fashion (Dubé and Paré 2003) and multiple-case design allows increased generalisability of the results (Yin 2009). Our case study design is described in Table 1 below.

			DIMENSIONS		
	Security Perspectives	**CASES**	Security factor 1	...	Security factor 5
UNIT	Security experts/managers	Security Expert/Manager 1–7	Differences in perspectives amongst security experts/managers and end-users regarding each dimension		
	End-users	End-user 1–16			
			OBSERVATIONS		

Table 1: Case study design

3.2 Context

To ensure the rigour of results derived from a descriptive case study method, there are criteria that need to be addressed in each stage of the research. The first criterion requires that the researchers to explicitly describe the context of the case study (Dubé and Paré 2003). Our study took place in Vietnam, a country in the South East Asia region, which is rapidly transforming into the world's IT sourcing hub. The overall information security landscape in Vietnam is still in its infancy. For instance, the recent Information and Communication Technology White book of the Vietnamese Ministry of Information and Communication reveals that in 2013 only 27.5 per cent of companies had published their information security policies while 21.7 per cent had implemented prescribed processes to handle information security matters (Vietnam-MIC. 2014). Funk and Garnaeva (2013) listed Vietnam in the top four countries in the world in terms of the highest risk of cyber threats.

3.3 Data collection

Informative cases are critical for a case study method given the small sample available for study. To conform to the complex nature of information security management and add value to the study outcome, our cases were drawn from a pool of participants from diverse industries and IT environments. Participants were recruited by sending invitations to personal contacts, as well as professional forums on social platforms such as Facebook and LinkedIn. The participants who agreed to take part in the research were screened to ensure that their companies had security policies and required security compliance at work (regardless of whether they had published IT policies according to the ICT White Book. Sixteen end-users and seven security experts and managers across a range of demographics took part in the

interviews. The profiles of the participants are summarised in Table 2. All 23 semi-structured interviews took one hour on average and were conducted in Vietnamese or English, dependent on the native-speaking background of the participant and were audio recorded.

End-user (U) Security Manager/Expert (E)	**Occupation**	**Industry**
U1–6	Counter teller	Banking
U7–8	Accountant	
U9–12	University lecturers	Education
U13–14	Admin staff	
U15–16	Marketing executive	Oil distribution
E1	IT Auditor/Consultant	Financial
E2	IT manager	IT services
E3	Security Consultant	Banking
E4	Security Officer	IT services
E5	Deputy IT director	Banking
E6	Data Security Manager	Engineering
E7	IT Director	Education

Table 2: Profiles of interviewees

3.4 Data analysis

NVivo 10 was used to analyse interview transcripts by following Yin's (2009) procedures, which include conducting within and cross case analysis in order to detect matching patterns to the predefined factors. The pre-determined five factors covered important components of data analysis, in which the interviewed data was classified to match with each identified factor description from prior literature and theories (Strauss and Corbin 1998). The five factors were then compared and discussed with coded data. To ensure reliability, a brief research report of the key findings was sent to the interviewees who were asked for their feedback, as well as verifying the coding with an IT expert who has more than 15 years of teaching IT disciplines.

4 Findings of the Study

4.1 Factor 1: Security risk evaluation

Security risk evaluation refers to the assessment of risk likelihood and severity. The security experts and end-users in our study held different perspectives about the significance of security risk evaluation. The majority of interviewed end-users reported that evaluating security risks consumed too much of their effort and time, as well as requiring skills that they did not have to perform the activity.

> *"I can click on the warning message to cancel or run the application, but thinking about what security risks might happen if I run it would be too much to handle." (U3, Counter teller)*

> *"It does not matter to me much as I don't have enough expertise and knowledge to assess the effectiveness of security tasks and the risks." (U13, University admin staff)*

End-users explained their focus on the severity of security risks, which had direct and immediate impacts on their jobs. Risks that affected the whole department or organisation were not obvious to these end-users. The security experts also shared this view such as E1 (IT Auditor) and E2 (IT manager) who contended that only high-level executives had the ability to assess organisational risks and transform them into strategic and tactical directives. Some security experts only expected employees to understand and comply with prescribed security procedures. E2 (IT manager) reasoned that not many regular end-users would care about security risks that affected the company's interests (e.g. reputation damage) because the impact of those high level threats were not relevant to their job. As a result, improving the

relevance of the risk communication was suggested to be important in designing information security training:

> *"The problem is like this, when you are the end-user and someone said: 'If you don't comply with information security then it will risk the reputation of the company.' Who cares? 'In the worst case I'd just quit the company, not my business.' That's how most of them would think like." (E2, IT Manager)*

Both the interviewed experts and end-users agreed that communication of risks should explain clearly the impact on the target audience's daily tasks. While the experts suggested using real life scenarios in security training sessions, the end-users agreed that they determined the risk's likelihood according to experience of real incidents. In addition, both groups agreed that frequent reminders were necessary and useful for developing a risk aware climate and improving security compliance.

The interviewed end-users also wanted to understand how implemented measures could prevent security threats, and suggested that having such knowledge would improve their risk evaluation. However, none of the interviewed experts mentioned explaining to the end-users the effectiveness of security measures.

Albrechtsen and Hovden (2009) discussed that security managers may focus more on the risk's likelihood while end-users reported paying more attention to the consequences of non-compliance. We found evidence that supported the different perceptions of security risks. The interviewed experts explained the opinions differed as a result of varied levels of perceived ownership of tasks in terms of their capacity to complete assigned tasks. This explanation supported findings from Adams and Blandford (2005) and Posey et al. (2014) that there would be discrepancies in the security experts and end-users' ownership of the security compliance activities, as well as their perceptions of the severity and likelihood of security threats.

4.2 Factor 2: Cost of security compliance

Both groups of participants agreed that compliance cost is inevitable and may not be avoided. A majority of the experts agreed that the only way to reduce response cost was to collaborate closely with department heads and incorporating their feedback when designing new security measures and procedures:

> *"There is no way that information security is comfortable, it is simply a trade-off of being secure and other things." (E2, IT Manager)*

> *"IT can control what people can do with IT resources, but if IT control starts to affect productivity then IT should open whatever the users need to do. IT should not be limiting the productivity. If IT needs to do something, it is business policy, not IT intention to do that for their own benefits." (E7, IT Director)*

Likewise, the end-users acknowledged that the cost of compliance was in terms of consumed time, even when security tasks were automated (e.g. auto updates and backup) and IT assistance was available. Realisation of response cost was also found to be associated with low perception of risks:

> *"For me as a user I understand that security compliance is only complying with organisation's requirements. However, I do not see the problem–why I need to do that. For the users, I find it wastes too much time." (U9, University lecturer)*

> *"Checking laptop hardware and security audit could take half a day. It is annoying and it is really a burden for us. (U15, Marketing executive)*

> *"The security task is time consuming. Some require just a couple of minutes of time while others virtually take away my time. Forgetting to change the password after the expiration date, teller is unable to log in the computer hence acquiring the assistance from IT to unlock the account. Due to the traffic of the bank, too crowded and sometimes multitasks, I could not change password immediately. (U3, Counter teller)*

The other interviewed users explained they would comply with security requirements regardless of the cost since compliance was required as a part of their job. This is in contrast to Posey et al. (2014)'s findings that the experts underestimated how much their end-users perceived compliance cost as an issue. The interviewed experts appeared to be more sympathetic to the end-users' challenges of achieving work productivity bound by security constraints. However, the shared perceptions of compliance cost as a contributing factor to compliance emphasised its inevitable nature and suggested that its effects could only be reduced by other factors but not eliminated.

4.3 Security compliance evaluation

Security compliance evaluation in our study refers to the weighting of rewards and sanctions for compliance versus non-compliance. We found discrepancies in how the interviewed experts and end-users perceived these rewards and sanctions. For instance, most end-users agreed that they would appreciate rewards such as recognitions or certificates as a result of performing compliant behaviour:

> *"We need some announcements about what we did. Maybe the IT department, the General Director, or department head can send out an announcement or letter of appreciation to acknowledge individuals who have done well in security. So that we can feel pride and we keep doing that." (U15, Marketing executive)*

> *"But in short term, there should be a clear "award – punishment", gradually, it will become self-consciousness. In the long term, we will aim for the improvement in each individual's consciousness as if we require that from the beginning, that would be very difficult." (U7, Bank accountant)*

On the contrary, only two experts recommended the use of rewards to encourage compliance, whereas the rest argued against it. Experts who objected to the use of rewards claimed that compliance was a part of the job's duties, which would be expected by default rather than a voluntary choice that required stimulus. Second, expert E6 (Data security manager) and E7 (Branch manager) expanded that they would avoid making information security compliance a competition with a reward system, as that would overly motivate employees to take excessive security protections and could interfere with work productivity.

> *"It is a commitment when you work somewhere and make sure that nothing… happen at the company you work for. If you ask for a reward for doing security, you are in the wrong mindset. The mindset is if you work somewhere, you are responsible and you should be compliant with any security requirements and use common sense to make sure that nobody steals your information. If you want a reward for that, I think it is wrong" and …*

> *"The reward also has a counter effect. When people are rewarded for their security effort, they would want to do more and more secure IT. Then it would reach a level where too much security and you can't work anymore. Or they try to secure many things, they may make mistakes and they may not work because they are not expert" (E7, IT director)*

In fact, most of the experts believed that the only reward for compliance was being able to avoid punishments and liability when a security breach occurs. Furthermore, E4 (Security officer) justified the reward of employees' compliance as mutually linked with the organisation's interests:

> *"All benefits of compliance should be explained as belonging to the company. The reason is that when the company receives the benefits, which would be shared with the employees. For example, the company could be trusted more by our clients, and they would give us more projects. The company's revenue would subsequently increase, and so would the bonus of the employees, if that is considered their personal gain." (E4, Security officer)*

Regarding the use of sanctions, most of our interviewed end-users acknowledged that their workplace did not implement any sanction schemes for non-compliance. On the one hand, one end-user who worked in the banking sector supported raising awareness of sanctions as he was concerned over financial risks that could result in serious consequences and should therefore be prevented. On the other hand, we found that all experts rejected using punishments for promoting compliance. However, respondents agreed that sanctions discouraged non-compliance. One expert explained that sanctions were more suitable to punish employees' security breaches and not suitable for proactively minimising security mistakes. Another expert (E3, Security consultant) reasoned that white-collar workers would perceive sanction measures as a personal threat, which may result in even more resistance:

> *"I always told my clients to never resort to sanctions. No matter how they look at it, the information security incidents that occurred are already in the past. The primary purpose of the security programs is to prevent incidents from happening, not to find ways to deal with things that already happened." (E3, Security consultant)*

Unlike Posey et al.'s (2014) finding that end-users thought more about intrinsic rewards while experts focused on extrinsic ones, we found that both of our interviewed groups recognised extrinsic rewards such as recognition and maintaining professional image as effective in motivating compliance. A potential explanation could be that information security has not yet been integrated into the organisational culture in our case studies, so compliance was still heavily dependent on the use of extrinsic incentives. In addition, our results reflected Albrechtsen and Hovden's (2009) findings that experts avoided imposing sanctions because they did not consider their role to be policemen or janitors.

4.4 Security self-efficacy

The possession of security knowledge and skills is essential to increase one's ability to perform required security tasks. Posey et al.'s (2014) study also reports that security experts were concerned about end-users' lack of security knowledge and considered knowledge and skill shortage as a major threat to security programs.

In our cases, most end-users perceived security compliance as simple and straightforward. End-users explained security compliance as following routines, such as changing passwords, locking computers, or not sharing computer accounts:

> *"The security procedures are quite easy to follow. As long as I just follow instructions and not touch on the IT parts or don't make mistake on the IT things." (U15, Marketing executive)*

All interviewed end-users reported that they were not required to perform any complex security tasks that needed special training. Some end-users admitted that they did not know what skills they were lacking until they were asked to do complex security tasks, such as verifying potential spoofing attacks in email or malicious websites. Most of them argued that security knowledge for regular end-users should be easy to understand and apply, whereas acquiring more advanced security skills ones should belong to IT specialists and not in the end-users' interest. Similar to the opinions of end-users, the interviewed experts only expected their end-users to follow step-by-step instructions as prescribed in the policies.

It was consistent between both interviewed groups that security skills were essential for security compliance, however, the challenge was how much security skill an end-user should acquire for effective compliance. The interviewed experts in our sample were concerned that highly skilful end-users may pose a deliberate threat, as they understand the information systems' vulnerabilities. Expert E7 (IT Director) was reluctant to educate end-users about the security infrastructure due to a fear that they could intentionally or by mistake breach the security systems. E7 (IT Director) also lacked trust in the end-users in regards to proper use of their security self-efficacy.

> *"Some end-users can set up own WI-FI network at work or home. There is no password, security protection on the WI-FI. Anyone can access their own network. People think they know but actually they don't." (E7, IT director)*

As a result, this raises questions about what types of security knowledge and system configurations should be included in training to ensure safe and secure information security systems in the organisation.

As highlighted in Albrechtsen and Hovden (2009), certain types of knowledge should be excluded from security training. However, excluding security specific information from training may also lead to end-users having low confidence in their security response efficacy.

4.5 Social influences

While the interviewed experts confirmed the important role of social norms in affecting individuals' attitudes and behaviours, they recommended not to rely on organisational norms to encourage compliance. Expert E6 (Data security manager) justified that employees with high information security awareness would be able to perform secure practices correctly even when the norms suggested alternative actions. Another expert E3 (Security consultant) was concerned that organisational norms may create strong subcultures that enact information security practices inconsistently among departments, especially in hierarchical organisations where autonomous work units were separate from top management executives' reach:

> *"Sometimes in Vietnamese firms the policy is announced from the higher level but enacted differently within the departments. Especially when departments can spend their allocated budget however… people in those departments would just care about what their direct supervisors do but not the distant corporate levels." (E1, IT Auditor)*

Moreover, the experts agreed that only managers with formal authority would be suitable for persuading compliance. In their expert roles, designated managers were required to possess leadership and communication skills, and especially proficiency in information security:

> *"We don't need influential opinion leaders in communicating information security. Because the nature of information security is being predominantly perceived as highly technical, so you need to have a technical person to gain people's trust. Then those people would listen to what that person says or trains them." (E3, Security consultant)*

Nevertheless, some interviewed end-users acknowledged that they usually sought assistance regarding information security matters from nearby colleagues rather than from the Information Technology (IT) department. A team's common practices, access convenience and response timeliness were reported as the main reasons for choosing to request information from a colleague rather than the IT staff. As team members operated on the same systems and handled similar security tasks, they formed local practices that all members followed. When dealing with unfamiliar security incidents, the end-users found it too time consuming and inconvenient to seek advice through formal channels, such as IT help desk or policies. Both University admin staff (U13 and U14) further suggested having area-specific champions who were active in updating security initiatives in the organisation and informing other team members of new tasks was advantageous.

> *"Because sometimes, it is like, we also know that it is important but there are so many things to do, and then, sometimes they (i.e. IT staff) are not very available, so the more people know about that, the better. Especially the one who is close to you, so you could come and see that person for security advice" (U13 and U14, University admin staff)*

5 Discussion

Overall the results of this study show an interesting conundrum for IT security practice. On the one hand managers are mostly interested in compliance: passive and procedural. They also have concerns with end-users becoming too qualified and representing a danger to the system.

As such their actions to enhance security are aimed at defining systems that limit expertise and decrease self-efficacy and skill development. As a method of illustrating this dilemma, Figure 1 depicts Ryan and Deci's self-determination continuum, which we believe highlights the gap between experts' views of compliance and end-users' views. The experts are applying external regulation; extrinsic motivations and focusing on compliance by way of externally applied rewards and punishments.

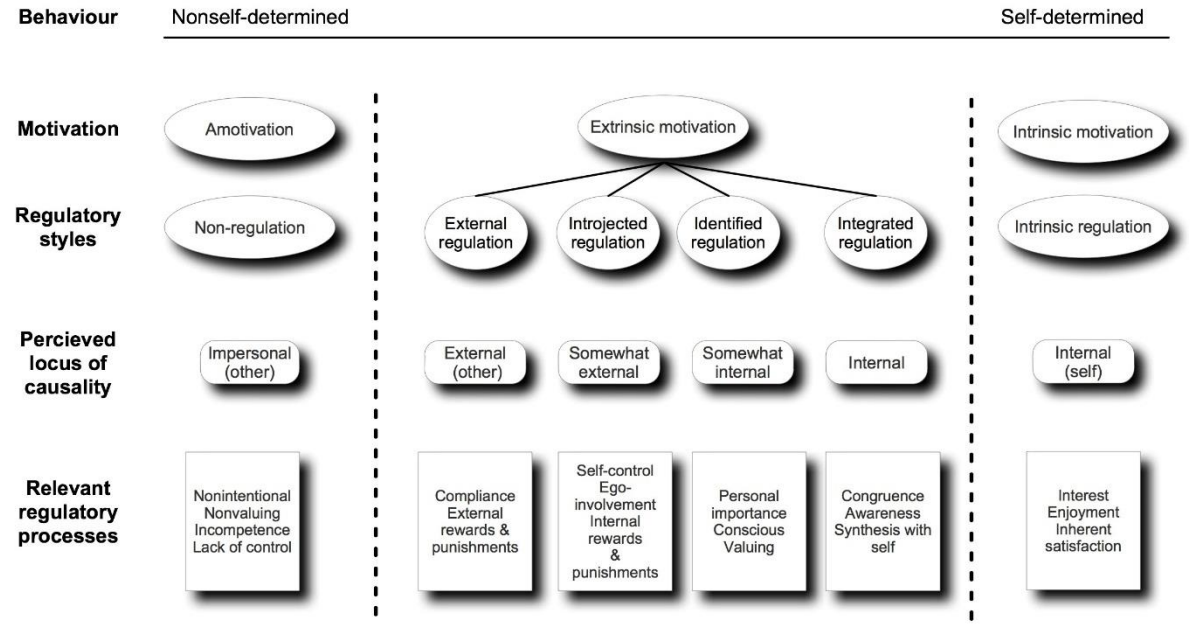

Figure 1: Self-determination theory (adapted from Ryan and Deci (2000))

On the other hand, the end-users are seeking to be self-determined; relying on intrinsic motivation and being engaged in IT security for interest, enjoyment and inherent satisfaction. They want to be active participants in developing skills that enable and empower them, not passive receivers of procedural information. The challenge for those managing IT security is to design a human system that allows for self-determination in compliance without increasing the risk to the organisation.

5.1 Improving risk communications between information security stakeholders

To enhance the likelihood that end-users will internalise security requirements, the regulatory processes need to shift from mere compliance (other directed) towards interest, enjoyment and inherent satisfaction (self-directed). Security managers need to tailor risk communication to emphasise on the consequences of the risks on daily operations rather than merely their likelihood, thereby increasing congruence and awareness of consequences. Outcomes of security breaches should be directly connected to the end-users' daily work: increasing personal importance. In addition, the effectiveness of the security controls needs to be clearly explained to end-users since perceived response efficacy was found to reduce compliance cost significantly (Dang-Pham and Pittayachawan 2015). We emphasise that educating the end-users about the security measures' effectiveness needs more attention from security practitioners. This will increase the conscious valuing of the IT system and improve the chances that the demands of IT security will be accepted, synthesised and internalised.

Communication of security issues can come from departmental security champions. Trained security champions are end-users who possess domain-specific security knowledge and can provide timely and accessible assistance to other users within a department. Prior studies have found the availability of information security resources has a positive impact on security compliance (Chan et al. 2005, Goo et al. 2014, Pham et al. 2015). While many organisations

cannot afford running frequent training programs and sending reminders are not effective in improving end-users' compliance, a team of dedicated security champions on site compensates for drawbacks, such as minimal reminders and a lack of training. Self-determined people can and will help themselves if the need to do so is clear and evident and the resources are available to assist. As internal IT security principally involves people not doing things, or doing everyday things safely, large-scale resources at the end-user level are not usually necessary. Although, that assumes that the IT infrastructure is secure in the first place.

5.2 Implementing the right incentives

In moving people along the spectrum towards self-determination, the incentives and rewards need to become less externally applied and more intrinsic. However, as our results show, experts believe that the only motivators that 'work' for compliance are external and punitive rather than rewarding. They do not believe that end-users are, or can be, intrinsically motivated, although the results of this study contest that view. As external regulations, such as tangible rewards and strict sanctions can have mixed impacts on security behaviour (Siponen et al. 2014, Vance and Siponen 2012) and only produce short-term effects resulting from poor-quality motivation (Stone et al. 2008), other forms of incentives should be employed. For example, formal recognition of security skills development can intrinsically motivate end-users to maintain their efficacy and practice recommended security tasks. Incentives for compliance should not promote over-protecting security activities but get the end-users interested and engaged with security practice on a regular basis. Such incentives should make the end-users find security skills and practices are essential work skills, not just simply following prescribed steps in the security policies.

5.3 Security training to provide value-added security skills

In order to assist the transition to self-determined and self-motivated end-users, consideration of the various types of regulatory processes is necessary. Using an externally derived, punitive system will not help people internalise the requirements and adopt them as a sustainable form of behaviour. As Figure 1 illustrates, the gap between mere compliance and self-motivation is a large one. The intervening steps incrementally increase 'self' control and decrease the locus of 'other' when it comes to motivational stimuli (i.e., causality). In order to foster the required shifts, security training should provide adequate skills to end-users without encouraging risky security behaviour due to over confidence in their capability. Management may just provide end-users with adequate skills to follow prescribed security policies; however, end-users want to see value in the acquisition of security skills beyond simple policy and process compliance. Security training could clearly communicate security objectives and the significance of security protection to individual's job and the whole organisation. Thereby, focusing on why it is important and increasing the sense of value that compliance contributes to the individual's daily activities. Similarly, security skills should be portrayed as critical to one's competence development and therefore seen as something desirable, as well as something that increases one's enjoyment and job satisfaction; rather than an onerous distraction from the primary role at work. In addition, employees should be aware that higher security skills may go with higher responsibilities and they can significantly contribute to the success of overall security programs in the organisation. End-users should not be treated as a potential threat, which often results in cautious approach to security training (Albrechtsen and Hovden 2009). Instead, they can be self-motivated allies in protecting the organisation in an insecure business environment.

6 Conclusion

Our study employed a multi-case approach and described the perspectives of information security experts/managers and end-users on the impact of risk evaluation, rewards and sanctions, security self-efficacy and social influences on individuals' security compliance. Distinct sets of beliefs were found between the two groups, except both groups agreed on the inevitable nature of compliance cost. Several practical lessons learned could be drawn from the findings. Given that there is a gap between expert and managers' views of security and end-users' views, this study highlights that establishing compliance may need to take into account

the different perspectives of end-users and experts or managers. Firstly, risk communication and a reward system should be implemented to promote risk-aware culture and recognition of end-users' security expertise that empowers and enables intrinsic self-regulation. Secondly, security training needs to balance between providing necessary skills and discouraging over-confident risk taking behaviour while still permitting the development of competences that lead to satisfaction with the role. In addition, our findings clearly explained the five theoretical constructs from protection motivation theory, theory of planned behaviour and general deterrence theory in the context of behavioural security compliance. Finally, this study contributes empirical findings in a non-Western context to the current body of knowledge in the information security domain, although it is feasible that these issues exist in Western IT security contexts as well.

References

Adams, A. & Blandford, A. (2005) "Bridging the Gap between Organizational and User Perspectives of Security in the Clinical Domain", *International Journal of Human Computer Studies,* **63**(1-2):175–202 doi:10.1016/j.ijhcs.2005.04.022.

Ajzen, I. (1991) "Theory of Planned Behavior", *Organizational Behavior and Human Decision Processes,* **50**(2):179–211. doi:10.1016/0749-5978(91)90020-T.

Albrechtsen, E. & Hovden, J. (2009) "The Information Security Digital Divide between Information Security Managers and Users", *Computers & Security,* **28**(6):476–490 10.1016/j.cose.2009.01.003.

Ashforth, B. (1985) "Climate Formation: Issues and Extensions", *Academy of Management Review,* **10**(4):837–847

Bandura, A. (1977) "Self-Efficacy: Toward a Unifying Theory of Behavioral Change", *Psychological Review,* **84**(2):191–215 http://dx.doi.org/10.1037/0033-295X.84.2.191.

Becker, G. S. (1968) "Crime and Punishment: An Economic Approach", *Journal of Political Economy,* **76**(2):169

Brennan, L., Binney, W., Parker, L., Nguyen, D. & Aleti, T. (2014). *Theories and Their Uses in Social Marketing, Social Marketing and Behaviour Change: Models, Theory and Applications*. Cheltenham, Glos GL50 2JA, UK: Edward Elgar Publishing.

Bulgurcu, B., Cavusoglu, H. & Benbasat, I. (2010) "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness", *MIS Quarterly,* **34**(3):523-548

Chan, M., Woon, I. & Kankanhalli, A. (2005) "Perceptions of Information Security at the Workplace: Linking Information Security Climate to Compliant Behavior", *Journal of Information Privacy and Security,* **1**(3) doi: 10.1080/15536548.2005.10855772.

Cialdini, R. B. & Goldstein, N. J. (2004) "Social Influence: Compliance and Conformity", *Annual review of psychology*, 55:591–621 doi: 10.1146/annurev.psych.55.090902.142015.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hud, Q., Warkentin, M. & Baskerville, R. (2013) "Future Directions for Behavioral Information Security Research", *Computer & Security,* **32**:90-101 doi:10.1016/j.cose.2012.09.010.

D'arcy, J., Herath, T. & Shoss, M. K. (2014) "Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective", *Journal of Management Information Systems,* **31**(2):285-318 doi: 10.2753/MIS0742-1222310210.

Dang-Pham, D. & Pittayachawan, S. (2015) "Comparing Intention to Avoid Malware across Contexts in a Byod-Enabled Australian University: A Protection Motivation Theory Approach", *Computers & Security,* **48**:281–297 doi:10.1016/j.cose.2014.11.002.

Dang-Pham, D., Pittayachawan, S. & Bruno, V. *Investigating the Formation of Information Security Climate Perceptions with Social Network Analysis: A Research Proposal*. 19th Pacific Asia Conference on Information Systems (PACIS), 2015 Singapore.

Deci, E. L. & Ryan, R. M. (2000) "The "What" and "Why" of Goal Pursuits: Human Needs and the Self-Determination of Behavior", *Psychological Inquiry,* **11**:227-268

Dourish, P., Grinter, R. E., Flor, J. D. D. L. & Joseph, M. (2004) "Security in the Wild: User Strategies for Managing Security as an Everyday, Practical Problem", *Personal Ubiquitous Computing,* **8**:391-401 doi: 10.1007/s00779-004-0308-5.

Dubé, L. & Paré, G. (2003) "Rigor in Information Systems Positivist Case Research: Current Practices, Trends, and Recommendations", *MIS Quarterly,* **27**(4):597–635

Funk, C. & Garnaeva, M., (2013), *Kaspersky Security Bulletin 2013* [Online]: SecureList. Available: https://securelist.com/analysis/kaspersky-security-bulletin/58265/kaspersky-security-bulletin-2013-overall-statistics-for-2013/ [Accessed 10 May 2016].

Furnell, S. & Rajendran, A. (2012) "Understanding the Influences on Information Security Behaviour", *Computer Fraud & Security,* **2012**(3):12-15 doi: 10.1016/s1361-3723(12)70053-2.

Gagné, M. & Deci, E. L. (2005) "Self-Determination Theory and Work Motivation", *Journal of Organizational Behavior,* **26**:331-362

Goo, J., Yim, M. & Kim, D. (2014) "A Path to Successful Management of Employee Security Compliance: An Empirical Study of Information Security Climate", *IEEE Transactions on Professional Communication,* **57**(4):1–24

Guo, K. H. & Yuan, Y. (2012) "The Effects of Multilevel Sanctions on Information Security Violations: A Mediating Model", *Information & Management,* **49**:320-326

Herath, T. & Rao, H. R. (2009a) "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness", *Decision Support Systems,* **47**:154-165 doi:10.1016/j.dss.2009.02.005.

Herath, T. & Rao, H. R. (2009b) "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations", *European Journal of Information Systems,* **18**:106-125 doi:10.1057/ejis.2009.6.

Hu, Q., Xu, Z. C., Dinev, T. & Ling, H. (2011) "Does Deterrence Work in Reducing Information Security Policy Abuse by Employees?", C*ommunications of the ACM,* **54**(6):54-60

Ifinedo, P. (2011) "Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory", *Computers & Security,* **31**:83-95 doi:10.1016/j.cose.2011.10.007.

Johnston, A. C. & Warkentin, M. (2010) "Fear Appeals and Information Security Behaviors: An Empirical Study", *Management Information Systems Quarterly,* **34**(3):549-566

Kankanhalli, A., Teo, H.-H., Tan, B. C. Y. & Wei, K.-K. (2003) "An Integrative Study of Information Systems Security Effectiveness", *International Journal of Information Management,* **23**:139-154

Leach, J. (2003) "Improving User Security Behaviour", *Computers & Security,* **22**(8) doi:10.1016/j.cose.2011.10.007.

Leenders, R. T. a. J. (2002) "Modeling Social Influence through Network Autocorrelation: Constructing the Weight Matrix", *Social Networks,* **24**(1):21-47 doi:10.1016/S0378-8733(01)00049-1.

Li, H., Zhang, J. & Sarathy, R. (2010) "Understanding Compliance with Internet Use Policy from the Perspective of Rational Choice Theory", *Decision Support Systems,* **48**:635-645

Mouratidis, H., Jahankhani, H. & Nkhoma, M. Z. (2008) "Management Versus Security Specialists: An Empirical Study on Security Related Perceptions", *Information Management & Computer Security,* **16**(2):187–205

Padayachee, K. (2012) "Taxonomy of Compliant Information Security Behavior", *Computer & Security,* **31**:673-680 doi:10.1016/j.cose.2012.04.004.

Pahnila, S., Siponen, M. & Mahmood, A. (2007). Employees' Behavior Towards Is Security Policy Compliance. the 40th Hawaii International Conference on System Sciences.

Pham, C. H., El-Den, J. & Richardson, J. *Influence of Security Compliance Demands and Resources on Security Compliance-an Exploratory Study in Vietnam*. Pacific Asia Conference on Information Systems (PACIS 2015), 2015 Singapore.

Pham, C. H. & Nkhoma, M. (2015) "Security Compliance-New Insight from Goal Orientations and Self-Regulation Theory", *Journal of Systemics, Cybernetics and Informatics* (JSCI), 13(3):56-61

Pham, H.-C., El-Den, J. & Richardson, J. (2016) "Stress-Based Security Compliance Model-an Exploratory Study", *Journal of Information and Computer Security,* **24**(4)

Posey, C., Roberts, T. L., Lowry, P. B. & Hightower, R. T. (2014) "Bridging the Divide: A Qualitative Comparison of Information Security Thought Patterns between Information Security Professionals and Ordinary Organizational Insiders", *Information and Management,* **51**(5):551–567 doi:10.1016/j.im.2014.03.009.

Rhee, H.-S., Kim, C. & Ryu, Y. U. (2009) "Self-Efficacy in Information Security: Its Influence on End Users' Information Security Practice Behavior", *Computer & Security,* **28**:816-826

Rogers, R. W. (1975) "A Protection Motivation Theory of Fear Appeals and Attitude Change", *Journal of Psychology,* **91**(1):93-114 doi:10.1080/00223980.1975.9915803.

Ruighaver, A. B., Maynard, S. B. & Chan, M. (2007) "Organisational Security Culture: Extending the End-User Perspective", *Computer & Security,* **26**:56-62

Ryan, R. M. & Deci, E. L. (2000) "Self-Determination Theory and the Facilitation of Intrinsic Motivation, Social Development, and Well-Being", *American Psychologist,* **55**(1):68-78 doi:10.1016/j.cose.2006.10.008.

Siponen, M., Mahmood, M. A. & Pahnila, S. (2014) "Employee's Adherence to Information Security Policies: An Exploratory Field Study", *Information & Management,* **51**:217-224 doi:10.1016/j.im.2013.08.006.

Sommestad, T., Hallberg, J., Lundholm, K. & Bengtsson, J. (2014) "Variables Influencing Information Security Policy Compliance: A Systematic Review of Quantitative Studies", *Information Management & Computer Security,* **22**(1):42–75 http://dx.doi.org/10.1108/IMCS-08-2012-0045.

Stone, D. N., Deci, E. L. & Ryan, R. M. (2008) "Beyond Talk: Creating Autonomous Motivation through Self-Determination Theory", *Journal of General Management,* **34**(3):75–91

Strauss, A. & Corbin, J. (1998) *Basics of Qualitative Research,* Thousand Oaks, CA, Sage.

Vance, A. & Siponen, M. (2012) "Is Security Policy Violations: A Rational Choice Perspective", *Journal of Organizational and End User Computing,* **24**(1):21-41 doi: 10.4018/joeuc.2012010102.

Vance, A., Siponen, M. & Pahnila, S. (2012) "Motivating Is Security Compliance: Insights from Habit and Protection Motivation Theory", *Information & Management,* **49**:190-198 doi:10.1016/j.im.2012.04.002.

Vietnam-Mic, 2014, *Vietnam Information and Data on Information and Communication Technology Whitebook 2014* [Online], Hanoi, Vietnam. Available:

http://english.mic.gov.vn/Upload/Store/tintuc/vietnam/43/Sach-Trang-2014-final.pdf [Accessed 10 May 2016].

Warkentin, M. & Willison, R. (2009) "Behavioral and Policy Issues in Information Systems Security: The Insider Threat", *European Journal of Information Systems,* **18**(2):101–105

Yin, R. K. (2009) *Case Study Research: Design and Methods,* Thousand Oaks, CA, Sage.