The Impact of Computer Monitoring on Policy Compliance: An Agency and Stewardship View

Submission Type: Research-in-Progress

Nirmalee Ratnamalala
Mississippi State University
nirmalee@nirmalee.us

Kent Marett
Mississippi State University
kmarett@cobilan.msstate.edu

Abstract

Several researchers have investigated the factors influencing individual's policy compliance utilizing theories such as Protection Motivation Theory and General Deterrence Theory. However, only a few research studies have focused on the impacts of controls such as computer monitoring or surveillance on organizational computer security compliance. This study attempts to fill that gap in research by focusing on Information Security Policy compliance intentions of employees by drawing upon Agency Theory and Stewardship Theory through the use of managerial controls such as computer monitoring.

Keywords

Agency Theory, Stewardship Theory, Computer monitoring, Security policy compliance.

Introduction

Organizations generate an influx of information on a routine basis while striving to secure these information assets from various threats from both external and internal parties. Securing information systems from these threats have become one of the paramount goals of many organizations. Technological tools and techniques such as firewalls, anti-malware software and penetration testing have been deployed by many organizations to improve information security (Straub 1990). While these techniques can be effective for deterring threats from outsiders, they are likely inadequate for eliminating the 'insider threat' from the company employees (Herath et al. 2009a; Siponen, 2005).

Employees are considered to be the weakest link when it comes to organizational information security (Warkentin et al. 2009), and security governance programs and managerial controls are often implemented to enforce employees to perform secure behaviors. Information security policies attempt to encourage employees to "ensure information security while they utilize information systems in the course of performing their jobs" (Bulgurcu et al. 2010, p. 524), and employees who follow policies are acting as "good stewards" of the organization's security goals. However, security policies alone may not always be sufficient. Other means of governing security may be necessary, such as employee computer monitoring, which is the focus of this study.

Computer monitoring of employees is becoming more prevalent in organizations where certain activities such as email communications, internet usage and social media usage of employees are under strict scrutiny of the employer (Post et al. 2007). While it is not practical for computer monitoring techniques to monitor every information security related action of each employee (Herath et al. 2009b), employees who are aware that their actions are being monitored are more likely to comply with security policies (Tosi et al. 2003). Previous literature also suggests that computer monitoring can enhance the relationship

between perceived impact of penalties and the behavioral intention to comply with security policies (D'Arcy et al. 2011; D'Arcy et al. 2009). However, employees who otherwise act as good stewards may resent being monitored, leading to unintended consequences. To our knowledge, these possible moderation impacts of computer monitoring have not been previously examined.

The purpose of this research-in-progress is to better understand how stringent governance mechanisms like computer monitoring might affect the relationship between employees, managers, and the organization. To do so, we draw upon two theories, agency theory and stewardship theory, and re-examine previous security literature, concluding by offering propositions regarding how we expect computer monitoring to influence intentions to comply with security policies.

Theoretical Background

Agency Theory

When considering employee compliance with any general company policy, it is important to acknowledge that the goals of the employee and management may not always be aligned. In terms of information security, the goal of the employer would be to ensure that employees use information systems in a secure manner that remains on task. The expected goals of the employee are to complete their tasks and receive rewards for their productivity, but opportunistic shirking behavior may persist. Agency theory names this potential misalignment of goals between the employer and employee as the 'principal-agent problem' (Eisenhardt 1989; Jensen et al. 1976), where the principal is the employer and the agent is the employee. Agency theory views policy-making and the use of managerial controls like monitoring as a means of (a) re-aligning the principal-agent goals, and (b) reducing information asymmetries (in the form of shirking) between the agent and the principal.

With computer monitoring allowing the measurement of policy compliance by specific employees, managerial controls in the form of rewards (positive sanctions) and penalties (negative sanctions) provide motivation for improved compliance. Rewards can be provided to the employees through monetary incentives such as salary increases or performance bonuses or through informal incentives such as appreciation and recognition of a job well done. These rewards are used to extrinsically motivate employees to comply with security policies, therefore aligning employee goals with the goals of their employer which can reduce the principal-agent problem. However, employers may resort to motivating employees to comply with security policies through negative sanctions or penalties such as public ridicule, demotion and employment termination (Herath et al. 2009b). For this study, we focus on penalties to investigate the impact of management controls on security policy compliance by employees.

Criminology literature provides the foundation to investigate the impact of penalties when agents decide whether or not to comply with security policies. General Deterrence Theory (GDT) suggests that when the threat of sanctions or penalties is increased, individuals are more likely to avoid deviant behavior, whereas the threat of sanctions is likely to influence employees to comply with organizational security policies (D'Arcy et al. 2012; D'Arcy et al. 2009; Herath et al. 2009a, 2009b; Hovav et al. 2012; Siponen et al. 2010). Previous IS literature have found empirical evidence to suggest that the three components of GDT: sanction severity, sanction certainty and sanction celerity have positive impacts on employee security policy compliance. The rest of this section examines the influence of penalties in reducing the principle-agent problem by utilizing the three components of GDT in our conceptual model.

Sanction severity is an individual's belief of the magnitude of the sanction that is experienced as a result of unwanted behavior. According to GDT, when the perceived severity of the sanctions increase, the

individuals are less likely to engage in deviant behavior. Herath et al. (2009a) utilized sanction severity as a component of penalties. This is a method of managerial control suggested in the agency theory in investigating an individual's intention to comply with company policies. Their findings suggest that severity of penalties had a negative effect on security behavior intentions.

Therefore, in the context of this study, high penalties are expected to increase agent's (employees) intention to comply with company policies. When the organization imposes high penalties for non-compliance such as heavy fines, demotion, or termination of employment, this can result in reducing the individuals intention to engage in deviant acts (Herath et al. 2009b). Therefore, we propose:

Proposition 1. Severity of penalty will positively influence behavioral intention to comply with organizational information security policies.

Sanction certainty is an individual's expectation of getting apprehended for performing illicit behavior. When an individual believes that he or she will get punished for deviating from company policy, it is likely that the individual will refrain from engaging in the act.

Thus, in the context of this study, high certainty of penalties in cases of detection of deviant behavior is expected to increase an agent's intention to comply with company policies. Therefore, we hypothesize:

Proposition 2: Certainty of penalty will positively influence behavioral intention to comply with organizational information security policies.

Sanction Celerity regards individuals' expectations of the swiftness that sanctions for non-compliance will be handed down, perhaps even right after illicit behavior occurs. When the organization imposes penalties for non-compliance such as heavy fines, demotion, or loss of a job in a very quick manner, this can result in reducing the individual's intention to engage in deviant acts. Therefore, we hypothesize:

Proposition 3: Celerity of penalty will positively influence behavioral intention to comply with organizational information security policies.

Stewardship Theory

Stewardship Theory suggests that both employees and managers strive to be good stewards of company assets, and compliance with company policy is founded on the shared goals held by both sets of stakeholders (Davis et al. 1997). The stewardship behavior displayed by managers, which is reflected by three psychological factors and three situational factors of Stewardship Theory, is likely to increase the employee intentions to comply with organizational security policies. In contrast to Agency theory, which asserts the need for managerial controls to align employer-employee goals, Stewardship Theory posits that organizational goals such as employee compliance of security policies can be achieved through stewardship behavior. In this section, we focus on the six psychological and situational factors that explains the stewardship behavior identified by Davis et al. (1997): motivation, identification, use of power, management philosophy, culture (Individualism-collectivism) and power distance. We expect that when stewardship behaviors exist, implementing managerial controls such as computer monitoring may negatively impact the manager-employee relationship. Employees would question the reasons they are being monitored and may question their loyalty to the organization and the management. This may result in a negative impact on the relationship between the stewardship components and security policy compliance intentions of employees.

Intrinsic Motivation: One of the major differences between Agency theory and Stewardship Theory lie in the dimension of motivation (Davis et al. 1997). Agency theory proposes that employees are motivated through extrinsic factors such as monetary rewards, promotions, and sanctions, while Stewardship Theory puts forth that employees are motivated through non-pecuniary, intrinsic factors, such as the satisfaction for a job well done. In order to attain these intrinsic rewards, stewards will attempt to align their goals with the principal by working towards the greater good of the organization. In the context of this particular study, we expect the stewardship behavior of a manager to influence the employees' behavior. As a steward, the manager will tend to influence the employees by motivating them intrinsically. When the employees are motivated intrinsically, they will be more likely to comply with company security policies. Therefore we hypothesize:

Proposition 4. Intrinsic motivation will positively influence behavioral intention to comply with organizational information security policies.

Organizational Identification refers to instances "when managers define themselves in terms of their membership in a particular organization by accepting the organization's mission, vision, and objectives" (Davis et al. 1997, p. 29). Identification will result in the steward considering the organization as part of her own mental structure. This will result in a steward feeling a belongingness towards the organization (Ashforth et al. 1989) where there will be an alignment of values between the organization and the steward (Pratt 1998). An employee who identifies herself as a part of the organization is more likely to infer the comments towards an organization as aimed at herself (Davis et al. 1997) and identify any success related to the organization as part of her own success (Salancik et al. 1984). The stewardship behavior exhibited by managers, on behalf of the organization, will in turn influence the identifying employees to behave in a similar manner.

Proposition 5. Organizational identification will positively influence behavioral intention to comply with organizational information security policies.

Use of Power has being identified to be an important aspect of the relationship between a steward/employee and the agent/manager (Davis et al. 1997). Several researchers have demonstrated that stewards tend to receive greater satisfaction through the enforcement of power over their agents (McClelland et al. 1976; McClelland 1970). Managers who have a high need for power tend to "influence or direct other people; express opinions forcefully; enjoy the role of leader and may assume it spontaneously"(Steers et al. 1994, p. 148). As Stewardship Theory suggests, the steward will rely heavily on her personal power as a means of persuading other agents while managers in an agency setting will utilize punishments, rewards as the principal means of control (Craig et al. 2011).

Employees acting as good organizational stewards are assumed to utilize their personal power inherent within their jobs in motivating employees to engage in good citizenship behavior that results in benefits to the organization. When utilizing personal power, managers will also attempt to justify their actions on certain decisions. Thus, good stewardship behavior of managers will involve the utilization of their personal power (with proper justification) in order to persuade the employees to comply with organizational policies. Thus, we propose:

Proposition 6. Use of power will positively influence behavioral intention to comply with organizational information security policies.

Management Philosophy (or Involvement Orientation) can be classified into control-oriented and involvement-oriented philosophies (Lawler 1992). Where the former is based on the philosophy that "the thinking and controlling part of the work must be separated from the doing part of the work," the latter does not create a separation among the thinking, controlling and the performing work (Davis et al. 1997, p. 32). In the control-oriented approach, organizational relationships will mainly be transactional and

base on organizational power that assumes a self-fulfilling prophecy. By contrast, in the involvement-oriented approach, when employees are assumed to take responsibility for certain actions and tasks, they will foster self-control and self-management (Craig et al. 2011; Davis et al. 1997), acting as good stewards of the organization.

In the context of this particular study, the stewardship behavior of the manager will result in herself involving all the employees in important organizational decisions. Hence, the employees will feel a responsibility to comply with organizational policies for the greater good of the organization.

Proposition 7. Involvement Orientation will positively influence behavioral intention to comply with organizational information security policies.

Collectivism: Culture lies along the dimensions of individualism and positivism with the former mainly focusing on achieving personal goals over the goals of a group. In organizations who value collectivist cultures, employees will be identified as part of the organization where the organization membership becomes an important aspect of the individual's self-identification (Davis et al. 1997). The success of the organization will be defined in terms of the success of the employees as a group.

We expect that a manager's stewardship behavior centers on a collectivist approach to managing and solving organizational problems. Therefore, managers and employees will consider acts of compliance as an important aspect of organizational success, which in turn leads to the success of the employees as a group. Given the above logic, we hypothesize:

Proposition 8. Collectivism will positively influence behavioral intention to comply with organizational information security policies.

Power Distance: Hofstede (1991) defines power distance as "the extent to which less powerful members of institutions and organizations within a country expect and accept that power is distributed unequally" (Hofstede 1991, p. 28). In a culture where there is a high power distance, less powerful members will depend on the more powerful members. In organizations with high power distance, managers will be favorable to agency relationships as opposed to stewardship behaviors since they value the unequal distribution of power among the agent and the steward. Low power distance cultures favor stewardship behavior since members place equal value towards the agent and the steward. This in turn will encourage the development of closer relationships among the steward and the agent (Davis et al. 1997).

Managers are likely to value power distance and exercise greater authority over their employees. Due to the difference in power among the employees and managers, it will result in managers frequently using authority and power over their subordinates. They will also make majority of the organizational decisions without any consideration to the input of the employees. In such a situation, when employees' input is less valuable, the employees will not feel the need to comply with company policies for the well-being of the organization. Thus, we propose:

Proposition 9. Power distance will negatively influence behavioral intention to comply with organizational information security policies.

Based on Agency theory and Stewardship theory, we propose a developmental research model presented in Figure 1 that summarizes the relationships leading an employees' intention to comply with company security policies. The research framework illustrated, will evaluate the importance of: 1) penalties; 2) psychological and situational factors related to a mangers characteristics; and 3) computer monitoring. It is important to note that, while some management literature describes Agency theory and Stewardship Theory as being alternate views of the manager-employee relationship, others suggest that the relationship exists along a continuum (Chrisman et al., 2014). That is, employees are neither exclusively

self-interested agents nor entirely good company stewards; it is expected that employees and their goals tend to drift between the two extremes. Thus, the model developed in this paper is designed to reflect that view of the two theories. Both the deterrence factors that are expected to align with the principal-agent control mechanisms and the six psychological and social factors reflecting good stewardship behavior are to be examined together.

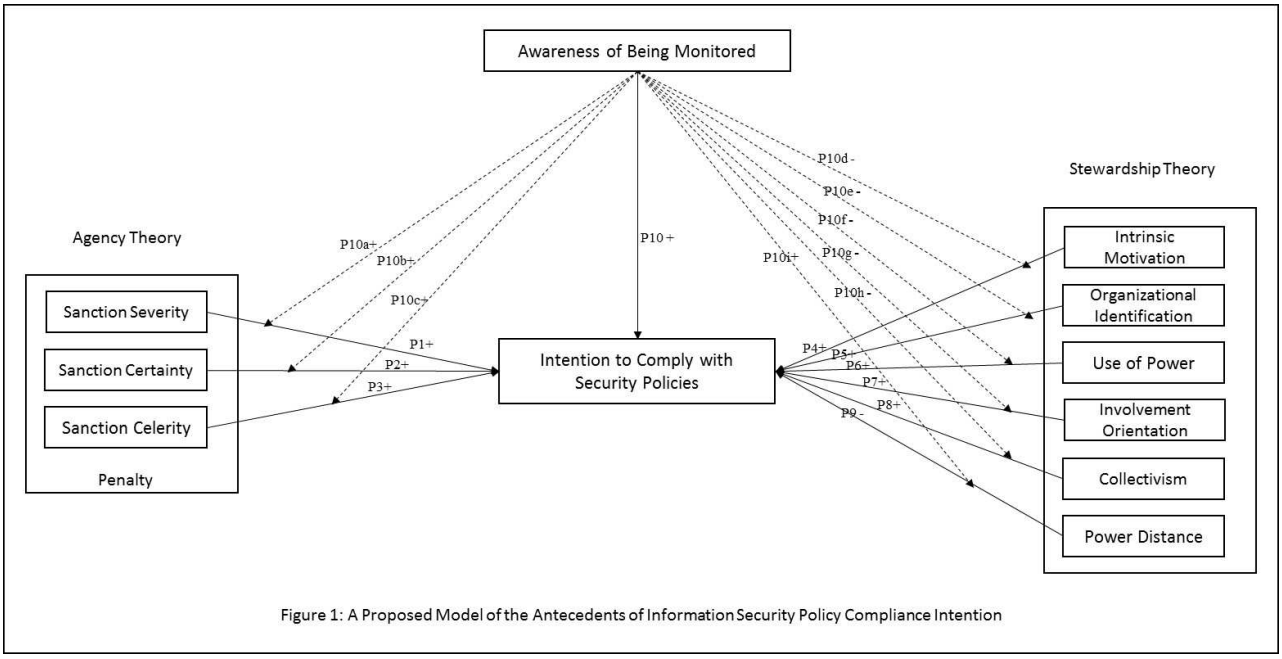

Figure 1. A Proposed Model of the Antecedents of Information Security Policy Compliance Intention

Direct and Moderating Effects of Computer Monitoring

With the use of computer monitoring and surveillance tools available, organizations can monitor employee activities related to e-mail communications, social network usage, internet usage etc. According to the Agency theory, employees are less likely to act in their own self-interest over the organizations when they are being monitored (Tosi et al. 2003). We propose that, when employees are aware that their computer activities are being monitored, they are more likely to follow security policies.

Proposition 10. Awareness of computer monitoring will positively influence behavioral intention to comply with organizational information security policies.

Penalties or disincentives can also be considered as types of managerial controls which are part of Agency theory. The influences of these penalties towards policy compliance are measured with components of deterrence theory such as sanction certainty, severity and celerity. D'Arcy et al. (2011) discuss several contextual factors that may moderate the relationships between components of deterrence theory and policy compliance intention. One such contextual factor is 'virtual status' which is defined as "the degree of work that an employee performs from dispersed locations compared to within the primary or central workplace" (D'Arcy et al. 2011, p. 646). The results of empirical studies regarding the virtual status suggest that deterrent effects of computer monitoring are weaker for employees who work remotely, presumably because they believe they are less easily monitored by the organization. Conversely, when employees are aware that they are being monitored, they are more likely to perceive the effects of deterrence that are in place. Therefore we propose that an employee's awareness of computer monitoring

awareness moderates the relationship between the three components of deterrence theory and policy compliance intention:

Proposition 10A. Awareness of computer monitoring will positively moderate the relationship between sanction severity and behavioral intention to comply with organizational information security policies.

Proposition 10B. Awareness of computer monitoring will positively moderate the relationship between sanction certainty and behavioral intention to comply with organizational information security policies.

Proposition 10C. Awareness of computer monitoring will positively moderate the relationship between sanction celerity and behavioral intention to comply with organizational information security policies.

As discussed previously, stewardship behaviors of managers are likely to increase the behavioral intention of employees to comply with security policies. Stewardship behavior implies the existence of a similar goal alignment between the employee and the manager. However, when employees become aware of computer monitoring and surveillance tools in place to monitor their work activities, the relationship between employees and managers, and as a result, their shared goal alignment, can be negatively impacted. Employees may no longer value the behavior exhibited by the managers as they are likely to feel that their loyalty to the organization is being questioned. In fact, we propose that employees' awareness of computer monitoring moderates the six factors put forth by Stewardship Theory such that they reduce the original intention to comply with security policies.

Proposition 10D. Awareness of computer monitoring will negatively moderate the relationship between intrinsic motivation and behavioral intention to comply with organizational information security policies.

Proposition 10E. Awareness of computer monitoring will negatively moderate the relationship between organizational identification and behavioral intention to comply with organizational information security policies.

Proposition 10F. Awareness of computer monitoring will negatively moderate the relationship between collectivism and behavioral intention to comply with organizational information security policies.

Proposition 10G. Awareness of computer monitoring will negatively moderate the relationship between involvement orientation and behavioral intention to comply with organizational information security policies.

Proposition 10H. Awareness of computer monitoring will negatively moderate the relationship between use of power and behavioral intention to comply with organizational information security policies.

Proposition 10I. Awareness of computer monitoring will positively moderate the relationship between power distance and behavioral intention to comply with organizational information security policies.

Future Research

This paper presents a developmental research model that seeks to examine the dynamics of the manager-employee relationship and how it may be affected when strict managerial controls, like computer monitoring and the various rewards and sanctions that correspond with it, are implemented. Empirical assessment of the model is currently being planned. Future steps in this research effort will involve conducting an online survey, which will be administered to organizational employees belonging to various organizations. As depicted in the research model, we will be assessing employee's behavioral intention to comply with organizational security policies rather than their actual policy compliance behavior, due to the fact that actual behavior is difficult for a researcher to measure (Vroom et al. 2004) since security policies can comprise of several guidelines some of which are not practical to be measured. Furthermore, security policies, their standards and the penalties imposed in non-compliance situations can greatly vary within and between organizations.

References

Ashforth, B., and Mael, F. 1989. "Social Identity Theory and the Organization," *Academy of Management Review* (14:1), pp. 20–39.

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.

Craig, J., Dibrell, C., Neubaum, D., and Thomas, C. 2011. "Stewardship Climate Scale: Measurement and an Assessment of Reliability and Validity," In *71st Annual Meeting of the Academy of Management (AOM)*New York.

Chrisman, J.J., Memili, E., and Misra, K. 2014 (in press). Non-family managers, family firms, and the winner's curse: The influence of non-economic goals and bounded rationality. *Entrepreneurship Theory and Practice*, 38.

D'Arcy, J., and Devaraj, S. 2012. "Employee Misuse of Information Technology Resources: Testing a Contemporary Deterrence Model," *Decision Sciences* (43:6), pp. 1091–1124.

D'Arcy, J., and Herath, T. 2011. "A Review and Analysis of Deterrence Theory in the IS Security Literature: Making Sense of the Disparate Findings," *European Journal of Information Systems* (20:6), pp. 643–658.

D'Arcy, J., Hovav, A., and Galletta, D. F. 2009. "User awareness of security countermeasures and its impact on information systems misuse: a deterrence perspective," *Information Systems Research* (20:1), pp. 79–98.

Davis, J., Schoorman, D., and Donaldson, L. 1997. "Toward A Stewardship Theory Of Management," *Academy oí Management Review* (22:1), pp. 20–47.

Eisenhardt, K. 1989. "AT: An Assessment and Review," *Academy Of Management Review* (14:1), pp. 57–74.

Herath, T., and Rao, R. 2009a. "Protection Motivation and Deterrence: a Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems* (18:2), pp. 106–125.

Herath, T., and Rao, R. 2009b. "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness," *Decision Support Systems* (47:2), pp. 154–165.

Hofstede, G. 1991. *Cultures and Organizations: Soltware of the Mind*, London: McGraw-Hill.

Hovav, A., and D'Arcy, J. 2012. "Applying an Extended Model of Deterrence Across Cultures: An Investigation of Information Systems Misuse in the U.S. and South Korea," *Information & Management* (20:1), pp. 79–98.

Jensen, M. C., and Meckling, W. H. 1976. "Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure," *Journal of Financial Economics* (3:4).

Lawler, E. 1992. *The Ultimate Advantage*, San Francisco: Jossey-Bass.

McClelland, D. 1970. "The Two Faces of Power," *Journal oí international Aíiairs* (24:1), pp. 29–47.

McClelland, D., and Burnham, D. 1976. "Power is the Great Motivator," *Harvard Business Review* (54:2), pp. 100–110.

Post, G. V., and Kagan, A. 2007. "Evaluating Information Security Tradeoffs: Restricting Access Can Interfere With User Tasks," *Computers & Security* (26:3).

Salancik, G., and Meindl, J. 1984. "Corporate Attributions as Strategic Illusions of Management Control," *Quarterly, Administrative Science* (29:2), pp. 238–254.

Siponen, M. T. 2005. "An Analysis of the Traditional IS Security Approaches: Implications for Research and Practice," *European Journal of Information Systems* (14:3), pp. 303–315.

Siponen, M., and Vance, A. 2010. "Neutralization : New Insights Into the Problem of Employee Information Systems Security Policy Violations," *MIS Quarterly* (34:3), pp. 487–502.

Steers, R., and Black, J. 1994. *Organizaíionaí Behavior*, New York: HarperCollins.

Straub, D. 1990. "Effective IS Security: An Empirical Study," *Information Systems Research* (1:3), pp. 255–276.

Tosi, H., Brownlee, A., Silva, P., and Katz, J. 2003. "An Empirical Exploration of Decision-making Under Agency Controls and Stewardship Structure," *Journal of Management Studies* (40:8), pp. 2053–2071.

Vroom, C., and Solms, R. von. 2004. "Towards Information Security Behavioural Compliance," *Computers & Security* (23), pp. 191–198.

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