8-6-2011

# EFFECTS OF DEVELOPER COGNITIVE STYLE AND MOTIVATIONS ON INFORMATION SECURITY POLICY COMPLIANCE

Lakshman Mahadevan
*University of Memphis*, lmahadvn@memphis.edu

Judith C. Simon
*University of Memphis*, jsimon@memphis.edu

Thomas O. Meservy
*University of Memphis*, tmeservy@memphis.edu

# EFFECTS OF DEVELOPER COGNITIVE STYLE AND MOTIVATIONS ON INFORMATION SECURITY POLICY COMPLIANCE

**Lakshman Mahadevan**
University of Memphis
lmahadvn@memphis.edu

**Judith Simon**
University of Memphis
jsimon@memphis.edu

**Thomas Meservy**
University of Memphis
tmeservy@memphis.edu

## ABSTRACT

Organizations are faced with information loss on a daily basis. Threats such as hacker attacks are mitigated by applying patches, improving encryption routines, closing security loop-holes in a program and keeping a constant vigil on virus and malicious threats with up-to-date scanning techniques. Companies invest millions of dollars to keep such attacks at bay since a loss of up-time to servers could cause a significant loss in customer revenue and thus result in catastrophic losses in customer satisfaction and ultimately profits. Organizations that create or modify software try to deter threats to their applications by providing information security policies that provide guidelines to developers on what best practices need to be adopted to make their applications safe and secure for customer consumption. This study presents a conceptual model for studying how cognitive style impacts software developer motivations as they approach the task of complying with information security policies. The model is informed by the literature on information security awareness, Protection Motivation Theory, Kirton's adaption-innovation theory and Herzberg's motivation and hygiene theory.

## KEYWORDS

Motivation, Cognitive Style, Information Security Policy, Compliance.

## INTRODUCTION

Enterprises establish computer security policies to ensure the security of information resources (Herath and Rao, 2009). Organizations try to deter threats to their applications by providing information security policies (ISP) that provide guidelines to software developers on what best practices need to be adopted to make their application safe and secure for customer consumption. Many security breaches are a result of negligence or ignorance of security policies (Vroom and Solms 2004). Given the information-intense characteristics of a modern economy (e.g., the Internet and World Wide Web), it is no surprise that information security is a growing spending priority among most companies (Gordon and Loeb 2002, Cavusoglu et al. 2005).

Employee compliance with information security policies has been studied extensively in recent years (Pahnila et al. 2007, Bulgurcu et al. 2010, Boss et al. 2009). These studies have investigated factors such as mandatoriness, rewards, sanctions, threat appraisals, and coping behavior, among other factors. Many of these factors have been found to significantly impact compliance, however, there have been conflicting results reported on the impacts of rewards and sanctions on compliance (Pahnila et al. 2007, Bulgurcu et al. 2010, Boss et al. 2009). Also, research on software developers has shown that motivation has been quite difficult to quantify due to many inter-related, context-dependent factors (Beecham et al. 2008). We suggest that an investigation using the lens of motivation and cognitive styles may provide an avenue to more finely partial out the differences of the mixed results seen with rewards/sanctions and better quantify developer motivation. While employee compliance to ISPs has received much attention, investigation into developer compliance with ISPs has received relatively little attention. We suggest that understanding software developer compliance is particularly important as developers are a front-line defense against malicious attacks of software they construct. While IT administrators, infrastructure support

personnel, and end-users comply with ISPs that relate to operating system patches, malware and viruses, ISP in a developer context relate to application security policies that resolve risks and malicious threats associated with injection, cross site scripting, broken authentication and session management and many more mentioned by the Open Web Application Security Project (OWASP, 2010). Compliance of ISPs in this context involves adhering to guidelines when creating new code, as well as, maintaining existing code. Security is an integral part of most modern software systems; however, acceptance of security policies is sometimes problematic for software developers because security interferes with developing features and compliance can slow a product's release to market (Lampson, 1974). Violations or mis-application of mandated application security fixes by the developers may compromise the fidelity and security of organizational information that ultimately may wreak financial havoc and irreparable damage to the firm.

In this paper we lay the foundation for a research stream related to motivation of software developers to comply with ISPs by looking at task characteristics, perceived risk, and coping behavior moderated by the cognitive style of the developer.

## LITERATURE REVIEW

### Information Security Compliance

Literature in the area of ISP compliance has looked at technical aspects of integration of security policy design into the software development process (Brose et al. 2001) and has also focused on the need for users in an organization to be aware of the ISPs and recommend a conceptualized persuasion strategy (Siponen, 2000). Searching for antecedents of employee compliance with ISP of an organization, Bulgurcu et al. (2010) found that employee's intention to comply with the ISP is significantly influenced by attitude, normative beliefs, and self-efficacy to comply. They also found that information security awareness has a strong positive influence on attitude towards compliance with ISPs. However, there are conflicting research results regarding rewards and information security compliance; Bulgurcu et al. (2010) found a positive relationship whereas Boss and Kirsch (2007) found a negative relationship. Fear appeals were found to have a non-uniform impact on information security behavior of the end user. It is determined in part by perceptions of self-efficacy, response efficacy, threat severity and social influence (Johnston and Warkentin 2010).

### Motivation

Employee motivation is driven by the concept of need fulfillment (Mak and Sokel, 2001). Though there are results that show Information System (IS) employees share the same motivation factors as non-IS employees (Ferrat and Short, 1986), there are other results that have taken a contrary view (Im and Hartland, 1990, Sutherland 1992). IS professionals display high growth needs and are concerned about learning new technology (Cougar and Zawacki, 1978). From a developer perspective, motivation is acknowledged to have a major impact on the quality of the software product and productivity during the software development process (Beecham et al 2008).

### Developer and Task Characteristics

The most frequently cited motivating factors are 'the need to identify with the task' such as having clear goals, a personal interest, understanding the purpose of a task, how it fits in with the whole, having job satisfaction; and working on an identifiable piece of quality work (Beecham et al. 2008). Hall et al. 2008 mention task characteristics should include technically challenging work and should offer variety where the developer feels his or her skills are being stretched and put to good use. From a coping behavior perspective, developers need to be technically competent, autonomous, marketable and creative (Hall et al. 2008). Beecham et al. 2008, in their survey of 92 papers related to motivation in software engineering found other developer characteristics to include organizational stability, need for feedback and challenge in the task at hand.

### Cognitive Style

Ryhammer and Smith [1999] identify organizational structure, culture, climate, resources, workload pressure, and leadership style as critical organizational influences on creativity. Amabile et al. (1996) suggests a model comprised of five environmental components that impact organizational creativity, namely, encouragement of creativity, autonomy, resources, pressures, and organizational impediments to creativity. From a job structure perspective, it has been noted that in large scale collaborative creativity situations, developers are expected to be creative while working under the constraints of extensive formalization and standardization of work processes and under the centralized authority in a finely graduated management hierarchy (Adler and Chen 2009). Research by Sagiv et al. (2009) found that intuitive individuals are more creative than systematic ones under free conditions and that the systematic individual could attain creativity levels similar to intuitive ones under highly structured conditions. Seidel et al. (2010) highlight how little attention the IS discipline has paid to the human phenomenon of creativity and how it unfolds in socio-technical processes. Companies depend on the creative capabilities of their developers to deliver quality software that meets or exceeds customer requirements to retain or gain on market share.

Research in the area of linking employee creativity, motivation and job complexity has found a positive relation between extrinsic rewards and creativity for employees with an adaptive cognitive style who worked on relatively simple jobs (Baer et al. 2003). The research also suggests a relation between rewards and creativity for employees with an innovative cognitive style who worked on complex jobs and a negative relation for those in the adaptive style/complex job and innovative style/simple job conditions. However, the research study was conducted in a manufacturing organization where the employees had skills such as line operator, tool maker and design drafter and as such the participants were not developers and the jobs undertaken by the employees were non-IT related. As pointed out the motivation of IS employees are different from those of non-IS employees (Im and Hartland, 1990, Sutherland 1992). Recently, Seidel et al. (2010) described that information technology creates an unprecedented environment that has great potential to nourish the creativity of individuals, organizations, and even societies. Yet, much regarding the underlying socio-technical processes related to creativity, motivation, and job complexity in the context of the using and applying information systems (IS) remains unknown. We suggest, as others have, that the IS discipline can meaningfully contribute to the understanding of the creative process and how it can deliberately be nourished, or hindered, by IS. Though motivation factors for developers in open source software conditions (Wu et al. 2007, Herman et al. 2003) and motivation and retention of IS employees (Mak and Sockel, 2001) have been researched, little research in IS has focused on motivation of developers to develop quality software that meets business requirements in an ISP perspective. Also, research that acknowledges developer creativity and their reaction to ISP hasn't been researched in much detail. Beecham et al. (2008), in their review of IS motivational research state that 'the job itself' continues to be the principal motivator. William and Yang (1999) state that the creative process is perceived as taking place within the context of a particular environment rather than in a vacuum. Therefore, considering the changes in job demands in terms of new skills and communicating with many different stakeholders, there appears to be a gap in defining what exactly it is about 'the job' that motivates developers. This research paper investigates the phenomenon of creativity and motivation in context of the job of applying information security patches to software applications.

## THEORETICAL FOUNDATIONS

### Protection Motivation Theory

Protection motivation theory (PMT) originally proposed by Rogers (1975) suggested three "critical components of fear appeal," identified as "(a) the magnitude of noxiousness of a depicted event; (b) the probability of that event's occurrence; and (c) the efficacy of a protective response." He indicated that, "with the protection motivation theory, people appraise the severity and likelihood of being exposed to a proposed noxious event, evaluate their ability to cope with the event, and alter their attitudes accordingly." One difference between PMT and other theories at that time was that PMT focused on the importance of cognitive rather than emotional influences in the mediating process of attitude change.

Other researchers have applied PMT to specific IS issues, including security. For example, Siponen et al. (2010) used PMT in developing a survey instrument for studying motivations that might cause employees to comply with organizational information security policies. Their findings included: (a) significant factors linked to an intention to comply with security policies included threat appraisal, self-efficacy, normative beliefs and visibility; (b) an intention to comply has a significant effect on actual compliance with security policies, (c) deterrence has a significant effect on actual compliance, and (d) rewards do not have a significant effect on actual compliance.

Herath and Rao (2009) also studied protection motivation related to security. They found that (a) policy attitudes are likely to be affected by threat perceptions about the severity of breaches as well as perceptions of response efficacy, self-efficacy, and response costs; (b) compliance intentions are significantly impacted by organizational commitment and social influence; and (c) self-efficacy is significantly enhanced by organizational commitment and social influence. This self-efficacy is a significant predictor of intent to comply with policies.

### Herzberg's Motivation and Hygiene Theory

Herzberg's motivation and hygiene theory describes intrinsic motivators are factors such as achievement, the work itself, responsibility, advancement and growth. In such conditions, developers love their work and find it challenging and are motivated to do the best they can to complete their program. Extrinsic motivators such as company policies, salary, coworker relations and supervisory styles, also called "hygiene" factors affect the developer attitudes towards their work. According to Herzberg, removing the hygiene factors will not necessarily translate to motivating the developers. It will simply maintain developers in their job and avoid dissatisfaction (Beecham et al. 2008). According to Deci and Ryan (1985) self-determination approach to motivation, intrinsic motivation is about doing an activity for the inherent satisfaction that it provides rather than for some separable consequence. When intrinsically motivated, the fun and challenge entailed in the

activity moves the person to take on the task rather than external factors such as rewards or pressures. Extrinsic motivation comes into play when the source of regulation is external to the activity.

### Kirton's Adaption-Innovation Theory

Cognitive style involves "characteristic modes of perceiving, remembering, thinking, problem solving, and decision making, reflective of information-processing regularities that develop… around underlying personality trends" (Messick, 1994). One view of cognitive style that has received extensive theoretical and empirical attention in the psychology and organizational literature is adaption-innovation (A-I) first articulated by Kirton (1976). A-I theory proposes that individuals have differing preferences for how they solve problems. Kirton and others demonstrated empirical support for each individual having a cognitive style on a continuum from adaption to innovation. Those developers who are relatively more adaptive prefer more structure in their software development realm. Adaptors make incremental improvements to the existing system, and carefully develop a few original ideas. The relatively more innovative think outside the current paradigm, prefer a looser structure, challenge existing rules and identify many solutions regardless of practicality (Kirton, 2003) (Robinson et al. 2010). Amabile (1996) proposed that intrinsic motivation is linked to creativity which can be viewed as a part of an individual's cognitive style. Creativeness in developers varies according to the situation. Based on Kirton's Adaptors-Innovation theory, developers can be either be content in utilizing their creative skills to modify the existing code base to meet business needs or would be very interested in using their creative energy in making whole sale changes to technology and has no issues taking on unknowns. Such developers jump into learning new technologies and programs that could shake the foundation of the existing technology base (Gallivan, 2003).

## RESEARCH QUESTIONS, PROPOSITIONS AND MODEL

General research questions about developer motivations have been extensively studied (Beecham 2010) and also employee compliance of ISPs in an organization has been widely recognized and studied (Siponen 2000, Bulgurcu et al. 2010, Boss and Kirsch 2007). However, research on creativity is limited in the IS context (Siedel et al. 2010) and little is known about inter-relationships between developer creativity and motivation, especially where a developer is required to comply with an ISP that requires changes to code that they may have created. Previous information security compliance studies have only looked at employee motivation to comply with ISPs where the employee is merely the user or consumer rather than having a vested interest (i.e., they created or have ownership) of the artifact that the ISP applies to. This conceptual paper, which lays the foundation for future empirical work, focuses on linking the creative persona as described by Kirton's A-I theory and other antecedents of motivation to motivational traits proposed by Herzberg's motivator-hygiene theory in the context of software developers applying security patches.

Based on the review of the literature, we suggest that several research questions should be investigated related to software developer compliance with ISP compliance. Specifically,

- What motivational factors influence software developers to comply with ISPs?
- How do task characteristics, risk of the security threat related to the task, and the coping behaviors (developer fit with task) influence the levels of intrinsic and extrinsic motivations to complete that task?
- How does individual cognitive style moderate the relationship between task characteristics (appraisal of threat/risk, coping behavior, and complexity/creativity) and motivational style (extrinsic/intrinsic)?

### Propositions

Developers with an innovative cognitive style would be very interested to take up the challenge of fixing code with an ISPs that is perceived to be high severity/high vulnerability. They would proactively work to rectify defect and would spend extra hours to understand the nature of the threat and patch the code accordingly. The challenging nature of the task would hold great appeal and bring out a sense of fulfillment in these developers (Kirton 2003, Beecham et al. 2008, Hall et al. 2008, Deci and Ryan, 1985). High severity of threat also improves the innovative developer's intention to comply with the ISP (Siponen et al. 2010). Our first proposition follows that:

*Proposition 1*: In general, a developer with innovative cognitive style who perceives the threat in the ISP to be of high severity and/or high vulnerability will be intrinsically motivated to address the ISP.

On the other hand, developers with an adaptive cognitive style who perceive high severity/high vulnerability with an ISP would comply with policy (Herath and Rao 2009) but not in a pro-active manner. There would be a tendency to complain about other tasks that they have on their list to complete and would bargain for reduction in their workload to complete this

task. They will see the patch work as a job to get done and wouldn't appreciate the challenge the job puts forth. They would do the job for the fear of sanctions (Pahnila 2007). Our second proposition follows that:

*Proposition 2*: A developer with adaptive cognitive style who perceives the threat in the ISP to be of high severity and/or high vulnerability will be extrinsically motivated to address the ISP.

In the case of complying with normal ISPs an innovative developer with the skills to complete the job would take on the task to keep his or her code current. In certain cases the code could have been written a while ago, requiring the developer to remember the logic and flow of the application to make sure that the patch is applied appropriately, an innovative developer is ready to do such work. Sometimes, the original developer of the application could have left the team, thus requiring a new developer to patch the code. Often it is a challenging task to come in the middle of things and do the patch work when the original application was written by another developer. This might take some time and there is a possibility that innovative developers even if they have the qualifications to do the job would resist doing this kind of work since it involves reviewing someone else's code. It follows that:

*Proposition 3*: Coping behavior - When an innovative developer has the skills and abilities to address an ISP ~~security threat~~ (and confidence to do so), in general they will be intrinsically motivated to comply with the ISP.

In the case of an adaptive developer with the necessary skills to complete the job (Siponen et al. 2010), he or she would be interested to take on the task to keeping the code current. In certain cases the code could have been written a while ago, requiring the developer to remember the logic and flow of the application to make sure that the patch is applied appropriately, an adaptive developer is ready to do such work since there are no major unknowns and is usually considered routine work. In the case of code where the original developer is no longer in the team, adaptive developers with the necessary qualifications to do the job would take up this kind of work since they have the skill set to complete the job and is usually not very challenging. It follows that

*Proposition 4*: Coping behavior - When an adaptive developer has the skills and abilities to address an ISP (and confidence to do so), in general they will be intrinsically motivated to comply with the ISP.

Information security patches may require the application of new technologies, approaches, or perhaps might even break existing code. These situations may require creativity on the part of the developers to patch the code and make it available for use. The challenge in such tasks would appeal greatly to innovative developers (Kirton 2003). Adaptive developers would be de-motivated to perform the task if the patch cannot be applied using familiar approaches with the skills sets they already have. They will hesitate to venture into the unknown to get to the bottom of the problem or look for out of the box solutions to rectify the issue. Extrinsic motivations, such as sanctions, would motivate them to get them out of their comfort zone to find a solution to the problem. It follows that

*Proposition 5*: Task Characteristic (Creativity) - When an innovative developer is presented with an ISP that requires creativity, they will be intrinsically motivated to comply with the ISP.

*Proposition 6:* Task characteristic (Creativity) - When an adaptive developer is presented with an ISP that requires creativity, they will be extrinsically motivated to comply with the ISP.

When task of patching the code is complex, an innovative developer should still like the challenge of complying with the ISP. Innovative developers take pride in their code and will go to great lengths to ensure that their code does not get exposed to vulnerabilities. Adaptive developers are well aware that they can comply with the information security guideline even though complexities exist and look for rewards to complete the work. It follows that:

*Proposition 7*: Task Characteristic (Complexity) – When an innovative developer is presented with a complex ISP, in general they will be intrinsically motivated to comply with the ISP.

*Proposition 8*: Task Characteristic (Complexity) – When an adaptive developer is presented with a complex ISP, in general they will be extrinsically motivated to comply with the ISP.

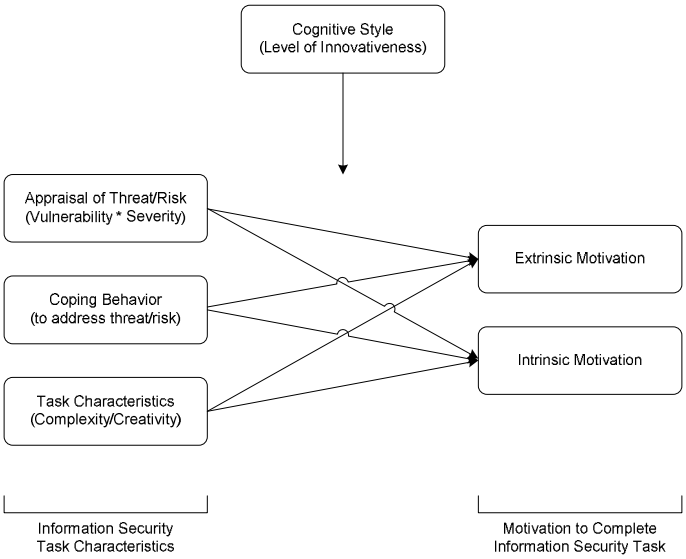


Figure 1. Conceptual Model of Propositions

Figure 1 presents a model that captures the propositions previously introduced. The model explains how developers with differing creative persona interact with motivations that can be either extrinsic or intrinsic when entrusted with the task of complying with ISPs.

## CONCLUSION

The concepts presented in this paper contribute to previous works on motivation and creativity from a developer context by introducing a framework to investigate the moderating influence of cognitive style on the impact of antecedents on motivations. Our initial investigations in a fortune 100 company reveal that some organizations impose a time limit on how soon the patch should be applied before upper management is notified that the task is incomplete. These sanctions are one mechanism to motivate developers to comply, however, we hope that our research could yield insights as to how management can have developers better comply with the task of applying information security patches to their code. While continuing our research in this fortune 100 company, we have also found that certain developers are pro-active and care a great deal about their code's success. Whereas certain other developers find complying with information security patches a chore.

We are currently designing a survey instrument, based on the propositions listed here, in an attempt to gather empirical support for our casual observations. This next study will survey developers from five organizations that focus on medical, transportation and hospitality markets. The survey will focus on security compliance in a maintenance context and will be sent to the software developers who had recently applied patches to applications following an ISP mandate. Empirical support gathered as part of this study may yield insights about what motivates developers to comply with ISPs and why certain individuals react differently to rewards and sanctions in the context security compliance.

ISPs may result in requiring developers to retro-fit their code for compliance purposes. Developers who do not show proclivity for such work might delay implementing security patches till the last moment and may not apply their minds to complete the task resulting in possible future vulnerabilities. Developers are vital to the success of an organization and the intent of the paper is to lay a framework for studying the developer's motivations to comply with information security guidelines keeping in mind the cognitive approach displayed. We hope to provide a practical contribution by developing a framework that management can use to ensure developer compliance with information security guidelines and keeping the cognitive capabilities of developers intact.

## REFERENCES

1. P. S Adler and C. X Chen, "Beyond intrinsic motivation: On the nature of individual motivation in large-scale collaborative creativity," *Social Science Research Network* (2009).

2. T. M Amabile et al., "Assessing the work environment for creativity," *Academy of Management Journal* 39, no. 5 (1996): 1154–1184.
3. M. Baer, G. R Oldham, and A. Cummings, "Rewarding creativity: when does it really matter?," *The Leadership Quarterly* 14, no. 4-5 (2003): 569–586.
4. A. Bandura, "Toward a unifying theory of behavior change," *Psychological Review* 84, no. 2 (1977): 91–215.
5. A. Bandura, "Social foundations of thought and action: A social cognitive theory" (1986).
6. R. Baskerville and M. Siponen, "An information security meta-policy for emergent organizations," *Logistics Information Management* 15, no. 5/6 (2002): 337–346.
7. S. Beecham et al., "Motivation in Software Engineering: A systematic literature review," *Information and Software Technology* 50, no. 9-10 (2008): 860–878.
8. S. R Boss and L. J Kirsch, "The Last Line of Defense: Motivating Employees to Follow Corporate Security Guideliness," in *Proceedings of the International Conference on Information Systems*, 2007, 1–18.
9. G. Brose, M. Koch, and K. P L\öhr, *Integrating security policy design into the software development process* (Citeseer, 2001).
10. B. Bulgurcu, "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly* 34, no. 3 (2010): 523–548.
11. H. Cavusoglu, B. Mishra, and S. Raghunathan, "The value of intrusion detection systems in information technology security architecture," *Information Systems Research* 16, no. 1 (2005): 28–46.
12. E. L Deci and R. M Ryan, *Intrinsic motivation and self-determination in human behavior* (Springer, 1985).
13. T. W Ferratt and L. E Short, "Are information systems people different: An investigation of motivational differences," *MIS Quarterly* 10, no. 4 (1986): 377–387.
14. M. J Gallivan, "The influence of software developers' creative style on their attitudes to and assimilation of a software process innovation," *Information & Management* 40, no. 5 (2003): 443–465.
15. L. A Gordon and M. P Loeb, "The economics of information security investment," *ACM Transactions on Information and System Security (TISSEC)* 5, no. 4 (2002): 438–457.
16. T. Hall et al., "What do we know about developer motivation?," *Software, IEEE* 25, no. 4 (2008): 92–94.
17. T. Herath and H. R Rao, "Protection motivation and deterrence: a framework for security policy compliance in organisations," *European Journal of Information Systems* 18, no. 2 (2009): 106–125.
18. G. Hertel, S. Niedner, and S. Herrmann, "Motivation of software developers in Open Source projects: an Internet-based survey of contributors to the Linux kernel," *Research policy* 32, no. 7 (2003): 1159–1177.
19. L. F Higgins, "A comparison of scales for assessing personal creativity in IS," in *System Sciences, 1996., Proceedings of the Twenty-Ninth Hawaii International Conference on,*, vol. 4, 2002, 13–19.
20. L. F Higgins and J. D Couger, "Comparison of KAI and ISP instruments for determining style of creativity of IS professionals," in *System Sciences, 1995. Proceedings of the Twenty-Eighth Hawaii International Conference on*, vol. 4, 2002, 566–570.
21. J. H Im and S. Hartman, "Rethinking the issue of whether IS people are different from non-IS people," *MIS Quarterly* 14, no. 1 (1990): 1–2.
22. A. C Johnston and M. Warkentin, "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly* 34, no. 1 (2010).
23. M. Kirton, "Adaptors and innovators in organizations," *Human Relations* 33, no. 4 (1980): 213.
24. M. J Kirton, *Adaption-innovation: In the context of diversity and change* (Psychology Press, 2003).
25. B. W Lampson, "Protection," *ACM SIGOPS Operating Systems Review* 8, no. 1 (1974): 18–24.
26. B. L Mak and H. Sockel, "A confirmatory factor analysis of IS employee motivation and retention," *Information & Management* 38, no. 5 (2001): 265–276.
27. OWASP, "Top 10 2010-Main," (2010), Retrieved January 14, 2011, from https://www.owasp.org/index.php/Top_10_2010-Main
28. S. Pahnila, M. Siponen, and A. Mahmood, "Employees' behavior towards IS security policy compliance," in *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on*, 2007, 156b.
29. S. Ramlall, "A review of employee motivation theories and their implications for employee retention within organizations," *Journal of American Academy of Business* 5, no. 1/2 (2004): 52–63.
30. D. F Robinson, A. L Sherwood, and C. A DePaolo, "Using Adaption-Innovation Theory to Enhance Problem-based Learning Experiences," in *Allied Academies International Internet Conference*, vol. 12, 2010.
31. R. W Rogers, "A Protection Motivation Theory of Fear Appeals and Attitude Change1," *The Journal of Psychology* 91, no. 1 (1975): 93–114.
32. S. Seidel, F. M\üller-Wienbergen, and J. Becker, "The Concept of Creativity in the Information Systems Discipline: Past, Present, and Prospects," *Communications of the Association for Information Systems* 27, No. 1 (2010): 14.

33. M. T Siponen, "A conceptual foundation for organizational information security awareness," *Information Management & Computer Security* 8, no. 1 (2000): 31–41.
34. E. Sutherland, "Strategic Management and Information Systems: An Ambiguous Relationship," *International Journal of Information Resource Management* 3, no. 2 (1992).
35. C. Vroom and R. Von Solms, "Towards information security behavioural compliance," *Computers & Security* 23, no. 3 (2004): 191–198.
36. C. G Wu, J. H Gerlach, and C. E Young, "An empirical analysis of open source software developers' motivations and continuance intentions," *Information & Management* 44, no. 3 (2007): 253–262.