Using Accountability Theory to Determine How Curiosity Affects Policy Compliance

Philip Menard
University of Texas at San Antonio
Philip.menard@utsa.edu

Hwee-Joo Kam
University of Tampa
hkam@ut.edu

Dustin K. Ormond
Creighton University
dustinormond@creighton.edu

Robert E. Crossler
Washington State University
rob.crossler@wsu.edu

ABSTRACT

Insider abuse is one of the most dangerous issues facing information security professionals due to employees' existing authorization within organizational systems and knowledge of critical data structures housing confidential information. Although prior research has examined ways to mitigate access policy violations through the implementation of accountability artifacts within systems, employees may still be motivated to violate policies due to their innate curiosity about information that has been withheld from their knowledge. In this paper, we discuss how curiosity may impact the previously demonstrated effects of accountability features on intention to violate policies. We propose a factorial survey design to explore the interaction of curiosity and accountability in determining employees' intentions to violate data access policies.

Keywords: Accountability, curiosity, security compliance, factorial survey method.

INTRODUCTION

Information security managers continually face the threat of insider abuse, or the violation of organizational trust as perpetrated by employees who have abused their authorized privileges (Willison and Warkentin 2013). A typical example of insider abuse is the violation of access policies, which takes place when an employee accesses confidential data in a manner that is counter to standard operating procedures (Ward and Smith 2002; Zhao and Johnson 2010). Employees violate access policies for a number of reasons, such as fraud, the sale of personally identifiable information (PII) on black market websites, or procuring trade secrets (Rubenstein and Francis 2008; Schmitt 2011).

One mechanism security managers may use to combat access policy violations among users with elevated privileges is the incorporation of user accountability within computerized systems. Security professionals typically integrate accountability in their systems through non-repudiation protections, often known as AAA considerations (authentication, authorization, and auditing). However, these countermeasures often occur in the background, and employees may not be aware of the level to which their behavior within the system is being logged. Employees' awareness and perceptions of these features may actually drive their intention to violate access policies. The notion of perceived accountability has been extensively studied in psychology and organizational behavior (Lerner and Tetlock 1999; Sedikides et al. 2002), and more recently in information security (Vance et al. 2013).

However, recent findings have demonstrated that a employees' innate curiosity may lead them to violate access policies despite being aware of their organization's accountability measures. One survey found that curiosity led 34% of users to click on a malicious link (Benenson 2016). Curiosity specifically led to unauthorized access at the Orlando Regional Medical Center when

employees illegally accessed medical records of survivors of the Pulse nightclub mass shooting, prompting resentment expressed by the LGBT Center of Central Florida (Grant 2016). In another recent example, a caregiver employed by the St. Charles healthcare system cited curiosity as the reason for accessing 2,459 patients' records without authorization (Spurr 2017). We argue that human curiosity, derived from a perception of a lack of knowledge (Loewenstein 1994), may supersede perceptions of accountability derived from information security design artifacts and lead employees to violate access policies anyway.

These recent events demonstrate that a gap exists in extant accountability and compliance research. Even when possessing the knowledge of how their organization will hold them accountable for their access of organizational records, employees still succumb to their innate curiosity and ultimately violate company policies. Hence, our research question is:

> *RQ: How does human curiosity interact with employees' perceptions of accountability in influencing policy compliance intention?*

LITERATURE REVIEW AND HYPOTHESIS DEVELOPMENT

Accountability Theory

To build the argument for the development of our research model, we must first understand how users' perceptions of certain systems features can lead to their perception of increased user accountability within the systems and ultimately to intention to comply with organizational ISPs. Based on the Vance et al. (2013) adaptation of Accountability Theory to the IS domain, accountability perceptions are formed by four IS design artifacts – identifiability, monitoring, evaluation, and social presence. These factors are described in detail in the following subsections.

Identifiability

Identifiability is defined as one's "knowledge that his outputs could be linked to him" (Williams et al. 1981, p. 309). Identifiability fosters perceptions of accountability because it

emphasizes that a person's behaviors can be attributed to him or her (Lerner and Tetlock 1999). When an individual perceives that his or her actions are identifiable, the individual is more prone to perform actions for which he or she would take responsibility. In security situations, the implementation of identifiability features should result in elevated perceptions of accountability among users.

> *H1: User-interface design artifacts that promote identifiability will decrease access policy violation intention.*

Monitoring

Monitoring is the act of recording someone's actions (Boss et al. 2009; Griffith 1993). In the information security domain, monitoring has been shown to increase policy compliance (Boss et al. 2009; Herath and Rao 2009). However, monitoring is only useful as a compliance mechanism when details of how monitoring occurs are articulated in the ISP (Boss et al. 2009; Kirsch 2004). Therefore, if an employee is aware of the monitoring features built into their organizational systems they will be less likely to violate policies related to information access.

> *H2: User-interface design artifacts that promote monitoring awareness will decrease access policy violation intention.*

Evaluation

Evaluation is one's awareness that his or her performance will be reviewed based on preconceived norms, implicitly resulting in consequences (Lerner and Tetlock 1999). Awareness of evaluation leads to performance of more socially acceptable behaviors (Hochwarter et al. 2007; Lerner and Tetlock 1999) and fewer unacceptable actions (Sedikides et al. 2002). This occurs due to evaluation apprehension, defined as the anxiety associated with the approval or disapproval of one's actions as judged by others (Geen 1991). When experiencing evaluation apprehension, one's self-awareness is elevated such that incongruencies between socially acceptable standards and

one's own behaviors are emphasized (Sedikides et al. 2002). In such a state, an individual will perform behaviors that match social norms and avoid actions that would damage his or her social standing (Baumeister 1982).

> *H3: User-interface design artifacts that promote evaluation awareness will decrease access policy violation intention.*

Social Presence

Social presence is defined as the knowledge of others' presence in computer-mediated situations (Rice 1993; Walther 1992). Although social presence was originally conceptualized around active and consistently engaged communication (Rice 1993; Walther 1992), Lerner and Tetlock empirically demonstrated that even just the presence of another who is not actively participating in ongoing communication still influences perceptions of accountability (Lerner and Tetlock 1999). Lowry et al. (2009) showed that social presence improved productivity, even when group participants were anonymous. This provides evidence that social presence can shape perceptions of accountability in not just face-to-face interactions, but in computer-mediated situations as well.

> *H4: User-interface design artifacts that promote awareness of social presence will decrease access policy violation intention.*

Human Curiosity Theory

One common reason an employee may violate an access policy is curiosity about confidential data. Although curiosity has been shown to have a positive effect on the effectiveness of security education training and awareness (SETA) program (Silic and Lowry forthcoming), curiosity may also drive employees toward accessing unauthorized information. Research indicates that curiosity may derive from perceptions of information deprivation (Litman 2005; Litman and Jimerson 2004; Loewenstein 1994). This type of curiosity begins with feelings of

anxiety, irritation, or displeasure and ultimately leads individuals toward a desire to know more (Berridge 1999; Berridge and Robinson 1998). Curiosity derived from deprivation elicits stronger emotions than curiosity as derived from interest in a subject matter area (Litman and Jimerson 2004).

Curiosity arises when an individual perceives a gap between the information forming his or her own understanding of a subject and the amount of accessible information related to that subject (Loewenstein 1994). Because curiosity elicits information seeking (Litman and Jimerson 2004; Loewenstein 1994), curiosity has the potential to negate the intended effects of the accountability features built into an organizational system. We posit that employees' perceptions of curiosity will interact with their perceptions of system accountability, such that as perceptions of curiosity rise, the effects of the various accountability system features on intention to violate will weaken. Conversely, if an employee is not particularly curious about a piece of confidential data, the employee is more likely will acknowledge the accountability features and be less likely to violate access policies.

H5a-d: Curiosity will weaken each design artifact's effect on access policy violation intention.

Using similar rationale as our previous hypothesis, perceptions of curiosity may also have a direct effect on intention to violate access policies, independent of accountability features built into the system. If an employee is curious enough about a piece of data, the employee will acknowledge the accountability features but violate the access policy anyway in an effort to satisfy his or her desire to know more information. In other words, the employee's innate curiosity will drive the intention to violate the policy, superseding perceptions of system accountability features.

H6. Curiosity will positively affect access policy violation intention.

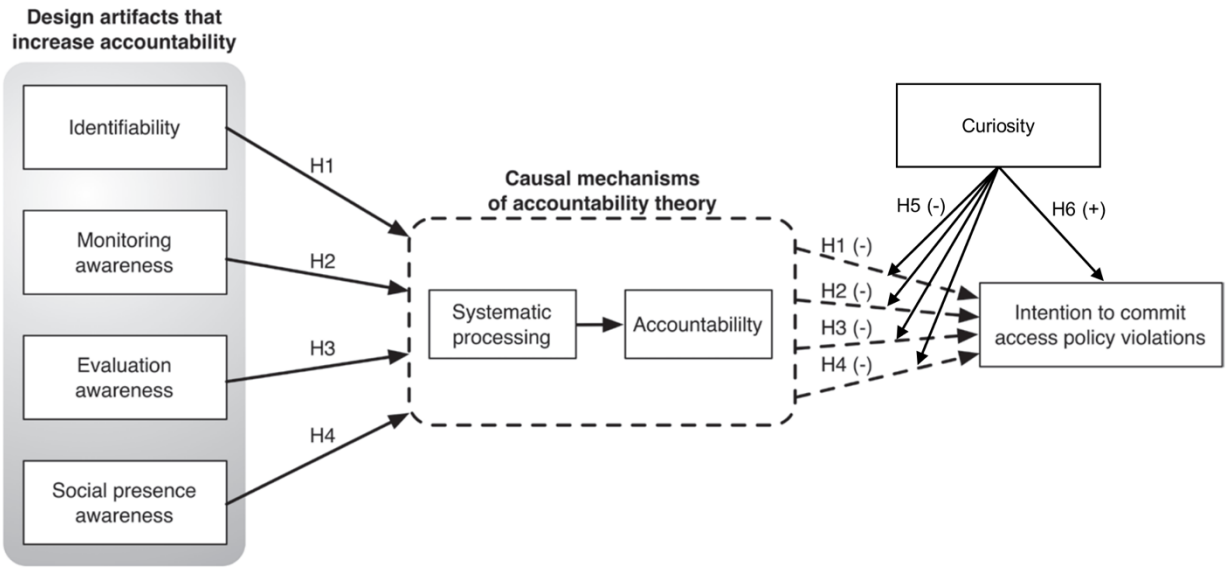

Figure 1. Research Model, adapted from Vance et al. (2013)

METHODS

To examine the influence of curiosity on individuals' perceptions of accountability and their intention to violate access policies, we will use a factorial survey design (Chatterjee et al. 2015; Vance et al. 2013). Within each scenario, a respondent will be shown a random combination of statements, where each statement is designed to bolster the respondent's perception of the research model's independent variables. This design will allow us to examine the individual influence, as well as interactions, of each independent variable on intention. Our model contains four independent variables (identifiability, monitoring, evaluation, social presence – see Figure 1). Additionally, we are capturing whether an explicit acknowledgment of policy awareness within the scenario impacts intention to violate. Thus, there are five possible manipulation statements that may be embedded in the scenario. This scenario design results in 2^5, or 32, possible combinations of statements to be embedded in the scenario. For more details on the construction of our scenarios, please see Appendix A.

Sampling Frame and Scenario Contextualization

Because we are analyzing the impact of curiosity on an individual's willingness to violate access policies, the appropriate respondent for our study will be an end user who has access to information at their organization that would otherwise be confidential to the public. We will solicit respondents from Qualtrics, whose platform we will also use for hosting the survey instrument. Following the survey design implemented by Vance et al. (2013), our scenarios also depict situations in which the scenario character has access to important information and decides to violate their access policy.

Instrument Design

First, we will ask respondents about their gender identification; this will allow us to embed the corresponding pronoun within our scenarios to better position our respondent to see themselves in the role of the scenario character (we will also use gender neutral names for the scenario characters – see Appendix A). Respondents will then be presented with each of the three base scenarios in random order. The scenario will contain random manipulations of each of the statements representing our independent variables. After the respondent reads each scenario, the respondent will report the likelihood that he or she would behave in the same way as the scenario character using a 10-point slider scale, where 10 is "extremely likely" and 0 is "not likely at all". Following the slider scale, we will ask the respondent a series of attention check questions to ensure the respondent read the scenario carefully and properly recognized the manipulations featured in the scenario. To ensure our scenarios are adequately realistic and reflect situations that employees may actually face at work, we will also ask respondents to rate the realism of each scenario. After respondents cycle through all three scenarios and associated measurement items,

we will present them with a measurement scale for curiosity, followed by demographic questions, including age, gender, ethnicity, and years of computing experience.

DATA ANALYSIS

To assess the effects of accountability and curiosity on intention to violate access policies, we will analyze our data using IBM SPSS 26 to conduct a series of MANOVA analyses. We will also employ multilevel model (MLM) analysis using the R package lavaan (version 0.6-5), which allows for multilevel structural equation modeling. This technique is necessary due to our inclusion of a latent construct (curiosity) in the research model. MLM is also more appropriate for analyzing factorial survey data where respondents are shown multiple scenarios in one data collection setting (Otondo et al. 2018).

CONCLUSION

Insider abuse will continue to be a serious problem for organizations. Understanding the mechanisms, both cyber-based and psychological, that improve or impede policy compliance is crucial in combating further organizational information loss.

REFERENCES

Baumeister, R. F. 1982. "A Self-Presentational View of Social Phenomena," *Psychological Bulletin* (91:1), pp. 3-26.

Benenson, Z. 2016. "Exploiting Curiosity and Context: How to Make People Click on a Dangerous Link Despite Their Security Awareness." from https://paper.seebug.org/papers/Security Conf/Blackhat/2016/us-16-Benenson-Exploiting-Curiosity-And-Context-How-To-Make-People-Click-On-A-Dangerous-Link-Despite-Their-Security-Awareness-wp.pdf

Berridge, K. C. 1999. "Pleasure, Pain, Desire, and Dread: Hidden Core Processes of Emotion,").

Berridge, K. C., and Robinson, T. E. 1998. "What Is the Role of Dopamine in Reward: Hedonic Impact, Reward Learning, or Incentive Salience?," *Brain research reviews* (28:3), pp. 309-369.

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* (18:2), pp. 151-164.

Chatterjee, S., Sarker, S., and Valacich, J. S. 2015. "The Behavioral Roots of Information Systems Security: Exploring Key Factors Related to Unethical It Use," *Journal of Management Information Systems* (31:4), pp. 49-87.

Geen, R. G. 1991. "Social Motivation," *Annual review of psychology* (42:1), pp. 377-399.

Grant, M. 2016. "Ormc Blames 'Personal Curiosity' for Pulse Survivor Data Breach." from https://www.wesh.com/article/ormc-blames-personal-curiosity-for-pulse-survivor-data-breach-1/4451797#

Griffith, T. L. 1993. "Monitoring and Performance: A Comparison of Computer and Supervisor Monitoring 1," *Journal of Applied Social Psychology* (23:7), pp. 549-572.

Herath, T., and Rao, H. R. 2009. "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness," *Decision Support Systems* (47:2), pp. 154-165.
Hochwarter, W. A., Ferris, G. R., Gavin, M. B., Perrewé, P. L., Hall, A. T., and Frink, D. D. 2007. "Political Skill as Neutralizer of Felt Accountability—Job Tension Effects on Job Performance Ratings: A Longitudinal Investigation," *Organizational Behavior and Human Decision Processes* (102:2), pp. 226-239.
Kirsch, L. J. 2004. "Deploying Common Systems Globally: The Dynamics of Control," *Information systems research* (15:4), pp. 374-395.
Lerner, J. S., and Tetlock, P. E. 1999. "Accounting for the Effects of Accountability," *Psychological bulletin* (125:2), p. 255.
Litman, J. 2005. "Curiosity and the Pleasures of Learning: Wanting and Liking New Information," *Cognition & emotion* (19:6), pp. 793-814.
Litman, J. A., and Jimerson, T. L. 2004. "The Measurement of Curiosity as a Feeling of Deprivation," *Journal of personality assessment* (82:2), pp. 147-157.
Loewenstein, G. 1994. "The Psychology of Curiosity: A Review and Reinterpretation," *Psychological bulletin* (116:1), pp. 75-98.
Lowry, P. B., Romano, N. C., Jenkins, J. L., and Guthrie, R. W. 2009. "The Cmc Interactivity Model: How Interactivity Enhances Communication Quality and Process Satisfaction in Lean-Media Groups," *Journal of Management Information Systems* (26:1), pp. 155-196.
Otondo, R. F., Crossler, R. E., and Warkentin, M. 2018. "Ranking Factors by Importance in Factorial Survey Analysis," *Communications of the Association for Information Systems* (42:8), pp. 183-232.
Rice, R. E. 1993. "Media Appropriateness: Using Social Presence Theory to Compare Traditional and New Organizational Media," *Human communication research* (19:4), pp. 451-484.
Rubenstein, S., and Francis, T. 2008. "Are Your Medical Records at Risk?," *Wall Street Journal* (251:100), pp. D1-D2.
Schmitt, E. 2011. "White House Orders New Computer Security Rules," *New York Times*).
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), p. 592.
Silic, M., and Lowry, P. B. forthcoming. "Using Design-Science Based Gamification to Improve Organizational Security Training and Compliance," *Journal of Management Information Systems*).
Spurr, K. 2017. "St. Charles: 2,500 Patient Records Accessed in Privacy Breach." from https://www.bendbulletin.com/localstate/st-charles-patient-records-accessed-in-privacy-breach/article_3e2d34d0-8bfc-5b66-b708-9f210453070d.html
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. 263-290.
Walther, J. B. 1992. "Interpersonal Effects in Computer-Mediated Interaction: A Relational Perspective," *Communication research* (19:1), pp. 52-90.
Ward, P., and Smith, C. L. 2002. "The Development of Access Control Policies for Information Technology Systems," *Computers & Security* (21:4), pp. 356-371.
Williams, K., Harkins, S. G., and Latané, B. 1981. "Identifiability as a Deterrant to Social Loafing: Two Cheering Experiments," *Journal of Personality and Social Psychology* (40:2), pp. 303-311.
Willison, R., and Warkentin, M. 2013. "Beyond Deterrence: An Expanded View of Employee Computer Abuse," *MIS Quarterly* (37:1), pp. 1-20.
Zhao, X., and Johnson, M. E. 2010. "Managing Information Access in Data-Rich Enterprises with Escalation and Incentives," *International Journal of Electronic Commerce* (15:1), pp. 79-112.

APPENDIX A

Scenario Implementation

Manipulation Statements

Identifiability Statements:

- Low - Users can use the system without logging in because all users share the same user ID.
- High - Users sign into the system using a unique user ID. The welcome screen displays the user's actual full name.

Monitoring Statements:

- Low - There is no indication that activities in the system are recorded.
- High - The login screen warns that the user's activities in the system will be recorded. Users can click to view a history of all their activity in the system. In addition, when a user is about to perform an action in the system, a notification message warns that the current action will be logged with the user ID.

Evaluation Statements:

- Low - There is no indication that audits of user activity will be performed.
- High - All user activity in the system is comprehensively audited, according to a warning on the login screen.

Social Presence Statements:

- Low - The user cannot see what other users are doing in the system.
- High - The system is set up so that a user can see what other users are doing and vice versa without any notification.

Explicit Policy Awareness Statements:

- Low - [He/She]
- High - Although [character name] believes doing so may be a violation of university policy, [he/she]

Gender Neutral Scenario Character names: Avery, Riley, Jordan

Base Scenarios

Base Scenario 1

[Character name] is a university employee with access to a student financial records system. [He/She] is approached by a supervisor of a computer support department who has noticed that some office equipment has gone missing. In looking over purchase reports involving the department purchase card, the supervisor discovered that certain goods purchased are no longer in the office. Any student employee can check out the purchase card to use it to run errands to the bookstore, but it appears one student has had more discrepancies than others. The supervisor thinks that a student employee is returning these items without a receipt in order to get credit on a signature card. He asks [Character name] to access this student's record in the financial accounts system in order to get things straightened out.

[Identifiability statement] [Monitoring statement] [Evaluation statement] [Social presence statement]

[Explicit policy awareness statement] accesses the student employee's record.

Base Scenario 2

[Character name] is a university employee with access to a student financial records system. [He/She] is approached by a reporter from a local newspaper who is writing an article about student school expenses. The reporter says he has general information about tuition and housing costs, published by the university, but he is interested in diving a little deeper. He asks [Character name] to give him some reports about loans, scholarships, and general account purchases made by students. He says he doesn't need any names or student IDs, just the numbers.

[Identifiability statement] [Monitoring statement] [Evaluation statement] [Social presence statement]

[Explicit policy awareness statement] looks up several records and provides the information to the reporter.

Base Scenario 3

[Character name] is a university employee with access to a student financial records system. [He/She] is approached by a friend who has a son attending college who has been living independently for a few years. The friend has asked her son a few times about his financial situation, but he has been repeatedly vague. The friend is concerned that he is going too much into debt to pay for his education. She asks [Character name] to look up his financial aid situation to see if her concern is founded.

[Identifiability statement] [Monitoring statement] [Evaluation statement] [Social presence statement]

[Explicit policy awareness statement] looks up the financial record of the friend's son.

Example Scenario with all low manipulations

Avery is a university employee with access to a student financial records system. She is approached by a supervisor of a computer support department who has noticed that some office equipment has gone missing. In looking over purchase reports involving the department purchase card, the supervisor discovered that certain goods purchased are no longer in the office. Any student employee can check out the purchase card to use it to run errands to the bookstore, but it appears one student has had more discrepancies than others. The supervisor thinks that a student employee is returning these items without a receipt in order to get credit on a signature card. He asks Avery to access this student's record in the financial accounts system in order to get things straightened out.

Users can use the system without logging in because all users share the same user ID. There is no indication that activities in the system are recorded. There is no indication that audits of user activity will be performed. The user cannot see what other users are doing in the system.

She accesses the student employee's record.

Example scenario with all high manipulations

Avery is a university employee with access to a student financial records system. She is approached by a supervisor of a computer support department who has noticed that some office equipment has gone missing. In looking over purchase reports involving the department purchase card, the supervisor discovered that certain goods purchased are no longer in the office. Any student employee can check out the purchase card to use it to run errands to the bookstore, but it appears one student has had more discrepancies than others. The supervisor thinks that a student employee is returning these items without a receipt in order to get credit on a signature card. He asks Avery to access this student's record in the financial accounts system in order to get things straightened out.

Users sign into the system using a unique user ID. The welcome screen displays the user's actual full name. The login screen warns that the user's activities in the system will be recorded. Users can click to view a history of all their activity in the system. In addition, when a user is about to perform an action in the system, a notification message warns that the current action will be logged with the user ID. All user activity in the system is comprehensively audited, according to a warning on the login screen. The system is set up so that a user can see what other users are doing and vice versa without any notification.

Although Avery believes doing so may be a violation of university policy, she accesses the student employee's record.