Association for Information Systems
AIS Electronic Library (AISeL)

MWAIS 2016 Proceedings

Midwest (MWAIS)

Spring 5-19-2016

Moral Beliefs and Organizational Information Security Policy Compliance: The Role of Gender

Gaurav Bansal
University of Wisconsin – Green Bay, bansalg@uwgb.edu

Kayla Hodorff
University of Wisconsin – Green Bay, hodok31@uwgb.edu

Kyle Marshall
University of Wisconsin – Green Bay, marskl14@uwgb.edu

Moral Beliefs and Organizational Information Security Policy Compliance: The Role of Gender

Gaurav Bansal
University of Wisconsin – Green Bay
bansalg@uwgb.edu

Kayla Hodorff
University of Wisconsin – Green Bay
hodok31@uwgb.edu

Kyle Marshall
University of Wisconsin – Green Bay
marskl14@uwgb.edu

ABSTRACT

Data breaches are a continuing problem for managers in the digital age. Currently, there is very little guidance available to companies and managers in particular on how to mitigate data breach risks arising due to malicious or negligent insiders. This study examines the factors impacting employees' intentions to violate an organization's information systems (IS) security policies – using hypothetical scenarios. Specifically, the research attempts to understand the role of gender on the relationship between moral beliefs, understandability of the security policy, underlying moral issue (necessity vs. metaphor of the ledger), and intentions to violate the security policy. Our results suggest that moral beliefs and understandability of the security policy lower intentions to violate the policy, and do so differently depending upon one's gender and the underlying moral issue. Data was gathered from 173 students using an online survey tool, and analyzed using multiple regression. We examined regression assumptions and found no major issues. The study has several practical and theoretical implications. The findings suggest that using ethical and gender perspectives provide additional insight into IS security non-compliance issues. The findings could help IS security managers as they develop effectual security policies and devise more effective training programs.

Keywords

Security compliance, ethics, gender, neutralization

INTRODUCTION

Computer security has been identified as a national threat and has assumed vast proportions such that President Obama has decided to fund a $19 billion initiative on Feb 9, 2016 to counter the computer security threat (Wall Street Journal). It is widely believed that human agents inside an organization could be more dangerous than those outside the organization because of their intimate knowledge of the system and privilege of access (Siponen et al. 2010). Such acts of human agents may be intentional such as sabotage or they may be unintentional or accidental such as forgetting to change passwords (Warkentin et al. 2009). Threat from insiders invariably increases when employees do not comply with organizations' IS security policies and procedures (Pahnila et al. 2007). In Information Systems (IS) literature security policy violations have been examined with multiple theoretical perspectives such as deterrence theory (rewards and punishment), criminology and neutralization, fear and threat appraisal, information security awareness and training, theory of cognitive moral development, social bonding and influence among others - refer to Sommestad et al. (2014) for a detailed review.

IS security policy compliance literature has so far has given limited attention to examining the compliance intentions explicitly from an ethical perspective – with exception of studies such as Myyry et al. (2009) who have examined non-compliance using cognitive moral development and theory of motivational types of values. Research shows that males and females have differences in ethical values and that they behave differently in ethical situations (Adam et al. 2000; Khazanchi 1995; Kreie et al. 1998; Peslak 2008). Gender social role (Franke et al. 1997) theory suggests that there are pre-career gender differences between male and females (socialization theory), however these differences diminish over time due to organizational structures and routines (structural theory). It is important to examine gender differences in IS security compliance intentions. First, there are limited studies in the IS area which have examined the role of gender in security policy compliance. Second, the studies which examined gender differences have used gender mostly as a direct control (e.g., Barlow et al. 2013; Siponen et al. 2010; Vance et al. 2012). Third, prior research mostly reports no significant gender differences on IS security compliance – except for some studies such as Ifined (2014). Hovav et al. (2012) also report no gender differences in the US sample they examined.

Thus, in this paper we study gender differences in security policy compliance using ethical perspective. Highlighting the importance of examining gender and ethics (Adam et al. 2000) noted that "much decision making in relation to computer technologies takes place within the workplace, therefore gender studies within business ethics and information systems are relevant" (p 18). Our literature search in this area (Table 1) shows that examination of gender and ethics in IS in general and security policy compliance in particular is still "undertheorized and underexplored" (Adam et al. 2000) (p 46).

Specifically, in this research we examine the role of gender on the relationship between moral beliefs, understandability, and the intentions to violate the IS security policy. The research model is inspired by Jones (1991) issue-contingent model of ethical decision making in organizations. According to Jones (1991), the moral decision making process begins with a problem which includes a moral component. This moral component can be characterized in terms of its moral intensity which is comprised of six factors - magnitude of consequences, social consensus, probability of effect, temporal immediacy, proximity and concentration of effect. These factors affect the ethical decision making process through their impact on the individual's recognition of the consequences of decisions. Using Prospect Theory (Kahneman et al. 1979) we argue that the recognition of the six moral factors would be perceived differently by individuals based on their experiences, preferences, underlying ethical lens (teleological, deontological, or feminist among others), and gender.

The paper is structured as follows. We provide a literature review, followed by the research model and hypothesis development. Subsequently, research method and data analysis are presented. Results are summarized in the following section. The paper concludes by providing discussion of the findings and implications.

LITERATURE REVIEW

Following table presents a summary of the salient research in IS pertaining to (a) gender and ethics, and (b) gender and IS security compliance. As evident IS literature has not adequately addressed the issue of gender and ethics, and there are mixed findings pertaining to the impact of gender on IS security policy compliance.

Literature Pertaining to *Gender and Ethics* in IS			
Paper	**Methodology**	**Sample Characteristics**	**Findings**
Peslak (2008)	Questionnaire with 12 statements	304 students and faculty/staff	Gender affected ethical decisions.
Adam et al. (2000)	Respondents were interviewed using scenarios	12 men and 12 women	Men and women differ in their ethical decision making process.
Kreie et al. (1998)	Used a set of five scenarios to judge differences between ethical considerations of men and women	307 IS students	There are gender differences in ethical assessments. Found that women have higher ethical standards.
Khazanchi (1995)	Survey containing seven scenarios	134 students	Gender differences vary depending upon the nature of the ethical dilemma.
Gender and IS Security Compliance			
Ifined (2014)	Field survey	68 non-IS managers in Canadian organizations	Females had significantly higher security compliance intentions.
Barlow et al. (2013)	Factorial survey method using scenarios. Each respondent answered questions pertaining to 4	Used 257 usable responses.	Gender did not have an effect on intentions to violate.

	scenarios (out of total 36 possible scenarios)		
Vance et al. (2012)	Six hypothetical scenarios and survey questions (respondents answered all six scenarios)	210 respondents from Finnish Municipal Organization	Found no differences in compliance based on gender.
Hovav et al. (2012)	Four IS misuse scenarios and survey questions (respondents answered all four scenarios)	269 from US, 145 from South Korea	There were no gender difference in the US sample. However, Korean females were found less likely to engage in IS misuse.
Siponen et al. (2010)	Each participant was randomly given one of three scenarios	Administrative personnel from three organizations in Finland	Gender did not have an effect on intentions to violate.

Table 1. Review of Salient Studies Pertaining to (a) Gender and Ethics and (b) Gender and Security Compliance in IS Literature

THEORY DEVELOPMENT AND RESEARCH MODEL

The research model is shown in figure 1, and discussed below.

Moral Beliefs: Moral beliefs refer to the degree to which a prohibited act is perceived to be morally offensive (D'Arcy et al. 2011). Prior research shows that moral beliefs have a strong negative influence on various unlawful behaviors such as corporate crime (D'Arcy et al. 2011). Hence,

> *H1: Moral beliefs are negatively associated with the IS security policy non-compliance intentions.*

Understandability of the security policy: IS security policy training and education helps ensure employee internalization on the importance of IS security policy compliance (Puhakainen et al. 2010). Understandability of the policy would influence perceived moral intensity factors such as magnitude of consequences and social consensus, and to some degree other factors as well such as concentration of effect, temporal immediacy, probability of effect, and proximity. Hence,

> *H2: Security policy understandability is negatively associated with the IS security policy non-compliance intentions.*

Moderating role of Gender: Women are more risk averse (Chung et al. 2003). So given the same degree of ethical beliefs, it can be argued that women will have higher compliance as opposed to men.

> *H3a: Gender has a moderating impact on the relationship between moral beliefs and non-compliance intentions such that moral beliefs have a stronger negative impact on non-compliance intentions for females as opposed to males.*

We use the following three arguments to hypothesize that gender would moderate the relationship between understandability of security policy and compliance.

1. Understanding of the security policy would help one to internalize the communal benefits of following IS security (Chung et al. 2003). Based on gender socialization theory we argue that in general females as opposed to men are persuaded more by normative appeals pertaining to the communal benefits (Chung et al. 2003).
2. Research in cognitive Psychology area shows that women are more risk averse relative to men (Chung et al. 2003), and hence are likely to have higher compliance intentions.
3. Research in criminal justice literature reports that men are more likely to engage in criminal activities than women are (Chung et al. 2003). Hence it could be argued:

H3b: Gender has a moderating impact on the relationship between understandability of the security policy, and IS security policy non-compliance intentions such that understandability has a stronger negative impact on non-compliance intentions for females as opposed to males.

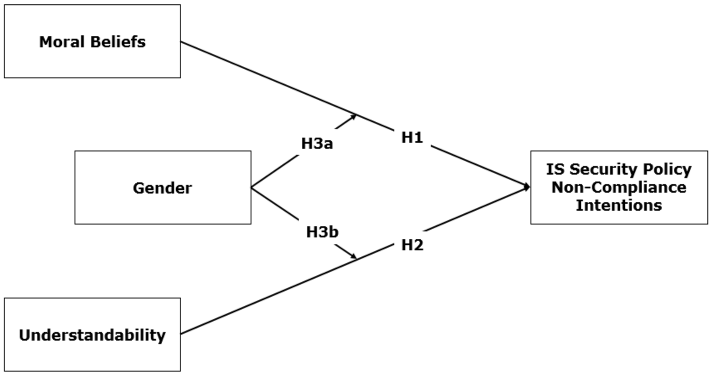


Figure 1. Research Model

RESEARCH METHOD

Data was collected using an online survey mechanism. We crafted a hypothetical security policy, and two scenarios (Necessity - NEC and Metaphor of the Ledger - MOL) to measure IS security policy non-compliance. Scenarios help to get true responses from participants about intentions to violate policies and also control for extraneous variables (Siponen et al. 2010). We asked three manipulation check questions to ensure that participants were paying attention to the scenarios presented in the study. Items were operationalized based on the existing literature - Neutralization scenario: (Siponen et al. 2010); Understandability (Bansal et al. 2008); Noncompliance Intentions (Liang et al. 2013) ; Moral beliefs (Vitell et al. 2005). Data analysis was carried out using SPSS. We excluded the respondents who did not answer the manipulation check questions correctly. After cleaning, we had a total of 231 responses - some respondents viewed 2 scenarios, and some viewed only 1. Thus, there were 173 unique respondents – 77 males and 96 females. Males had average age of 23.12 years (std. dev. 3.61 yrs.), females had average age of 22.91 years (std. dev. 5.60 yrs.). We conducted exploratory factor analysis and found no issues. Hypotheses were testing using multiple linear regressions. We examined regression assumptions (Fig. 2) and found no issues. Hypotheses 1 and 2 were tested together in one regression (shown in figure 3a), while hypotheses 3a and 3b were tested by creating two different regression models separately for females and males and comparing the H1 and H2 path significance across the two regressions (shown in figure 3b).

Results

Results show that H1 was supported at $p < 0.001$ level and H2 was supported at $p < 0.05$ level. The results show that moral beliefs (H1) and understandability of the security policy (H2) significantly lower intentions to violate (INT) the IS security policy. Results show that H3b was supported, whereas H3a was not supported. Gender impacts relationship between understandability and INT (H3b), and has no overall moderating impact on the relationship between moral beliefs and INT (3a). We further examined 3a and 3b by analyzing four different regressions – NEC (F), NEC (M), MOL (F), MOL (M) (Fig. 4). The post-hoc analysis shows that gender impacts H1 and also H2 depending upon the underlying neutralization scenario – NEC or MOL. Whereas in the overall results we found no moderating impact of gender on H1 – the post-hoc analysis shows that there is a moderating role of gender, such that H1 and H2 are significant for both males and females for NEC scenario, however in MOL, both H1 and H2 are significant only for females and not for males. Even though the results show a significant moderating gender impact on non-compliance intentions, the direct control effect as noted in Fig 3a shows non-significance.

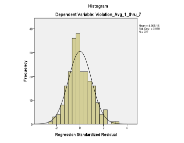
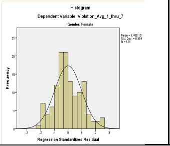
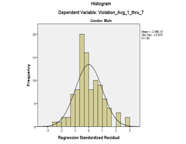
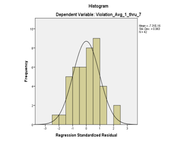
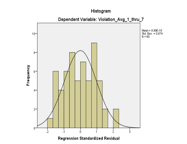
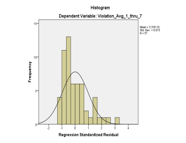
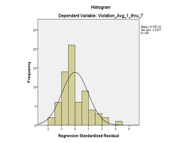
Overall	Females Only	Males Only	NEC (M)	NEC (F)	MOL (M)	MOL (F)
						

Figure 2a. Regression Assumptions (Normality)

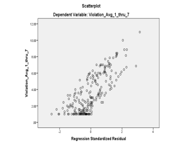
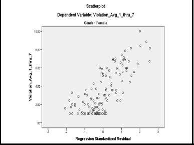
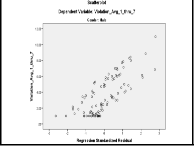
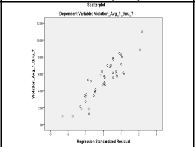
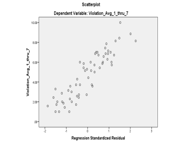
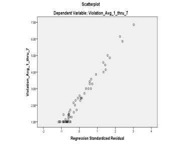
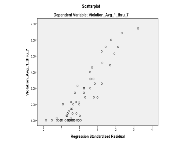
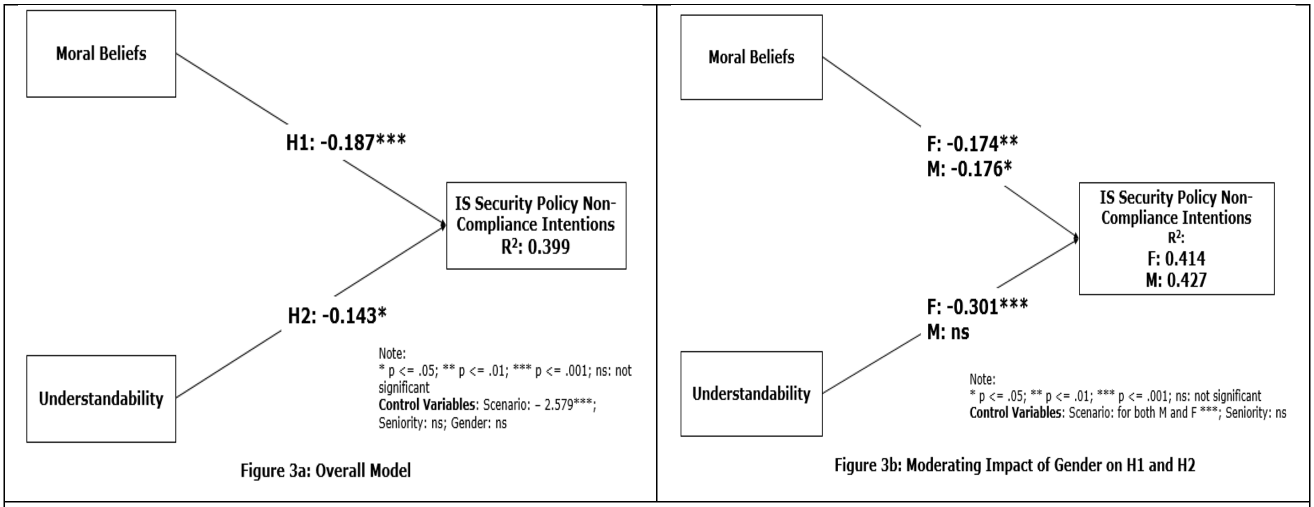
Overall	Females Only	Males Only	NEC (M)	NEC (F)	MOL (M)	MOL (F)
						

Figure 2b. Regression Assumptions (Linearity and Equal Variance)

<>



Note:
* p <= .05; ** p <= .01; *** p <= .001; ns: not significant
Control Variables: Scenario: – 2.579***; Seniority: ns; Gender: ns

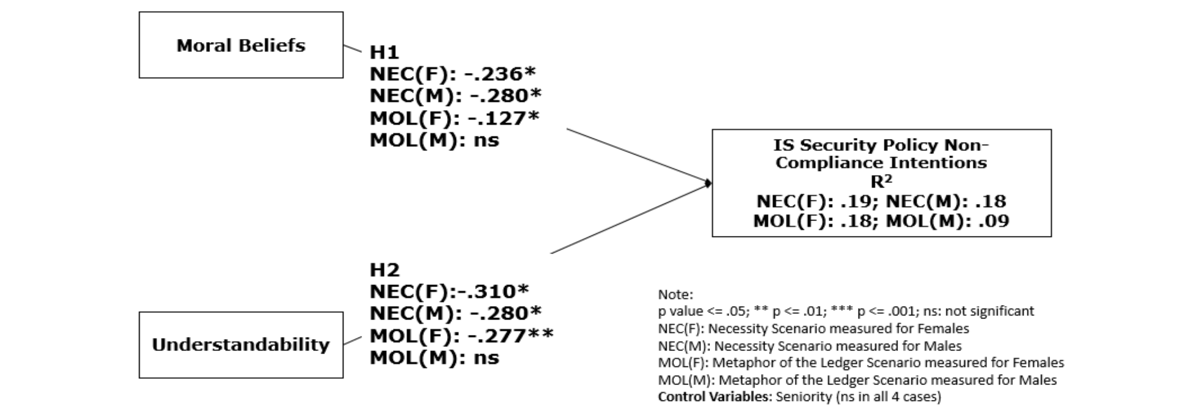
Figure 3a: Overall Model

Note:
* p <= .05; ** p <= .01; *** p <= .001; ns: not significant
Control Variables: Scenario: for both M and F ***; Seniority: ns

Figure 3b: Moderating Impact of Gender on H1 and H2

Figure 3. Result

<>



Note:
p value <= .05; ** p <= .01; *** p <= .001; ns: not significant
NEC(F): Necessity Scenario measured for Females
NEC(M): Necessity Scenario measured for Males
MOL(F): Metaphor of the Ledger Scenario measured for Females
MOL(M): Metaphor of the Ledger Scenario measured for Males
Control Variables: Seniority (ns in all 4 cases)

Figure 4: Moderating Role of Gender and Scenario

Figure 4. The Post-hoc analysis (Results from 4 different Regressions)

DISCUSSION

The paper shows that gender impacts IS security policy non-compliance intentions, and the effect varies according to the underlying rationale (necessity or metaphor of the ledger). The results show that males are probably more "immersed" by MOL that both moral beliefs and understandability have limited effect on them in lowering non-compliance intentions. The results show that males and females have different ethical perspectives when dealing with the moral component of IS security policy non-compliance. The paper makes several contributions. First, it helps explain inconsistencies in the prior research pertaining to the role of gender on IS security compliance. It shows that gender has a moderating impact (and not a direct impact) on IS security compliance intentions – such that gender influences security compliance indirectly by affecting the relationships between antecedents and non-compliance intentions. Second, this research shows that gender impacts the relationship between antecedents and non-compliance intentions differently based on the underlying neutralization scenario. The findings could help IS security managers in framing effective security policies and training programs.

REFERENCES

Adam, A., and Ofori-Amanfo, J. 2000. "Does gender matter in computer ethics?," *Ethics and Information Technology* (2:1), pp 37-47.

Bansal, G., Zahedi, F. M., and Gefen, D. 2008. "The moderating influence of privacy concern on the efficacy of privacy assurance mechanisms for building trust: A multiple-context investigation," *Twenty Ninth International Conference on Information Systems*, Paris, France.

Barlow, J. B., Warkentin, M., Ormond, D., and Dennis, A. R. 2013. "Don't make excuses! Discouraging neutralization to reduce IT policy violation," *Computers & security* (39), pp 145-159.

Chung, J., and Trivedi, V. U. 2003. "The effect of friendly persuasion and gender on tax comliance behavior," *Journal of Business Ethics* (47:2), pp 133-145.

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.

Franke, G. R., Crown, D. F., and Spake, D. F. 1997. "Gender differences in ethical perceptions of business practices: A social role theory perspective," *Journal of applied psychology* (82:6), p 920.

Hovav, A., and D'Arcy, J. 2012. "Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the US and South Korea," *Information & Management* (49:2), pp 99-110.

Ifined, P. 2014. "Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition," *Information & Management* (51), pp 69-79.

Jones, T. M. 1991. "Ethical decision making by individuals in organizations: An issue-contingent model," *Academy of management review* (16:2), pp 366-395.

Kahneman, D., and Tversky, A. 1979. "Prospect theory: An analysis of decision under risk," *Econometrica* (47:2), pp 263-292.

Khazanchi, D. 1995. "Unethical behavior in information systems: The gender factor," *Journal of Business Ethics* (14:9), pp 741-749.

Kreie, J., and Cronan, T. P. 1998. "How men and women view ethics," *Communications of the ACM* (41:9), pp 70-76.

Liang, H., Xue, Y., and Wu, L. 2013. "Ensuring employees' IT compliance: carrot or stick?," *Information Systems Research* (24:2), pp 279-294.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., and Vance, A. 2009. "What levels of moral reasoning and values explain adherence to information security rules: An empirical study," *European Journal of Information Systems* (18:2), pp 126-139.

Pahnila, S., Siponen, M., and Mahmood, A. 2007. "Employees' behavior towards IS security policy compliance," *40th Annual Hawaii International Conference on System Sciences*.

Peslak, A. R. 2008. "Current information technology issues and moral intensity influences," *Journal of Computer Information Systems* (48:4), pp 77-86.

Puhakainen, P., and Siponen, M. 2010. "Improving employees' compliance through information systems security training: An action research study," *MIS Quarterly* (34:4), pp 757-778.

Siponen, M., and Vance, A. 2010. "Neutralization: New insights into the problem of employee information systems security policy violations," *MIS Quarterly* (34:3), p 487.

Sommestad, T., Hallberg, J., Lundholm, K., and Bengtsson, J. 2014. "Variables influencing information security policy compliance," *Information Management & Computer Security* (22:1), pp 42-75.

Vance, A., Siponen, M., and Pahnila, S. 2012. "Motivating IS security compliance: Insights from babit and protection motivation theory," *Information & Management* (49:3–4), pp 190-198.

Vitell, S. J., and Muncy, J. 2005. "The Muncy–Vitell consumer ethics scale: A modification and application," *Journal of Business Ethics* (62:3), pp 267-275.

Warkentin, M., and Willison, R. 2009. "Behavioral and policy issues in information systems security: The insider threat," *European Journal of Information Systems* (18:2), pp 101-105.