Security compliance-New insight from Goal orientations and Self-regulation theory

Hiep Cong PHAM
School of Business Information Technology and Logistics, RMIT Vietnam University, HCMC, Vietnam

and

Mathews NKHOMA
School of Business Information Technology and Logistics, RMIT Vietnam University, HCMC, Vietnam

ABSTRACT

This paper explores how self-set security goal orientations and self-regulation theory can provide potential venues to motivate end-user sustained IS security compliance. Organisations have found that it is essential to motivate end-users to comply with information security measures and policies on a regular basis. The research aims to obtain an understanding of the relationship between individual IS security goal orientations, self-regulation process and IS security compliance. The outcome of the research will facilitate the establishment of a security training program and communication strategy to increase self-regulated IS security compliance from end-users.

Keywords: Security goal orientations, Self-regulation theory, Security compliance.

1. INTRODUCTION

The risks to an organization's sensitive information are constantly changing and the loss of sensitive information continues to be a very real concern. Organizations often implement a wide range of information security measures to ensure the security of their information and computer resources. One of security measures is to develop information security policies which provide guidelines and instructions that an end-user should be aware and comply with to reduce information security risks. Majority of organizational security problems are indirectly caused by employees who violate or neglect the information security polices of their organizations, thus end-user compliance choices are critical to the overall effectiveness of security programs (Warkentin et al. 2007). Furthermore, end-users' attitudes, positive or negative, towards information security policies can improve or detract from security compliance (Bulgurcu et al. 2010; Colwill 2009; Herath and Rao 2009b).

Due to the complex nature of information security risks, effectiveness of organizational information security programs requires regular self-regulated compliance and vigilance from employees. Identification of organizational and personal factors that motivate self-regulated and continued compliance is essential to any security training and communication programs.
This paper aims to explore how goal orientations in the self-regulation process can influence the effort to maintain security compliance. The remainder of this paper is organized in 5 sections. Section 2 provides an overview of current research in information security compliance. Section 3 explains self-regulation for security behavior maintenance. Sections 4 describes individual goal orientations and compliance self-regulation. Section 5 proposes future work to validate the proposed model.

2. OVERVIEW OF INFORMATION SYSTEM SECURITY COMPLIANCE

The main objective of information system (IS) security is to ensure confidentiality, integrity and availability of respective information and computer services for organizations (Dhillon and Backhouse 2001). IS security is essential to ensuring that organizational information assets are safely guarded from both technical and user-related risks.

Organizations and end-users play critical role in the effectiveness of IS security. Organizations should implement effective security controls, develop thorough security processes, and provide trainings to end-users. However, end-users are often the weakest link in the security program (Crossler et al. 2013). Research has showed that most security problems are more often resulted from end-users' negligence rather than by deliberate attacks (Chang and Ho 2006). Thus, an organization's approach to IS security should also focus on its end-users behavior, as the organization's security success or failure effectively depends on the things that its employees do or fail to do (Siponen et al. 2009).

Traditionally, IS security measures are designed to address security risks at four phases: deterrence, prevention, detection, and recovery (Warkentin and Willison 2009). IS security compliance research aims to improve effectiveness of the 'prevention' phase through motivating end-user compliance with security policies and measures.

IS security compliance research focuses in two broad preventive approaches. First approach emphasizes the use of rewards and sanctions for compliance and on-compliance respectively. In this approach the use of punitive penalties and/or rewards is employed to achieve the desired behaviors. General deterrence theory has been used as a theoretical basis for understanding why employees follow (or do not follow) an organization's IS security policies (Herath and Rao 2009a; Hu et al. 2011; Lee et al. 2004). However, perception of consequences and penalties for non-compliance has been found to have different impacts on IS security behavior. For example, Herath and Rao (2009b) and Kankanhalli et al. (2003) found fear of penalties for non-

compliance affected security compliance behavior. An employee would more likely to comply if the certainty and severity of penalties are clear. Other studies (Cox 2012; Dhillon and Mishra 2007; Hu et al. 2011) have reported insignificant influence of penalties and rewards on employee security conducts. Hu et al (2011) explained that the use of rewards and penalties can be practically difficult to apply and often non-existent in organisations, thus such constructs would not be affect the studied employees. Following this approach, organisations can communicate certainty and severity of penalties for rule-breaking behavior to prevent employees from misusing the information assets of their organizations.

The second preventive approach aims to increase understanding of the reasons behind compliance and non-compliance by studying human behavior in rule-following (Boss et al. 2009; Pahnila et al. 2007; Siponen et al. 2009; Warkentin and Willison 2009). This approach assumes that human nature is complex and consequently IS security compliance behavior can be influenced by other factors than just by fear of sanctions or desire for rewards. Thus behavioral theories such as protection motivation theory and rational choice theory can help understand factors that can influence security compliance.

Security risks are can cause damages to organizations such as destroying data, revealing confidential information, or wreaking computer systems (i.e. hardware and software). Such potential security consequences can create fear from the end-users. Protection motivation theory (Rogers 1975) has been employed to study end-user security compliance through fear appeal. Protection motivation theory explains that individuals can be motivated to take appropriate measures in response to a threat when the threat is clear and the coping measures are effective against the threat. Several studies (Herath and Rao 2009a; Ifinedo 2011; Vance et al. 2012) have explored fear appeal of security risks on security compliance. Studies on the use of fear appeal in security compliance have shown that the level of evoked fear due to calculated evident security risk and the perceived effectiveness of the measures to prevent non-compliant security behavior have an influence on the adoption of requisite organizational security processes (Ifinedo 2011; Vance et al. 2012).

However, users do not feel personally at risk, and the risk can be difficult to be judged accurately due to inherent risk complexity, or heuristic factors such as optimism bias which make people consider risks are more likely to happen to others rather than themselves (Schneier 2008; West 2008). Moreover, Brennan and Binney (2010) stated that externally motivated fear and threat communication have a short term motivating influence and are not self-sustaining.

Another approach to understand security compliance is drawn from the rational choice theory. Rational choice theory (Becker 1968) puts forward two premises for the consideration of an offence: (1) balancing of both costs and benefits of the offending and (2) the decision maker's perceived or subjective expectation of reward and cost. Security tasks are often regarded by the end-users as supportive tasks (secondary) to their main (primary) job tasks. Thus the extent of the efforts or demands on work time he/she is required to exercise would influence their security compliance. The burden of compliance with security tasks imposed on the end-users has been identified as one of the major factors leading to non-compliance (Furnell and Rajendran 2012a; Leach 2003; Vance and Siponen 2012).

3. SELF-REGULATION AND SUSTAINED SECURITY COMPLIANCE

Human motivations in rule-following behavior are often explained by two models: extrinsic and intrinsic motivation models (Tyler and Blader 2005). Extrinsic motivation focuses on the perceived consequences, such as reward or punishment of complying or breaking the rules. Intrinsic motivation explains one's following the rules because of their own desire to do so. In other words, intrinsic motivation of compliance results from one's interest in and enjoyment of the task itself, whereas extrinsic motivation of compliance results from the need to obtain outcomes external to the task, such as reward or penalty. Self-determination theory (SDT) explains how individuals' different motivations direct one's behavior over time (Deci and Ryan 1985). SDT distinguishes autonomous (intrinsic) and controlled (external) motivation. SDT argues that that intrinsic motivations and factors known to enhance intrinsic motivation (e.g., autonomy-supportive environments) lead to more sustained behavior change than external (controlled) motivations (Deci and Ryan 1985; Deci and Ryan 2000). Behavior that is not motivated intrinsically is not persistent (Obaldiston and Sheldon 2003). The importance of intrinsic motivation is particularly apparent with more difficult behaviors such as quitting smoking or doing regular exercises, or performing safe security practice.

In IS security compliance research, extrinsic factors such as organizational penalties or rewards for compliance, or fear of security threats have mainly been used to explain rule-following behaviors (Hu et al. 2011; Padayachee 2012; Tabernero and Hernández 2011; Vance and Siponen 2012). Achieving proper IS security behavior through extrinsic motivation such as rewards, penalties, or fear appeal is not ideal because, without strict monitoring, employees may find a way to subvert an unordinary security situation. Moreover, mostly short term behavior change can be achieved by external factors such as financial incentives or persuasive communication (Obaldiston and Sheldon 2003). The desired behavior will stop when the intervention is removed. For ongoing maintenance of behavior change, such intervention strategies are expensive and difficult to maintain (Green-Demers et al. 1997). Similarly, externally motivated fear and threat communication has a short term motivating influence and are not self-sustaining (Brennan and Binney 2010). Thomson and Niekerk (2012) found that lack of intrinsic motivation is a common obstacle to joint effort between management and employees working toward the same information security goals

It is ideal when the end-users would exercise safe security practice and actively develop general security knowledge with or without the existence of regular external motivation factors. Self-regulation in exercising IS security practice comes from its effectiveness in maintaining a new behavior over time in different contexts (Ridder and Wit 2006). Self-regulation has been defined as "the capacity to guide one's activities over time and across changing circumstances" (Kanfer 1990). Self-regulation is the individual's purposive self-adjustment(s) towards the achievement of a goal (Carver and Scheier 2011). Motivating self-regulation in end-user security compliance has an important implication to organizations. It is much more cost effective and effective to facilitate and intrinsically motivate end-users to self-regulate their own security practice in different contexts than constantly monitoring and enforcing security compliance.

Self-regulation comprises of four processes: self-monitoring, self-evaluation, self-reactions, and self-efficacy judgments (Kanfer 1990). Each of these processes is now explained with implications for security compliance.

Self-set goals and externally assigned goals are the core of self-regulation (Locke and Latham 1990; Locke and Latham 2002). Self-monitoring involves seeking and interpreting feedback on progress of attaining a task goal. Such feedback enables self-adjustment toward achieving a goal. End-users by performing self-monitoring of their security practice can consult with the IT department for proper security handling, seeking advice from supervisors for unfamiliar security risks.

Self-evaluation assesses progress toward achieving goals based on feedback. If progress is not sufficient, one may change current strategies or adapt to new process to ensure the chance of achieving a goal and improving performance. The outcome of self-evaluation process highly influences the effort, self-rated performance, adjusted self-set goals, and goal commitment that one performs (Cellar et al. 2011). Self-evaluation in security compliance can go in the forms of making suggestions to improve security practice in organizations, expressing the need for further training, and putting effort to ensure proper security practice followed.

Self-reactions are mainly affective in nature that display satisfaction and/or positive affect when a goal attainment or a faster progress toward a goal is achieved. Some individuals may feel dissatisfied and/or negative affect when failing to achieve a goal or a much slower progress toward goal achievement (Bandura and Locke 2003; Carver and Scheier 1990). Such reactions are important for task persistence as dissatisfied individuals would be more likely to discontinue the task (Kanfer 1990). Negative affective reactions are likely to disrupt self-regulation activities leading to less self-regulatory behavior and lower performance (Diefendorff and Lord 2008b). End-users can be dissatisfied with their own security practice or with the organization's security response efficacy, and may result in lacking self-regulation effort. It is important for the organizations to assess satisfaction level of end-users towards the overall security program and their own achievements so that suitable timely measures can be introduced to reduce negative affection.

Finally, self-efficacy, a key construct of social cognitive theory, can be defined as an individual's confidence about his or her ability to mobilize motivation, cognitive resources, and actions needed to successfully complete a specific task within a given context (Bandura 1997). Bandura (1997) indicated that self-efficacy is enhanced as goals are set, performance monitored, adjustments are made based on feedback, and goals attained. Self-efficacy has been recognized as a key factor to motivate security compliance (Johnston and Warkentin 2010; Rhee et al. 2009). However, with the light of self-regulation approach, other factors such as clear goals, monitored progress, and regular feedback are essential to enhance self-efficacy adjustment of the end-users, not simply providing training is sufficient.

The four-process self-regulation is important to maintain effective IS security compliance. However, sustaining security compliance self-regulation, especially when there is a considerable lag time that exists between the time of a security violation and the impact of the violation, or unclear self-evaluation outcome or goal attainment evaluation process, can be challenging. The following section will examine the nature of the individual self-set goals that can have different impacts to the self-regulation effort and offers insights on how organizations can improve security compliance through developing effective security training programs.

4. GOAL ORIENTATIONS AND SECURITY COMPLIANCE SELF-REGULATION

It is important to understand how individual IS security goals guide end-users' security behavior. Goal-oriented self-regulation model dictates that successful behavior maintenance relies on the long-term goals that people have adopted (Diefendorff and Lord 2008a). Organizations can mandate IS security policies and provide training to users, however, what self-set goals that the end-users establish for themselves may most influence their corresponding behaviors. External factors such as reward or penalty may not be evident immediately for an act of security compliance, thus the issue of behavioral maintenance is thus particularly important for security compliance. As a result, understanding the influence of end-user self-set goals to security behavior is essential to motivate security compliance.

According to goal orientation theory, individuals have goals they implicitly pursue while achieving performance outcomes (Dweck and Leggett 1998). The goals that individuals pursue can have different orientations which utilize different affective, cognitive, and behavioral patterns during task engagement and performance (Duda and Nicholls 1992; Dweck and Leggett 1998). Elliot and McGregor (2001) identified three goal orientations namely mastery-approach, performance-approach, and performance-avoidance that an individual may possess.

Mastery-approach aims to obtain self-competence when acquiring new skills and mastering new situations (Dweck and Leggett 1998). Performance-approach is concerned with demonstrating and validating one's competence with others. Finally, performance-avoidance demonstrates one's effort to avoid displaying incompetence to others; this orientation aims to avoid negative outcomes as the outcome (Elliot and Harackiewicz 1996).

The three forms of goal orientations can occur due to different focuses of security programs. For example, a security program that promotes security skill necessities as part of one's job can encourage end-users to learn and equip necessary new competence (i.e. mastery-approach). If rewards and recognitions are associated with demonstrating new skills and competence, one may want to demonstrate their security superiority to others (i.e. performance-approach). And if penalties and sanctions can be applied if one fails to attain the required skills or knowledge, one may employ performance-avoid technique to hide their incompetence to avoid negative outcomes such as poor performance evaluation or penalties.

Individuals high in mastery-approach and performance-approach goal orientations in task performance may employ adaptive self-regulatory processes by engaging in higher levels of cognitive process in their goal pursuits (Cellar et al. 2011; Porath and Bateman 2006; Radosevich et al. 2008). Cellar et al. (2011) find both mastery and performance-approach correlate positively with self-monitoring. Both approach-goal orientations score high on self-evaluation process of self-set

goals, effort, self-rating of performance, and goal commitment. Approach goal orientations would also influence positively with self-efficacy: the more mastery and performance focus, the higher perceived self-efficacy one has, though mastery would have a more impact than performance approach. Importantly, intrinsic motivation can be promoted through setting mastery-approach goals by fostering perceptions of challenging tasks, encouraging task involvement, and generating excitement in pursuing goals. Though mastery and performance approach goals may have different effect to intrinsic motivation. Performance-approach goals can undermine intrinsic motivation by projecting perceptions of threat of competition and failure which may lead to disrupting task involvement and increasing anxiety and evaluative pressure (Radosevich et al. 2008). However, Butler (1992) found the negative effects of performance-approach goals on intrinsic motivation should manifest only at low levels of perceived self-efficacy.

Security compliance can be considered as an enduring task that an end-user needs to self-regulate. Potentially, if end-users have either mastery or performance-approach goals they would be more likely to seek feedback, accepting challenging tasks, and especially be motivated intrinsically to fulfil compliance tasks. In all cases, self-efficacy is essential to maintain intrinsic motivation and effective self-regulation process.

On the contrary, individuals high in performance-avoidance can take self-protective processes (i.e. maladaptive responses) to ease negative evaluative perceptions rather than increasing on-task focus for being influenced by fear of failure or threat perception (Radosevich et al. 2008). Performance-avoidance can interfere with or prevent optimal task engagement. Individuals with high performance-avoidance level tend to view ability as fixed, negative feedback as threatening, and spending high effort in completing tasks as an indication of low ability. Therefore, individuals with high performance-avoidance are less likely to perform self-monitoring or self-evaluation in the self-regulation process.

End-users with performance-avoidance goals in security compliance would take challenging tasks as threatening, showing lacking skills as incompetence, or asking for advice as indication of low ability. These end-users may not try to improve their security skills, hide security incidents for fear of embarrassment or disciplinary actions.

Another important aspect of goal orientations in helping understanding behavior change is that goal orientations can be considered as an individual's traits rather than situational characteristics. These traits would be more consistent across time and situations (Cellar et al. 2011). Traits are more enduring than attitudes or intentions and are potentially more predictive of behaviors (Mowen et al. 2004). This aspect is especially important in a IS security domain where the users need to maintain persistent behavior across time and situations. Any initiatives from organizations to improve user compliance would benefit if they can be developed to align with the users' more enduring personal traits. Thus by understanding individuals' goal orientations in IS security compliance, organizations can develop more effective security strategies by taking into account of employees' enduring and long-term goal orientations.

5. CONCLUSION AND FUTURE RESEARCH

Successful behavior change requires that people are not only motivated and capable of initiating a change in their behavior, but also able to sustain that change over time. The paper has proposed a more focus on sourcing intrinsic motivation (enjoyment and interest) from self-set goal orientations to motivate self-regulation in security compliance than extrinsic motivation (external factors) such as punishment or reward. Security self-regulation involves ongoing personal efforts to actively monitor, evaluate and react to security risks which are essential to reduce human risks in information security programs. Specific self-set security goal orientations could be sources of intrinsic motivations which have influence to self-regulation effort and task performance and persistence. In particular, both mastery-approach and performance-approach orientation towards security tasks should lead to higher correlations with security self-regulation. Conversely the negative emotion associated with the performance-avoid goal would lead to negative relationships between this orientation and security self-regulation.

The paper contributes to the security compliance research by proposing that the effect of different goal orientations on the security self-regulation process could be the key for better security compliance. Organizations could develop security programs and provide trainings that promote competence-focused, interesting and challenging tasks. Additionally, providing supervisory feedback, encouraging error-taking, and avoiding public discipline of non-compliance are some other techniques to promote mastery-approach or at least performance-approach goals in security compliance.

A limitation of the study is lacking empirical data to support the correlations among security goal orientations, self-regulation, and the resulting security compliance in the end-users. The next stage of the study will be to develop scale measurements of the constructs proposed in this study and conduct large scale survey to quantitatively examine the impact level of security goal orientations on self-regulation process. This will enhance the generalization of the study's outcome.

9. REFERENCES

[1] Bandura, A. 1997. Self-Efficacy: The Exercise of Control. New York: Freeman.

[2] Bandura, A., and Locke, E. A. 2003. "Negative Self-Efficacy and Goal Effects Revisited", Journal of Applied Psychology (88), pp. 87–99.

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

[4] Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., and Boss, R. W. 2009. "If Someone Is Watching, I'll Do What I'm Asked: Mandatoriness, Control, and Information Security", European Journal of Information Systems (18), pp. 151-164.

[5] Brennan, L., and Binney, W. 2010. "Fear, Guilt and Shame Appeals in Social Marketing", Journal of Business Research (63:2), pp. 140-146.

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

[7] Butler, R. 1992. "What Young People Want to Know When: Effects of Mastery and Ability Goals on Interest in Different Kinds of Social Comparisons", Journal of Personality and

Social Psychology (62), pp. 934-943.
[8] Carver, C. S., and Scheier, M. F. 1990. "Origins and Functions of Positive and Negative Affect: A Control-Process View", Psychological Review (97), pp. 19–35.
[9] Carver, C. S., and Scheier, M. F. 2011. "Self-Regulation of Action and Affect", in Handbook of Self-Regulation, K.D. Vohs and R.F. Baumeister (eds.). New York: The Guildford Press, pp. 3-21.
[10] Cellar, D. F., Stuhlmacher, A. F., Young, S. K., Fisher, D. M., Adair, C. K., Haynes, S., Twichell, E., Arnold, K. A., Royer, K., Denning, B. L., and Riester, D. 2011. "Trait Goal Orientation, Self-Regulation, and Performance: A Meta-Analysis", Journal of Business Psychology (26), pp. 467-483.
[11] Chang, S. E., and Ho, C. B. 2006. "Organizational Factors to the Effectiveness of Implementing Information Security Management", Industrial Management & Data Systems (106:3), pp. 345-361.
[12] Colwill, C. 2009. "Human Factors in Information Security: The Insider Threat - Who Can You Trust These Days?", Information Security Technical Report (14), pp. 186-196.
[13] Cox, J. 2012. "Information Systems User Security: A Structured Model of the Knowing–Doing Gap", Computers in Human Behavior (28), pp. 1849-1858.
[14] Crossler, R. E., Johnston, A. C., Lowry, P. B., Hud, Q., Warkentin, M., and Baskerville, R. 2013. "Future Directions for Behavioral Information Security Research", Computer & Security (32), pp. 90-101.
[15] Deci, E. L., and Ryan, R. M. 1985. Intrinsic Motivation and Self-Determination in Human Behavior. New York: NY: Plenum Press.
[16] Deci, E. L., and Ryan, R. M. 2000. "The "What" and "Why" of Goal Pursuits: Human Needs and the Self-Determination of Behavior", Psychological Inquiry (11), pp. 227-268.
[17] Dhillon, G., and Backhouse, J. 2001. "Current Directions in Is Security Research: Towards Socio-Organizational Perspectives", Information Systems (11), pp. 127-153.
[18] Dhillon, G., and Mishra, S. 2007. "Information Systems Security Governance Research: A Behavioral Perspective", in: 2nd Annual Symposium on Information Assurance. New York State.
[19] Diefendorff, J. M., and Lord, R. G. 2008a. "Goal-Striving and Self-Regulation Processes", in Work Motivation: Past, Present, and Future, R. Kanfer, G. Chen and R.D. Pritchard (eds.). New York: Routledge, pp. 151–196.
[20] Diefendorff, J. M., and Lord, R. G. 2008b. "Goal-Striving and Self-Regulation Processes", in Work Motivation: Past, Present, and Future, R. Kanfer, G. Chen and R.D. Pritchard (eds.). New York: Routledge., pp. 151–196).
[21] Duda, J. L., and Nicholls, J. G. 1992. "Dimensions of Achievement Motivation in Schoolwork and Sport", Journal of Educational Psychology (84), pp. 290–299.
[22] Dweck, C. S., and Leggett, E. L. 1998. "A Social-Cognitive Approach to Motivation and Personality", Psychological Review (95), pp. 256–273.
[23] Elliot, A. J., and Harackiewicz, J. M. 1996. "Approach and Avoidance Achievement Goals and Intrinsic Motivation: A Mediational Analysis", Journal of Personality and Social Psychology (70), pp. 461–475.
[24] Elliot, A. J., and McGregor, H. A. 2001. "A 2 X 2 Achievement Goal Framework", Journal of Personality and Social Psychology (80:3), pp. 501-519.
[25] Furnell, S., and Rajendran, A. 2012a. "Understanding the Influences on Information Security Behaviour", Computer Fraud & Security (2012:3), pp. 12-15.
[26] Furnell, S., and Rajendran, A. 2012b. "Understanding the Influences on Information Security Behaviour", Computer Fraud & Security:Feature Issue).
[27] Green-Demers, Isabelle; Pelletier, L. G., and Menard, S. 1997. "The Impact of Behavioural Difficulty on the Salience of the Association between Self-Determined Motivation and Environmental Behaviours", Canadian Journal of Behavioural Science (29:3), pp. 157-166.
[28] Guo, K. H., and Yuan, Y. 2012. "The Effects of Multilevel Sanctions on Information Security Violations: A Mediating Model", Information & Management (49), pp. 320-326.
[29] Herath, T., and Rao, H. 2009a. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations", European Journal of Information Systems (18), pp. 106-125.
[30] Herath, T., and Rao, H. R. 2009b. "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness", Decision Support Systems (47), pp. 154-165.
[31] Hu, Q., Xu, Z. C., Dinev, T., and Ling, H. 2011. "Does Deterrence Work in Reducing Information Security Policy Abuse by Employees?" Communications of the ACM (54:6), pp. 54-60.
[32] 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), pp. 83-95.
[33] Johnston, A. C., and Warkentin, M. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study", Management Information Systems Quarterly (34:3), pp. 549-566.
[34] Kanfer, R. 1990. "Motivation Theory and Industrial and Organizational Psychology", in Handbook of Industrial and Organizational Psychology, M.D. Dunnette and L.M. Hough (eds.). Palo Alto, CA: Consulting Psychologists Press, pp. 75-170.
[35] Kankanhalli, A., Teo, H.-H., Tan, B. C. Y., and Wei, K.-K. 2003. "An Integrative Study of Information Systems Security Effectiveness", International Journal of Information Management (23), pp. 139-154.
[36] Leach, J. 2003. "Improving User Security Behaviour", Computers & Security (22:8).
[37] Lee, S. M., Lee, S.-G., and Yoo, S. 2004. "An Integrative Model of Computer Abuse Based on Social Control and General Deterrence Theories", Information & Management (41), pp. 707-718.
[38] Locke, E. A., and Latham, G. P. 1990. A Theory of Goal Setting and Task Performance. Englewood Cliffs: NJ: Prentice-Hall.
[39] Locke, E. A., and Latham, G. P. 2002. "Building a Practically Useful Theory of Goal Setting and Task Motivation - a 35-Year Odyssey", American Psychologist (57:9), pp. 705-717.
[40] Mowen, J. C., Harris, E. G., and Bone, S. A. 2004. "Personality Traits and Fear Response to Print Advertisements: Theory and an Empirical Study", Psychology & Marketing (21:11), pp. 927-943.
[41] Obaldiston, R., and Sheldon, K. M. 2003. "Promoting Internalized Motivation for Environmentally Responsible Behaviors: A Prospective Study of Environmental Goals", Journal of Environmental Psychology (23), pp. 349–357.
[42] Padayachee, K. 2012. "Taxonomy of Compliant Information Security Behavior", Computer & Security (31), pp. 673-680.
[43] Pahnila, S., Siponen, M., and Mahmood, A. 2007.

"Employees' Behavior Towards Is Security Policy Compliance", in: the 40th Hawaii International Conference on System Sciences.
[44] Porath, C. L., and Bateman, T. S. 2006. "Self-Regulation: From Goal Orientation to Job Performance", Journal of Applied Psychology (91:1), pp. 185-192.
[45] Radosevich, D. J., Radosevich, D. M., Riddle, M. R., and Hughes, P. A. 2008. "Goal Orientation as a Predictor of Cognitive Engagement, Performance, and Satisfaction", Journal of Academy of Business and Economics (8:3).
[46] Rhee, H.-S., Kim, C., and Ryu, Y. U. 2009. "Self-Efficacy in Information Security: Its Influence on End Users' Information Security Practice Behavior", Computers & Security (28:8), pp. 816-826.
[47] Ridder, D. T. D. d., and Wit, J. B. F. d. 2006. "Self-Regulation in Health Behavior: Concepts, Theories, and Central Issues", in Self-Regulation in Health Behavior. John Wiley & Sons Ltd.
[48] Rogers, R. W. 1975. "A Protection Motivation Theory of Fear Appeals and Attitude Change", Journal of Psychology (91:1), pp. 93-114.
[49] Schneier, B. 2008. "The Psychology of Security." Retrieved 20/7, 2013, from http://www.schneier.com/essay-155.html
[50] Siponen, M., Mahmood, M. A., and Pahnila, S. 2009. "Are Employees Putting Your Company at Risk by Not Following Information Security Policies?", COMMUNICATIONS OF THE ACM (52:12), pp. 145-147.
[51] Tabernero, C., and Hernández, B. 2011. "Self-Efficacy and Intrinsic Motivation Guiding Environmental Behavior", Environment and Behavior (43:5), pp. 658-675.
[52] Thomson, K., and Niekerk, J. v. 2012. "Combating Information Security Apathy by Encouraging Prosocial Organisational Behaviour", Information Management & Computer Security (20:1), pp. 39-46.
[53] Tyler, T. R., and Blader, S. L. 2005. "Can Businesses Effectively Regulate Employee Conduct? The Antecedents of Rule Following in Work Settings", Academy of Management Journal (8:6), pp. 1143-1158.
[54] Vance, A., and Siponen, M. 2012. "Is Security Policy Violations: A Rational Choice Perspective", Journal of Organizational and End User Computing (24:1), pp. 21-41.
[55] Vance, A., Siponen, M., and Pahnila, S. 2012. "Motivating Is Security Compliance: Insights from Habit and Protection Motivation Theory", Information & Management (49), pp. 190-198.
[56] Warkentin, M., Shropshire, J., and Johnson, A. 2007. "The It Security Adoption Conundrum: An Initial Step Towards Validation of Applicable Measures", Proceedings of the 13th Americas Conference on Information Systems, Keystone, CO.
[57] Warkentin, M., and Willison, R. 2009. "Behavioral and Policy Issues in Information Systems Security: The Insider Threat", European Journal of Information Systems (18), pp. 101-105.
[58] West, R. 2008. "The Psychology of Security: Why Do Good Users Make Bad Decisions?", Communications of the ACM (51:4), pp. 34-40.