Winter 12-14-2013

How Moral Intensity and Impulsivity Moderate the Influence of Accountability on Access Policy Violations in Information Systems

David Eargle
University of Pittsburgh

Anthony Osborn Vance
Brigham Young University - Utah, anthony@vance.name

Paul Benjamin Lowry
City University of Hong Kong

How Moral Intensity and Impulsivity Moderate the Influence of Accountability on Access Policy Violations in Information Systems

David Eargle
University of Pittsburgh, USA

Anthony Vance[1]
Brigham Young University, USA

Paul Benjamin Lowry
City University of Hong Kong, Hong Kong

ABSTRACT

A persistent threat to the security of information systems is that of malicious insiders. These insiders, who by definition are trusted, are a major concern for organizations because of their ability to misuse access privileges, steal intellectual property, and commit fraud. The recent high-profile cases of Private Manning and Edward Snowden have further raised organizations' concerns of the insider threat. Consequently, it is important to identify ways to reduce insiders' abuse of information systems.

Previous research has shown the potential of perceived accountability within systems to reduce access policy violations, one common form of insider abuse (Vance et al. 2013). This research expands on this previous effort by showing how the constructs of moral intensity and impulsivity moderate the influence of accountability mechanisms on access policy violations.

Keywords: Insider threat, Accountability theory, Factorial survey method, Scenario method.

[1] Corresponding author: anthony@vance.name

INTRODUCTION

A persistent threat to the security of information systems is that of malicious insiders. These insiders, who by definition are trusted, are a major concern for organizations because of their ability to misuse access privileges, steal intellectual property, and commit fraud (Rubenstein 2008; Schmitt 2011). The recent high-profile cases of Private Manning and Edward Snowden have further raised organizations' concerns of the insider threat (Savage 2013). Consequently, it is important to identify ways to reduce insiders' abuse of information systems.

Previous research has shown the potential of perceived accountability within systems to reduce access policy violations, one common form of insider abuse (Vance et al. 2013). This research expands on this previous effort by showing how the constructs of moral intensity and impulsivity moderate the influence of accountability mechanisms on access policy violations. Our research question is,

RQ*: How do moral intensity and impulsivity influence the effect of accountability on intentions to violate the access policy?*

We conducted a field study that presented hypothetical scenarios and a simulated accountability user interface (UI) artifacts to professional users of an Oracle PeopleSoft human resource management system (HRMS) and financial management system (FMS). We anticipate that the analysis will show how the influence of impulsivity and moral intensity influence the effectiveness of these accountability UI artifacts in reducing access policy violations.

THEORY AND HYPOTHESES

Our theoretical model of accountability within a system is presented in Figure 1. Accountability is "the implicit or explicit pressure to justify one's beliefs and actions to others" (Tadmor and Tetlock 2009, p. 8). It is a multifaceted construct, as "even the simplest

accountability manipulation necessarily implicates several empirically distinguishable submanipulations" (Lerner and Tetlock 1999, p. 255), including the presence of another, identifiability, and evaluation. These constructs are particularly amenable to manipulation by system-related artifacts because of the potential of IT to monitor and/or record behavior (D'Arcy et al. 2009).

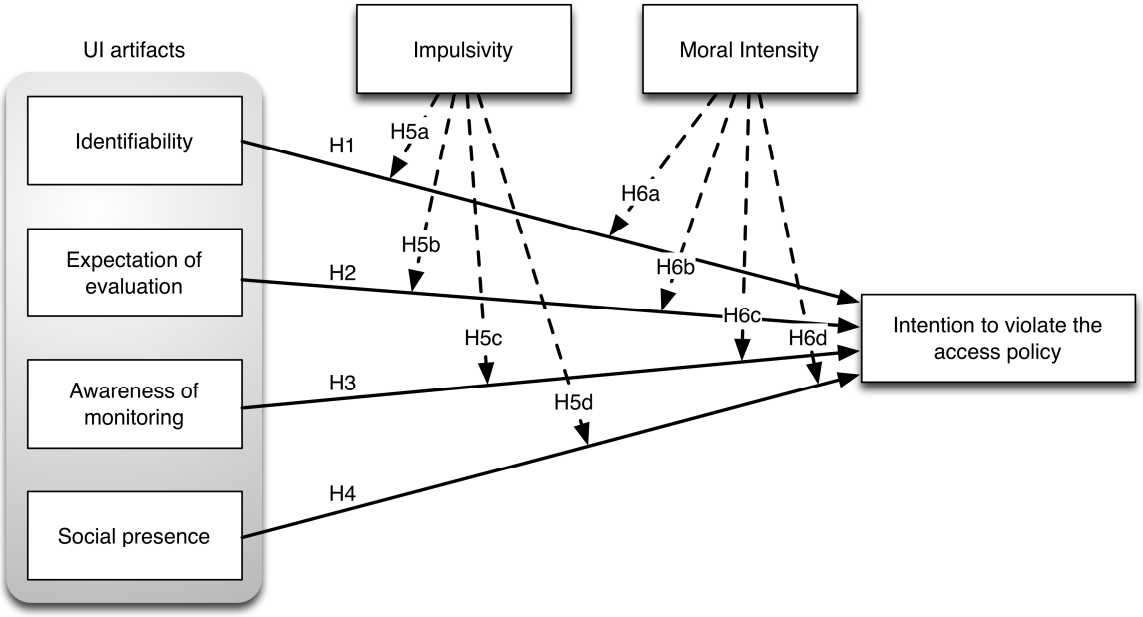

Figure 1. Theoretical model.

Identifiability is a person's "knowledge that his outputs could be linked to him" (Williams et al. 1981, p. 309). Identifiability is a necessary facilitator of accountability because this mechanism causes a person to know his or her actions can be traced back to him or her and that he or she can therefore be made responsible for those actions (Lerner and Tetlock 1999). When a person is thus performing behaviors that are identifiable, he or she is more likely to engage in systematic processing to ensure he or she performs only behaviors for which he or she is willing to be responsible. Conversely, if a person is not identified, he or she has less incentive

to engage in systematic processing to accept responsibility for an outcome. Thus, we hypothesize the following:

H1. *User-interface artifacts that foster identifiability will decrease intention to commit access policy violations.*

Evaluation is the belief that a person's "performance will be assessed by another [party] according to some normative ground rules and with some implied consequences" (Lerner and Tetlock 1999, p. 255). Our research focuses on two fundamental forms of evaluation: (1) logging or observing a person's behavior by an organization (monitoring), and (2) the person's expectation of being evaluated based on the behavior observed or recorded.

Studies have shown that awareness of evaluation increases socially desirable behaviors (Lerner and Tetlock 1999) and deters socially undesirable ones (Sedikides et al. 2002). This is because awareness of evaluation can create *evaluation apprehension* (Geen 1991), a state of mind in which self-focused attention is increased and performance is modified in the presence of those who can disapprove or approve of actions.

For a person to have evaluation awareness, he or she must first be aware that his or her performance or actions might be observed either directly or indirectly by others (Griffith 1993). We propose that a user needs to be made aware that both monitoring and evaluating behavior are going to occur, and that this awareness can be raised using UI artifacts. Thus, we propose the following:

H2. *User-interface artifacts that foster expectation of evaluation will decrease intention to commit access policy violations.*

H3. *User-interface artifacts that foster awareness of monitoring will decrease intention to commit access policy violations.*

Social presence is the awareness of others, in our context within a system (Rice 1993). In a review of more than 280 studies, Guerin (1986) found that people change their behavior simply with the passive presence of another, especially when the observer's behavior cannot be watched. We theorize that this same effect will hold within the context of a system. We thus hypothesize:

H4. *User-interface design artifacts that foster awareness of social presence will decrease intention to commit access policy violations.*

MORAL INTENSITY AND IMPULSIVITY

Moral intensity is a theory from the field of ethics that describes the impacts that attributes of a situation have on an individual's ethical decision-making process (Jones 1991). The theory contributes to ethical decision-making theories by reasoning about the context or situation surrounding an ethical decision. The theory proposes that acts in situations high in moral intensity will be more likely to be perceived as being ethical acts. Conversely, if an act is not perceived to be ethical, then it is proposed that an individual will be less likely to engage in ethical cognitive processing (Jones 1991). We reason that a morally intense situation will assist the decision-maker in perceiving the act to be an ethical one, which will help them see more clearly the pro-social acceptable choice. Accordingly:

H5a-d. *Moral intensity amplifies the influence of (a) identifiability, (b) evaluation expectation, (c) awareness of logging, and (d) social presence on intentions to violate organizational access policies.*

Impulsivity, a personality trait, has appeared in multiple forms in academic literature, including urgency, lack of premeditation, lack of perseverance, and sensation seeking (Whiteside and Lynam 2001). The facet of impulsivity of interest in this study is *lack of premeditation*,

which can be defined as the propensity of an individual to act without considering consequences for a given behavior (Whiteside and Lynam 2001). Linking this to accountability theory, an implicit requirement in the mechanism of accountability is that individuals will be held responsible for their actions to an outside party (Lerner and Tetlock 1999), which prompts the individual to systematically process their acts before performing them. However, acting impulsively without consideration of consequences sabotages the systematic processing that would normally prompt feelings of accountability. Thus, we provide the following hypotheses:

> **H6a-d**. *Impulsivity attenuates the influence of (a) identifiability, (b) evaluation expectation, (c) awareness of logging, and (d) social presence on intentions to violate organizational access policies.*

METHODOLOGY

To test our hypotheses, we used the factorial survey method (Jasso 2006), a variation of the scenario method increasingly used to study information security policy violations and computer abuse (D'Arcy et al. 2009). The factorial survey differs from typical scenario-based surveys in that textual elements within the scenario are experimentally varied. This technique combines the large number of factors afforded by field surveys with the control and orthogonality provided by experimental designs. The factorial survey has been called the "gold standard" for accessing ethical beliefs and normative judgments (Seron et al. 2006, p. 931).

To create a factorial survey to test our hypotheses, we used the three scenarios developed in (Vance et al. 2013). Additionally, we developed four graphical UI artifacts corresponding to the effects of (1) identifiability, (2) expectation of evaluation, (3) awareness of monitoring, and (4) social presence. Each of these four artifacts had two levels: visible and not visible. We combined these artifacts to create a factorial of 16 unique graphical vignettes (2x2x2x2). Each

graphical vignette was then superimposed over a screenshot of the actual PeopleSoft login screen (see Figure 2). Each respondent received 4 of the 16 possible combinations of graphical artifacts randomly.

Survey Instrument

Respondents answered demographic questions regarding gender, age, work experience, and their level of impulsivity. In addition, respondents read one of the three scenarios describing an access policy violation. Next, the respondent answered a moral intensity scale to gauge the perceived wrongness of the violation. Finally, the respondent was presented with the instructional scenario again, this time along with one of the four graphical vignettes. As part of this fifth step, the respondent had the opportunity to report his/her intention to act as the character did, given the context provided in the instructional scenario and the UI depicted in the graphical vignette.

Data Collection

Our primary sample consisted of 106 employees with privileged access to a university's Oracle PeopleSoft financial and human resources system, constituting a 29 percent response rate. As is typical with factorial survey designs, the level of analysis was not the participant, but the vignette (Jasso 2006). Thus, since each respondent rated four graphical UI vignettes, the final N for the survey was 424.

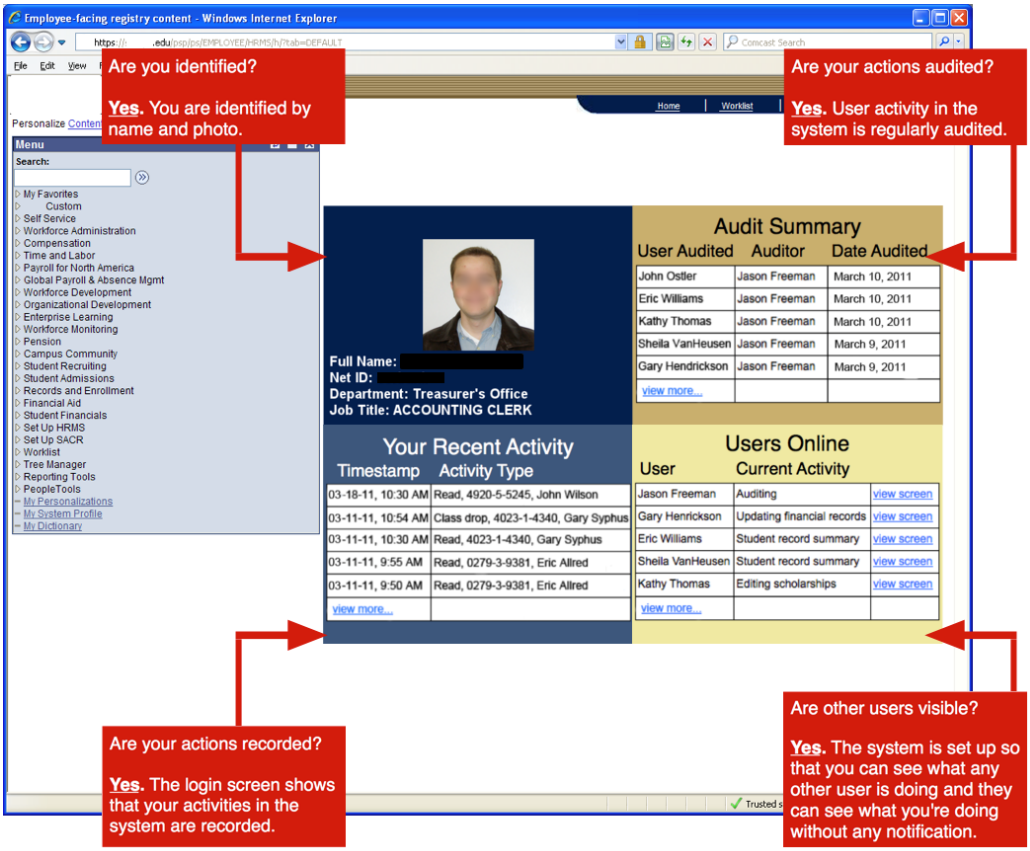

Figure 2. A graphical vignette showing the PeopleSoft UI with accountability mechanisms

Expected Contributions

We expect to contribute by showing how graphical vignettes can be used with the factorial survey method to show the impact that the user interface can have on user perceptions and their intentions. Although we examined how accountability UI artifacts decrease employees' intentions to violate the access policy, this technique could be used to study a range of security behaviors. Second, we expect to show how the influence of the accountability UI artifacts are moderated by moral intensity and impulsivity, two constructs we theorize are especially useful for understanding the threat of organizational insiders.

REFERENCES

D'Arcy, J., Hovav, A., and Galletta, D.F. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1), pp. 79-98.

Geen, R. 1991. "Social Motivation," *Annual Review of Psychology* (42:1991), pp. 377-399.

Griffith, T. 1993. "Monitoring and Performance: A Comparison of Computer and Supervisor Monitoring," *Journal of Applied Social Psychology* (23:1993), pp. 549-572.

Guerin, B. 1986. "Mere Presence Effects in Humans: A Review," *Journal of Experimental Social Psychology* (22:1986), pp. 38-77.

Jasso, G. 2006. "Factorial Survey Methods for Studying Beliefs and Judgments," *Sociological Methods & Research* (34:3), pp. 334-423.

Jones, T. 1991. "Ethical Decision Making by Individuals in Organizations: An Issue-Contingent Model," *The Academy of Management Review* (16:2), pp. 366-395.

Lerner, J.S., and Tetlock, P.E. 1999. "Accounting for the Effects of Accountability," *Psychological Bulletin* (125:2), pp. 255-275.

Rice, R.E. 1993. "Media Appropriateness: Using Social Presence Theory to Compare Traditional and New Organization Media," *Human Communication Research* (19:4), pp. 451-484.

Rubenstein, S. 2008. "Are Your Medical Records at Risk?," *Wall Street Journal (Asia Edition)*, retrieved: May 18, 2013, from http://online.wsj.com/article/SB120941048217350433.html.

Savage, C. 2013. "Soldier Admits Providing Files to Wikileaks," *New York Times*, retrieved: July 20, 2013, from http://www.nytimes.com/2013/03/01/us/bradley-manning-admits-giving-trove-of-military-data-to-wikileaks.html.

Schmitt, E. 2011. "White House Orders New Computer Security Rules," *New York Times*, retrieved: July 27, 2013, from http://www.nytimes.com/2011/10/07/us/politics/white-house-orders-new-computer-security-rules.html.

Sedikides, C., Herbst, K.C., Hardin, D.P., and Dardis, G.J. 2002. "Accountability as a Deterrent to Self-Enhancement: The Search for Mechanisms," *Journal of Personality and Social Psychology* (83:3), pp. 592-605.

Seron, C., Pereira, J., and Kovath, J. 2006. "How Citizens Assess Just Punishment for Police Misconduct," *Criminology* (44:4), pp. 925-960.

Tadmor, C., and Tetlock, P.E. 2009. "Accountability," in *The Cambridge Dictionary of Psychology,* D. Matsumoto (ed.), Cambridge: Cambridge University Press, p. 8.

Vance, A., Lowry, P.B., and Eggett, D. 2013. "Using Accountability to Reduce Access Policy Violations in Information Systems," *Journal of Management Information Systems* (29:4), pp. 263-289.

Whiteside, S.P., and Lynam, D.R. 2001. "The Five Factor Model and Impulsivity: Using a Structural Model of Personality to Understand Impulsivity," *Personality and individual differences* (30:4), pp. 669-689.

Williams, K., Harkins, S., and Latane, B. 1981. "Identifiability as a Deterrent to Social Loafing: Two Cheering Experiments," *Journal of Personality and Social Psychology* (40:1981), pp. 303-311.