COMPUTERS & SECURITY XXX (2012) 1–8

Available online at www.sciencedirect.com

SciVerse ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Taxonomy of compliant information security behavior

*Keshnee Padayachee**

University of South Africa, School of Computing, Unisa 0003, South Africa

ARTICLE INFO

Article history:
Received 4 February 2011
Received in revised form
19 March 2012
Accepted 14 April 2012

Keywords:
Access control
Compliance
Deterrence control
Behavior
Motivation

ABSTRACT

This paper aims at surveying the extrinsic and intrinsic motivations that influence the propensity toward compliant information security behavior. Information security behavior refers to a set of core information security activities that have to be adhered to by end-users to maintain information security as defined by information security policies. The intention is to classify the research done on compliant information security behavior from an end-user perspective and arrange it as a taxonomy predicated on Self-Determination Theory (SDT). In addition, the relative significance of factors that contribute to compliant information security behavior is evaluated on the basis of empirical studies. The taxonomy will be valuable in providing a comprehensive overview of the factors that influence compliant information security behavior and in identifying areas that require further research.

1. Introduction

Information security is a matter of growing disquiet in most organizations. According to the Global Security Survey conducted by Deloitte (2007), concern has shifted predominantly to the human element of information security. The survey found that 91% of participants are concerned about employee security weaknesses, and 79% of participants 'cite the human factor as the root cause for information security failures'. The insider threat is even more dangerous than external threats, as an insider may easily misuse the skills and knowledge gained through legitimate work duties for illegitimate gain (Willison and Siponen, 2009). From the various definitions formulated to characterize 'insider attacks' (see Schultz (2002)), it is clear that the term refers to any individual who works in an organization and uses the authority granted to him/her for illegitimate gain. According to Shaw et al. (1998), 'it is people who designed the systems, people who attack the systems, and understanding the psychology of computer criminals is crucial to protecting those systems'. It is a fundamental requirement for any information security intervention that it should increase an end-user's compliance intention and encourage him/her to obey and uphold information security policies. Compliant information security behavior refers to the set of core information security activities that have to be adhered to by end-users to maintain information security as defined by information security policies. The compliance mindset also subscribes to what might be called a deterrence theory of motivation, which employs mandates, procedural controls and threats of punishment to manage and motivate people (Herath and Rao, 2009b). The aim of this paper is to classify the various factors that motivate or negate compliant security behavior so as to alert organizations to the strategies that are most effective to this end. A secondary aim is to highlight areas that require further research.

An individual's motivation to comply may be considered an inherent characteristic and may be related to personality, habits and skills. The external environment could influence some of these factors, while others may be too innate to modify. In general, external environmental factors would be classified as extrinsic factors, while the innate traits that influence an individual to comply are typically classified as intrinsic factors. The extrinsic factors are related to the social climate and working

* Tel.: +27 124296460.
E-mail address: padayk@unisa.ac.za.

0167-4048/$ – see front matter © 2012 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2012.04.004

Please cite this article in press as: Padayachee K, Taxonomy of compliant information security behavior, Computers & Security (2012), doi:10.1016/j.cose.2012.04.004

conditions that prevail on an individual to comply. Aside from the non-technical measures, preventative software measures such as deterrent controls and monitoring may be of significance. According to D'Arcy and Hovav (2007), the success of security countermeasures (i.e. deterrence mechanisms) ultimately depends on the actions and awareness of end-users; managers should therefore understand the effect of these controls from the end-user's perspective. Such an understanding would allow a more realistic evaluation of the effect of security countermeasures on end-users' computing behavior. Consequently, information security systems should provide countermeasures that dissuade users from committing data abuse to ensure compliance. However, deterrence controls intend to deter individuals from non-compliance rather than to encourage compliance. These factors are given consideration in the derived taxonomy.

The current study aims to decode the behavioral element in the factors that influence compliance. Self-Determination Theory (SDT), proposed by Deci and Ryan (1985), hypothesizes about the nature of human motivation and is one of the most influential behavioral theories in psychology. The aforementioned authors also derived a taxonomy of human motivation based on their theory (Ryan and Deci, 2000). Their taxonomy serves as a foundation for the taxonomy presented in this article. It is applicable to this study as the taxonomy of human motivation is also concerned with extrinsic and intrinsic motivations for behavior. Deci and Ryan's theory has been applied in many instances of information systems research, for example, in usability research (see Wiklund-Engblom et al. (2009)), e-learning research (see Jovanovic et al. (2011)) and in studies concerned with the motivations behind technology adoption such as system adoption within open source software (see Li et al. (2011)). As this study seeks to understand the motivations behind compliance, it is apt to apply SDT to dichotomize the taxonomy. Although SDT is usually applied to education, its application to security compliance may also be pertinent, as the theory serves to understand how individuals can be motivated to comply. Similar to rationality advocated by Ryan and Deci (2000) in terms of learning, it is important for organizations to not only rely on the individual's motivation to comply. Organizations need to 'promote active and volitional (versus passive and controlling) forms of extrinsic motivation', which may be more successful toward ensuring compliance.

This paper attempts to categorize research outputs in the area of compliant security behavior and deterrent control into a taxonomy predicated on SDT. This theory was selected as it provides a basis for explaining human behavior. The rest of the paper is structured as follows: Section 2 elaborates on compliant security behavior in general. In Section 3 a taxonomy of factors that influence compliant behavior is contextualized, after which the implications for practice are addressed in Section 4. Section 5 concludes with possible future research opportunities.

2. Background to compliant security behavior

Herath and Rao (2009a, 2009b) considered both extrinsic and intrinsic motivators that may encourage compliant security behavior. They considered the impact of *penalties* (extrinsic), *social pressures* (extrinsic) and *perceived value or contribution* (intrinsic) in terms of security measures. Chan et al. (2006) considered comparable factors relating to compliant security behavior, namely *upper management practices*, *direct supervisory practices*, *co-worker socialization*, *perception of information social climate* and *self-efficacy*, as well as how these factors influence compliant behavior. The factors of *upper management* and *direct supervisory practices* focused on the corporate structure, while *co-worker socialization* and *perception of information social climate* related to how others perceive information security. Siponen et al. (2010) suggested that *normative beliefs*, *threat appraisal*, *self-efficacy*, *response efficacy*, *visibility* and *deterrents* were contributing factors to compliant behavior. These variables help to gage whether a user might contravene information system security, but they also explain why a user might have a propensity toward ignoring security measures (Workman et al., 2008).

The compliance mindset subscribes to what might be called a deterrence theory of motivation, which employs mandates, procedural controls and threats of punishment to manage and motivate people (Herath and Rao, 2009b). D'Arcy and Hovav (2009) studied the countermeasures that deter internal systems misuse and focused on four factors, namely awareness of security policies, monitoring, preventative software, and training. These four factors deter users from misuse and hence promote compliant security behavior. In general, deterrence is defined as the preventative effect that actual or threatened punishment has on potential offenders (Ball, 1955). Deterrence theory is based on *certainty of detection*, *severity of punishment* and the swiftness (i.e. *celerity of being detected*) of punishment, all of which are factors that affect an individual's decision about whether or not to commit a crime (Higgins et al., 2005). In an information systems security context, these may be visualized in terms of an employee's assessment of the consequences of a security threat and the probability of exposure to a substantial security threat (Herath and Rao, 2009b). These factors deter an individual from non-compliance. Deterrents could involve the threat of *certainty of detection* (Herath and Rao, 2009a, 2009b) through monitoring mechanisms or via usage control deterrents. The latter concept was explored by Padayachee (2009) and involved deterring users from non-compliance through the stipulation of obligations that the user has to fulfill and system conditions that deter the user from illicit actions.

According to D'Arcy and Herath (2011), the aforementioned theory that is moderated by certainty of detection, severity of punishment and the celerity of detection is known as the **classical deterrence theory**. An annex to this theory is the **contemporary deterrence theory**, which is based on informal sanctions such as *social disapproval* and *self-disapproval* and moral inhibition. It is proposed that *self-disapproval* (internalized norms such as embarrassment or shame), *social disapproval* (fear of informal sanctions from peers) and *internalization of legal norms* (moral commitment) may also be deterrents to crime (Grasmick and Bursik, 1990). The concept of *low self-control*, which is diametrically opposed to moral commitment, has been shown to be instrumental in understanding software piracy (George et al., 2004). Software piracy research has also revealed that *past deviant behavior* is a good predictor of future deviant behavior (George et al., 2004). A propensity for risk-taking behavior is a factor in computer crime that involves an

Please cite this article in press as: Padayachee K, Taxonomy of compliant information security behavior, Computers & Security (2012), doi:10.1016/j.cose.2012.04.004

individual's weighing of 'cost and benefit probabilities of a crime', and assessing the ease of committing the crime as well as the odds of being detected (Sherizen, 1990). These notions may be collectively considered as *opportunistic* behavior. Hence, the factors of *self-disapproval* and *social disapproval* may be considered as deterrents to non-compliance, while *past deviant behavior*, *low self-control* and *opportunistic* behavior should also be considered as factors that promote a maladaptive response to compliant security behavior.

Compliance is more than ensuring that end-users comply with the information security policy; it may also influence the way preventative software measures are designed. This highlights another, more significant, issue regarding security usability. According to Whitten and Tygar (1999) security software is usable if the individuals who are expected to use it:

- are reliably made aware of the security tasks they need to perform;
- are able to figure out how to successfully perform those tasks;
- do not make dangerous errors; and
- are sufficiently comfortable with the interface to continue using it.

However, other issues have to be considered with respect to security usability. End-user compliance is influenced by the user's perception of the effectiveness of preventative software measures (Workman et al., 2008). Perceptions relate to *response efficacy* (perceived benefits of the action) (Herath and Rao, 2009b; Pahnila et al., 2007; Siponen et al., 2010) and *response cost* (i.e. how costly the recommend response would be) (Herath and Rao, 2009b; Pahnila et al., 2007; Siponen et al., 2007). Hence, end-users have to perceive that their actions in taking a security precaution would be effective and that the time and effort required to do so would not incur a huge cost to them. According to Workman et al. (2008), *self-efficacy* and *locus of control* are intrinsic motivators that offer a useful framework to help explain why users may or may not take security precautions. *Self-efficacy* is developed through the ongoing acquisition of knowledge related to an information security countermeasure (Chan et al., 2006). According to Chan et al. (2006), individuals with *self-efficacy* believe that they have the ability to perform a behavior and are therefore motivated to perform that behavior. In terms of usability of a preventative software measure, this factor should be considered because it increases the propensity for compliance. An individual's *locus of control*, on the other hand, may explain why people assume the responsibility for information system security precautions or forego them – and leave the responsibility to others, such as information security specialists. The *locus of control* is a more interactive expression of the relationship between a person and his/her environment (Workman et al., 2008), and therefore the question is whether end-users consider preventative security measures to be within their locus of control.

To conclude, it is clear that compliance is a function of two factors: the individual's innate behavior *and* the influence of the external environment. The next section presents the taxonomy of the factors that have an impact on end-user compliance.

3. Derivation of the taxonomy of factors that influence compliance

Related taxonomies have been established before by different researchers. For example, the taxonomy by Predd et al. (2010) considers four dimensions to understand these risks: the organization, the individual, the system, and the environment with relation to the insider threat. The taxonomy derived in this paper, designated the Classification of Security Compliant Behavior predicated on Self-Determination Theory (**CSCB^{SDT}**), also covers those aspects – however, in more depth and relative to the behavioral aspect. Magklaras and Furnell (2001) developed a taxonomy for classifying the nature of IT insider misuse. This taxonomy classified the insider threat in terms of the factors that create it. Similar to the **CSCB^{SDT}**, the taxonomy for Insider Misuse Classification has a human-centric focus; however, it did not consider the motivational aspects. The **CSCB^{SDT}** taxonomy aims to identify the factors that may be related to each of the different types of motivation, based on prior empirical research.

The **CSCB^{SDT}** is based on the taxonomy of human motivation by Ryan and Deci (2000), which distinguishes the following types of motivation (Deci and Ryan, 1985):

- *Intrinsic motivation*: Refers to performing an activity because it is inherently interesting or enjoyable.
- *Extrinsic motivation*: Refers to performing an activity because it leads to a separable outcome.
- *Amotivation*: Refers to a 'state of lacking an intention to act and results from not valuing an activity or not feeling competent to carry out the activity'.

In the taxonomy derived by Ryan and Deci (2000), they relate *extrinsic motivation* to the following constructs:

- *External regulation*: Refers to an external demand such as a reward.
- *Introjection*: Refers to instances where a person performs an act in order to maintain self-esteem.
- *Identification*: Refers to a situation where a person has accepted extrinsic regulation as his/her own.
- *Integration*: Refers to when identified regulations have been fully assimilated into the self.

It is evident that each level is part of a continuum, and as one's motivations move from external regulation thorough to integration, the motivation becomes increasingly internalized. Internalization is the process of motivation, for behavior can range from amotivation to passive compliance to active personal commitment (Deci and Ryan, 1985). In other words, although an individual may initially be unmotivated to act, he/she may (through the process of extrinsic motivation) experience an activity to become increasingly innate, to the extent that the individual no longer requires the extrinsic motivation and is essentially self-motivated to act. According to Ryan and Deci (2000), research in learning contexts has shown that intrinsic motivation is most successful toward high-quality learning. However, intrinsic motivation can be engendered through extrinsic motivations and strategies that

Please cite this article in press as: Padayachee K, Taxonomy of compliant information security behavior, Computers & Security (2012), doi:10.1016/j.cose.2012.04.004

appear to be self-endorsed, as one cannot rely solely on intrinsic motivation.

The user's common sense and decision-making skills (Leach, 2003) may be considered as intrinsic motivation. In terms of intrinsic behaviors in security compliance, these relate to an individual's personality, skills (Alfawaz et al., 2010; Marcinkowski and Stanton, 2003) and good habits (Pahnila et al., 2007). To be more precise, in the taxonomy these aspects will be referred to as *competence* and *etiquette* respectively. A good habit, for example, could be to consistently update one's password (Pahnila et al., 2007). It is reasonable to assume that ensuring that end-users have the skills and knowledge to maintain security controls will affect their competency. Thus one is more likely to adopt and internalize a goal if one has the competence to achieve that goal (Ryan and Deci, 2000). The employee needs not only to be influenced by a conducive information security environment, but must also possess the skills to perform the required actions (Chan et al., 2006). Hence an individual's possession of appropriate job skills is a necessary requirement to fulfill policy stipulations (Marcinkowski and Stanton, 2003). Moreover, an individual's personality encompasses values or attitudes as well as an own standard of conduct (Leach, 2003). Values and attitudes include aspects such as *commitment*, *obedience* (Furnell and Thomson, 2009) and *self-disapproval* (D'Arcy and Herath, 2011). According to Predd et al. (2010), *ethical* values may constrain the conduct of an insider threat.

According to SDT, extrinsic motivation is regulated by four constructs, namely *external regulation*, *introjection*, *identification* and *integration*. *External regulation* ensures that behaviors are satisfied by applying an external demand that includes *deterrent controls* and *rewards*. Incentives such as *rewards* influence whether employees are inclined to follow the policies (Marcinkowski and Stanton, 2003). In terms of *introjection*, which refers to when people feel pressurized to perform actions merely to avoid anxiety or maintain their ego (Ryan and Deci, 2000), this may be associated with the *social climate* of an organization. *Social climate* relates to the general security culture, which includes behaviors demonstrated by senior management and colleagues (Leach, 2003). Such behavior, for instance upper management practices, direct supervisory practices and co-worker socialization (Chan et al., 2006), motivates an individual to comply.

The next two regulators of behavior, namely *identification* and *integration* appear to be intrinsic – however, there is still an external force that regulates the behavior despite the fact that *identification* and *integration* are more autonomous and self-determined. *Identification* occurs when an individual has identified with the personal importance of a behavior (Ryan and Deci, 2000). Inculcating the value of compliance could be accomplished through less rigid controls by creating *awareness* of security policies (D'Arcy, 2009), which relates to the knowledge (Alfawaz et al., 2010) of the values, policies, standards and procedures (Leach, 2003) concerning security. This may be achieved by facilitating conditions (Pahnila et al., 2007) that foster *awareness* (Furnell and Thomson, 2009; Marcinkowski and Stanton, 2003). *Organizational commitment* (Herath and Rao, 2009b) may be another factor in encouraging behavior motivated by *identification*. 'Although not always well understood, organizational culture shapes (and is shaped by) behavior, suggesting that it influences insider behavior's nature and appropriateness' (Predd et al., 2010). Protection Motivation Theory (PMT) has been used by several studies to survey compliant security behavior (Herath and Rao, 2009b; Pahnila et al., 2007; Siponen et al., 2010). PMT has evolved from the cognitive appraisal of two processes, *threat appraisal* and *coping appraisal*. The former refers to the extent to which an individual feels threatened, while the latter refers to whether a coping response will be effective in removing the threat (Herath and Rao, 2009b). Although most studies akin to Workman et al. (2008) would consider coping and threat appraisal to be intrinsic, SDT would consider these factors to be motivated by *integration*. Integration is the most autonomous form of extrinsic regulation (Ryan and Deci, 2000). It occurs through introspection and assimilating regulations with one's values and needs. Although the behavior is not entirely innate, it is most definitely more internalized. The ultimate aim of any organization should be to apply external regulators so that the resultant compliant security behavior becomes increasingly internalized.

The least desirable motivation for behavior is *amotivation*. An individual that is *amotivated* 'lacks the intentionality and sense of personal caution'. *Amotivation* may result from *incompetence* or devaluing an activity (Ryan and Deci, 2000). An individual may be unmotivated to comply because of *apathy*, *resistance* and *disobedience* (Furnell and Thomson, 2009) toward security measures. He/She may also be *opportunistic* and have *low self-control* (Siponen et al., 2010), thus a propensity toward risky behavior if there is possible gain. In addition, *past deviant behavior* is a good predictor of future deviant behavior (George et al., 2004). *Incompetence* may well result in an individual failing to recognize the value of security measures. Thus it is vital for organizations to empower staff with the knowledge and skills that motivate an individual to comply with security policies.

Fig. 1 below shows the taxonomy of the motivational factors associated with compliant security behavior. Aspects such as personality traits and cultural norms are relevant to motivation, however, these aspects were not considered in the taxonomy. These factors are orthogonal to the taxonomy and have little pragmatic significance for the intervention strategies of an organization. However, motivation by extrinsic regulation, which organizations can reasonably encourage, warrants a deeper analysis. The taxonomy presented provides a conceptual model for higher-order classification of extrinsic motivation. This class was further refined in order to provide organizations with pragmatic solutions to engender security compliant behavior.

The next enhancement of the taxonomy involved a closer examination of some the third-level ranks, that is – *deterrent controls*, *social climate*, *awareness*, *threat appraisal*, and *coping appraisal*. The various types of *deterrent controls* considered include *sanctions*, *monitoring*, *policies*, and *technological controls*. The *technological controls* involve mechanisms such as *usage control deterrents* (Padayachee, 2009) and *access controls* (Hunker and Probst, 2011). *Sanctions* are moderated by *certainty of detection*, *severity of punishment* and the *celerity of detection* of the crime (Higgins et al., 2005). The *social climate* class includes *peer behavior*, *management practices* and *social disapproval*, and may persuade an individual to maintain security controls so as to

Please cite this article in press as: Padayachee K, Taxonomy of compliant information security behavior, Computers & Security (2012), doi:10.1016/j.cose.2012.04.004

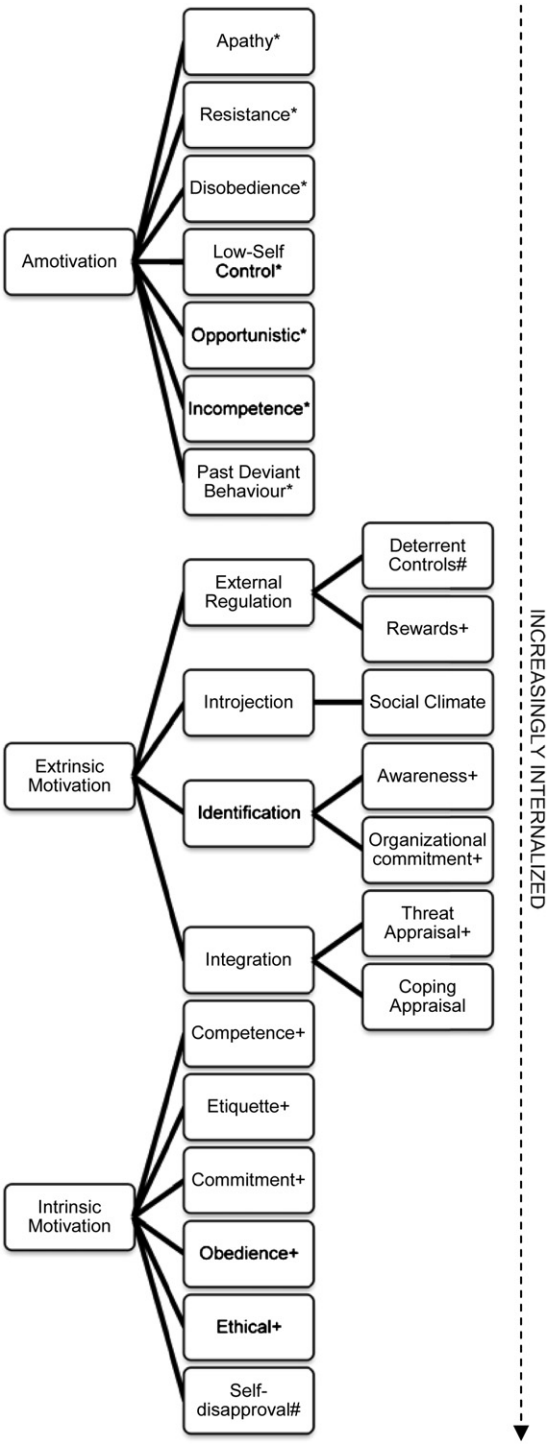

Fig. 1 – The Classification of Security Compliant Behavior predicated on the Self-Determination Theory ($CSCB^{SDT}$).

protect his/her self-esteem. The identification with security compliance was extended by including facilitating conditions that foster *awareness* such as *resource availability, training and visibility* (Siponen et al., 2010) and *information quality* (Pahnila et al., 2007). *Visibility* involves the use of information security campaigns, posters and advertisements to send a persuasive message about the importance of compliance (Siponen et al., 2010). *Resource availability* is about ensuring that resources such as security policies are readily accessible (Herath and Rao, 2009b). *Information quality* relates to providing information that is perceived to be valuable to the end-user. In general, facilitating conditions involve creating feasible conditions by providing appropriate tools and time to 'facilitate enactment of the behaviors prescribed by policy' (Marcinkowski and Stanton, 2003). *Threat appraisal* was further dichotomized to include the *perceived severity of a security breach* (Herath and Rao, 2009a) or the *perceived probability of a security breach* (Herath and Rao, 2009b). *Coping appraisal,* in turn, relates to *response efficacy* (perceived benefits of the action) (Herath and Rao, 2009b; Pahnila et al., 2007; Siponen et al., 2010), *self-efficacy* (Chan et al., 2006; Pahnila et al., 2007; Siponen et al., 2010), *response cost* (Herath and Rao, 2009b; Pahnila et al., 2007) and the individual's *locus of control* (Workman et al., 2008). However, even though *integration* regulation appears to be intrinsically motivated, behavior is motivated 'for its presumed instrumental value with respect to some outcome'. Since *self-efficacy* may be considered to be more on the intrinsic side of motivation, this factor is classified on the periphery of the intrinsic motivation taxonomy. The higher-classification of extrinsic motivation is shown in Fig. 2 below.

According to Vance et al. (2009), compliance with information security is an adaptive response, while non-compliance is a maladaptive response. In the taxonomy, there are aspects that increase the likelihood of an adaptive response and these are denoted with a plus sign (+). There are also aspects that decrease the likelihood of a maladaptive response and these are denoted with a minus sign (–). For example, a *reward* would be a mechanism that encourages compliance and therefore it elicits an adaptive response. A *sanction,* on the other hand, is an aspect that discourages non-compliance and therefore suppresses maladaptive responses. In the taxonomy, activities that encourage a maladaptive response toward compliance are denoted by an asterisk (*), for example *apathy*, *incompetence,* etc.

As part of the analysis, several extant empirical studies were investigated to highlight the factors that are significant for compliant security behavior versus those that are insignificant. Empirical studies conducted by Pahnila et al. (2007) and Herath and Roa (2009b) have shown that neither *sanctions* nor *rewards* have a significant impact on compliance. This conclusion concurs with SDT, as it was reported that external regulations are both controlling and alienating (Ryan and Deci, 2000). It seems that attitude and normative beliefs have a more significant effect on the intention to comply (Pahnila et al., 2007). Normative beliefs refer to one's perception of *peer behavior*. In a survey conducted by Pahnila et al. (2007), it was found that *information quality*, a *positive attitude, normative beliefs* and *habits* have a significant effect on an employee's intention to comply. This is also supported by a study conducted by Ifinedo (2011). In the survey conducted by Siponen et al. (2010), it was found that *threat appraisal*, *self-efficacy*, *normative beliefs* and *visibility* were significant with regard to the intention to comply, whereas *response efficacy* did not have a significant effect on the intention to comply. Alfawaz et al. (2010) found that knowledge (i.e. *awareness*) and skills (i.e. *competence*) are important, although by themselves they are not enough to ensure a positive contribution. Technology, social environment, regulation and self-interest all

Please cite this article in press as: Padayachee K, Taxonomy of compliant information security behavior, Computers & Security (2012), doi:10.1016/j.cose.2012.04.004

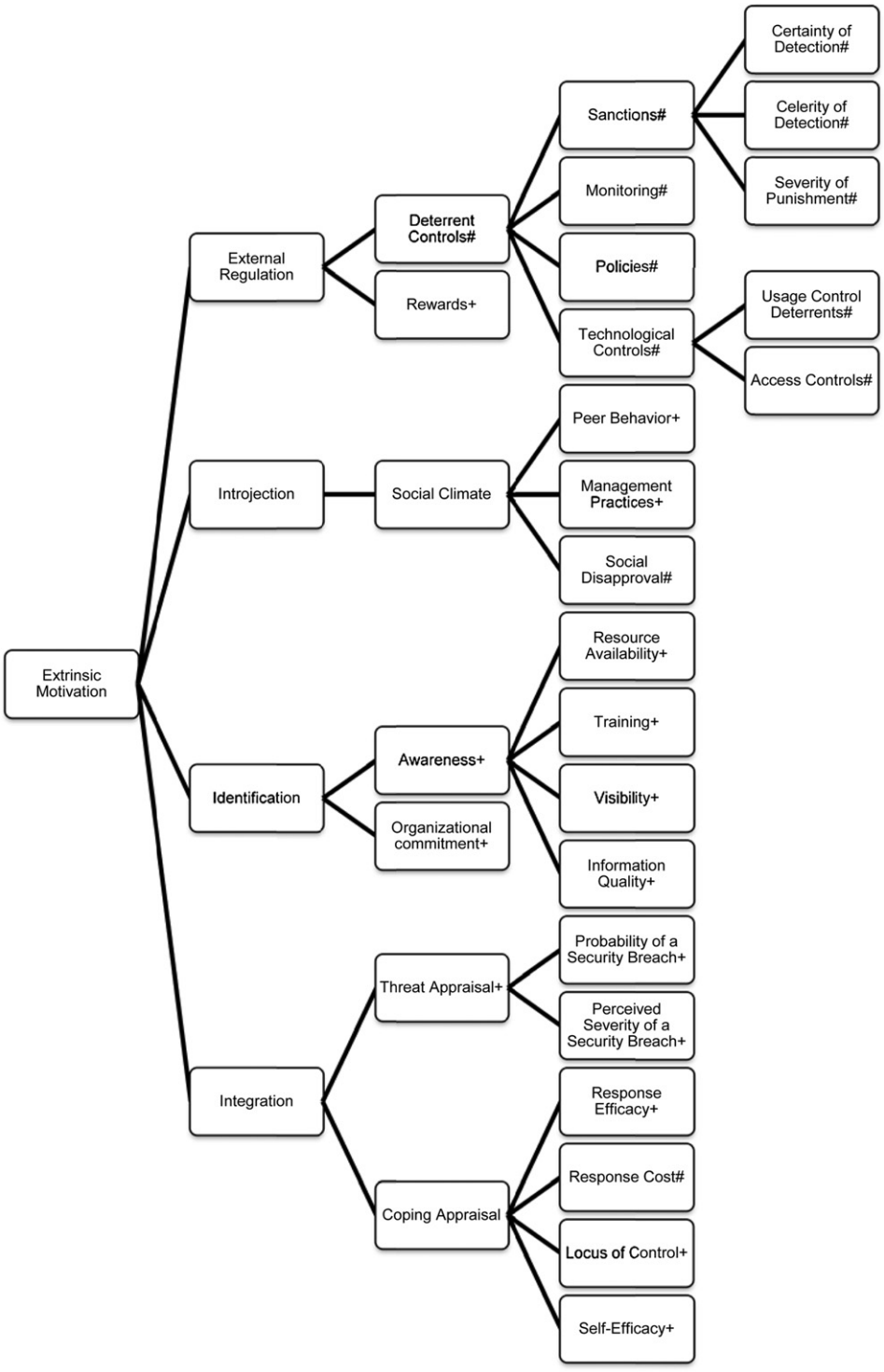

Fig. 2 – The higher-order classification of extrinsic motivation conceptualized from CSCB[SDT]

influence and contribute toward employees' security-related behavior. Herath and Rao (2009b) found that *perceived severity of breach* did not have an impact on compliance. In contrast, Workman et al. (2008) found that *perceived severity* was significant, as was the *probability of a security breach* factor. *Resource availability*, *self-efficacy* and *response efficacy* were found to play a significant role in encouraging compliance, whereas *response cost* was inconsequential. Ifinedo (2011), on the other hand, found that *response cost* had a positive impact on compliance intention behavior, which is contrary to expectations. Chan et al. (2006) found that the perception of *social climate* and peers' perception of the *social climate* were significant factors in compliant behavior. The link between *locus of control* and actual behavior was found to be inconsequential, although it 'might be acting as an antecedent to self-efficacy' (Workman et al., 2008).

Please cite this article in press as: Padayachee K, Taxonomy of compliant information security behavior, Computers & Security (2012), doi:10.1016/j.cose.2012.04.004

4. Implications for practice

The proposed taxonomy of compliant information security behavior could empower organizations to take cognizance of the factors that motivate an individual's behavior. It is clear that technological controls alone are insufficient and that both socio-organizational and sociological regulations are vital for encouraging compliant security behavior. Nevertheless, the position of SDT is that although intrinsic motivation is most sought after, it must initially be prompted by external regulators. The theory also explains the need for *relatedness*, which is about providing a sense of belonging and connectedness (Ryan and Deci, 2000). Hence, fostering *organizational commitment* is vital. The other issue is competence. Reportedly 'students are more likely to adopt and internalize a goal if they understand it and have the relevant skills to succeed at it' (Ryan and Deci, 2000). The same notion would apply to employees who would be more motivated to adopt a security goal if they had the skills and knowledge to succeed. The aim of every organization should be to propel an unmotivated individual to successively move along the continuum, from having external regulators, through to *identification* and *integration,* and finally to the state where compliant security behavior is so innate that there is little need for external enforcements. Hence it is important to understand the factors that engender intrinsic motivation, versus the factors that undermine it (Ryan and Deci, 2000).

In a study on the motivation behind open source adoption conducted by Li et al. (2011), it was stated that the developers involved should design their products with the end-users in mind, as contradictory expectations may prevent adoption. Similarly, with security compliant behavior, technological controls should be developed with the end-user in mind. This implies that the security software must be usable, as feelings of incompetence may be influenced by a system that is not user friendly and may descend into amotivated behavior. As indicated earlier, end-users need to be aware of the security tasks they have to perform and be able to successfully carry out those tasks (Whitten and Tygar, 1999). They first need to perceive security measures as valuable before they will be motivated to adopt the control. A well-designed security system will engender these sentiments. Thus, the relationship between security usability and compliance needs to be given due consideration in security systems.

Taxonomies such as the proposed one could serve as a useful basis for a threat prediction tool, as with the taxonomy defined for internal misuse by Magklaras and Furnell (2001). The **CSCB**^{SDT} taxonomy could be developed into a tool to detect insider threats by evaluating end-user motivations. By understanding whether an individual is intrinsically motivated, extrinsically motivated or precariously amotivated, organizations would be empowered to accurately identify those individuals who may become a future insider threat. This could assist personnel security officers in preventing, detecting and possibly counteracting such insider threats. Furthermore, this type of prediction tool may also assist in developing customized mitigation strategies based on differing motivations and to determine the granularity of access an individual could possibly be trusted with. For example, an individual that is amotivated should not be given access to highly classified information.

5. Conclusion

Industry surveys prove that a substantial portion of computer security incidents are due to the intentional actions of legitimate users. The consequences of such actions include negative publicity, a competitive disadvantage and the loss of consumer confidence (D'Arcy and Hovav, 2007). Hence, considering the factors that motivate compliant security behavior constitutes a significant step in preventing information security risks. The **CSCB**^{SDT} taxonomy was derived to this end to classify the various factors that contribute toward compliant security behavior. The taxonomy is by no means exhaustive. However, according to Siponen et al. (2007), the results of a study of this nature are relevant to both researchers and practitioners alike. It is useful to obtain empirically proven information on how organizations can improve their employees' adherence to information security policies and thus boost the information security of their organizations. The suggested taxonomy may be used to evaluate preventative measures for promoting compliant information security behavior. After all, the most important aspect of a security system is whether users comply with the security policies that are being implemented by the system.

D'Arcy and Herath (2011) reviewed the information security literature for the period 1990 to 2010 regarding extant empirical studies on deterrence theory. They established that findings are 'discrepant' and advocate that future research should explore the interactive influences of the certainty, severity and celerity dimensions of both formal and informal sanctions, as well as self-disapproval. It was found that there was a proliferation of research to consider coping appraisal and threat appraisal, whereas relatively little research had been conducted with regard to habits, skills and awareness, which – according to the taxonomy – may have a greater influence on engendering users' internalization of security compliant behavior. With regard to extrinsic regulators, research has been done on the social climate, software measures and facilitating conditions. It is, however, evident that compliant security behavior greatly influences the protection of information assets. Hence, there is a need for more evaluative studies regarding the intrinsic motivations toward security compliant behavior.

REFERENCES

Alfawaz S, Nelson K, Mohannak K. Information security culture: a behavior compliance conceptual framework. In: Proceedings of the 8th Australasian Information Security Conference (AISC); 2010. p. 47–55.

Ball JC. The deterrence concept in criminology and law. The Journal of Criminal Law, Criminology, and Police Science 1955; 46:347–54.

Chan M, Woon I, Kankanhalli A. Perceptions of information security in the workplace: linking information security

Please cite this article in press as: Padayachee K, Taxonomy of compliant information security behavior, Computers & Security (2012), doi:10.1016/j.cose.2012.04.004

climate to compliant behavior. Journal of Information Privacy and Security 2006;1:18–41.
D'Arcy D, Hovav A. Deterring internal information systems misuse. Communications of the ACM 2007;50:113–7.
D'Arcy D, Hovav A. Does one size fit all? Examining the differential effects of IS security countermeasures. Journal of Business Ethics 2009;89:57–71.
D'Arcy D, Herath T. A review and analysis of deterrence theory in the IS security literature: making sense of disparate findings. European Journal of Information Systems 2011;20:643–58.
Deci EL, Ryan RM. Intrinsic motivation and self-determination in human behavior. New York: Plenum; 1985.
Deloitte. Global security survey [cited 26 October 2010]. Available from:, http://www.deloitte.com/view/en_GX/global/industries/financial-services/5f5d5724a82fb110VgnVCM100000ba42f00aRCRD.htm; 2007.
Furnell S, Thomson K-L. From culture to disobedience: recognising the varying user acceptance of IT security. Computer Fraud & Security 2009;2009:5–10.
George E, Higgins GE, Makin DA. Self-Control, deviant peers and software piracy. Psychological Reports 2004;95:921–31.
Grasmick HG, Bursik RJ. Conscience, significant others, and rational choice: extending the deterrence model. Law & Society Review 1990;24:837–62.
Herath T, Rao HR. Encouraging information security behavior in organizations: role of penalties, pressures and perceived effectiveness. Decision Support Systems 2009a;47:154–65.
Herath T, Rao HR. Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems 2009b;18:106–25.
Higgins GE, Wilson AL, Fell BD. An application of deterrence theory to software piracy. Journal of Criminal Justice and Popular Culture 2005;12:166–84.
Hunker J, Probst CW. Insiders and insider threats – an overview of definitions and mitigation techniques. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA) 2011;2:4–27.
Ifinedo P. Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. Computers & Security 2011;31:83–95.
Jovanovic M, Starcevic D, Minovic M, Stavljanin V. Motivation and multimodal interaction in model-driven educational game design. IEEE Transactions on Systems, Man and Cybernetics Systems and Humans, Part A 2011;41:817–24.
Leach J. Improving user security behaviour. Computers & Security 2003;22:685–92.
Li Y, Chan-Hoo T, Heng X, Hock-Hai T. Open source software adoption: motivations of adopters and amotivations of non-adopters. SIGMIS Database 2011;42:76–94.
Magklaras GB, Furnell SM. Insider threat prediction tool: evaluating the probability of IT misuse. Computers & Security 2001;21:62–73.
Marcinkowski SJ, Stanton JM. Motivational aspects of information security policies. In: IEEE internal conference on systems, man and cybernetics; 2003. p. 2527–32.
Padayachee K. An aspect-oriented approach towards enhancing optimistic access control with usage control. Pretoria: University of Pretoria (Doctoral-Thesis) [cited 5 November 2010]; Available from: http://upetd.up.ac.za/thesis/available/etd-07262010-142652/; 2009.
Pahnila S, Siponen M, Mahmood A. Employee's behavior towards IS security policy compliance. In: Proceedings of the 40th Hawaii international conference on system sciences; 2007. p. 1561.
Predd J, Pfleeger SL, Hunker J, Bulford C. Insiders behaving badly. IEEE Security & Privacy 2010;6:66–70.
Ryan RM, Deci EL. Intrinsic and extrinsic motivations: classic definitions and new directions. Contemporary Educational Psychology 2000;25:54–67.
Schultz EE. A framework for understanding and predicting insider attacks. Computers & Security 2002;21:526–31.
Shaw E, Ruby K, Post J. The insider threat to information systems. Security Awareness Bulletin; 1998:2–98.
Sherizen S. Criminological concepts and research findings relevant for improving computer crime control. Computers & Security 1990;9:215–22.
Siponen M, Pahnila S, Mahmood A. Employees' adherence to information security policies: an empirical study. In: IFIP International Federation for Information Processing; 2007. p. 133–44.
Siponen M, Pahnila S, Mahmood MA. Compliance with information security policies: an empirical investigation. Computer 2010;43:64–71.
Vance A, Siponen M, Pahnila S. How personality and habit affect protection motivation. In: Workshop on Information Security and Privacy (WISP 2009); 2009. p. 14–21.
Whitten A, Tygar JD. Why Johnny can't encrypt: a usability evaluation of PGP 5.0. In: Proceedings of the 8th USENIX security symposium; 1999. p. 14.
Wiklund-Engblom A, Hassenzahl M, Bengs A, Sperring S. What needs tell us about user experience. In: Gross T, Gulliksen J, Kotzé P, Oestreicher L, Palanque P, Prates R, et al., editors. Human-computer interaction – INTERACT 2009. Berlin/Heidelberg: Springer; 2009. p. 666–9.
Willison R, Siponen M. Overcoming the insider: reducing employee computer crime through situational crime prevention. Communications of the ACM 2009;52:133–7.
Workman M, Bommer WH, Straub D. Security lapses and the omission of information security measures: a threat control model and empirical test. Computers in Human Behavior 2008;24:2799–816.

Keshnee Padayachee obtained a BSC degree from the University of Durban-Westville (now known as the University of Kwazulu Natal) in 1995 and a BSC (Hons) Computer Science in 1996. This was followed in 2002 by an MSC in Information Technology from the same institution. She was employed by the ML Sultan Technikon in 1997 where she lectured in the Department of Computer Studies for 3 years. Since 2000, she has been employed by the University of South Africa as a lecturer in the School of Computing. During this time she has presented numerous conferences papers covering aspect-oriented programming and its relation to information security. She has also published a journal article on optimistic access control. She has since obtained her PhD (Computer Science) from the University of Pretoria in South Africa in 2010.

Please cite this article in press as: Padayachee K, Taxonomy of compliant information security behavior, Computers & Security (2012), doi:10.1016/j.cose.2012.04.004