2013

Information Security Policy Compliance: An Empirical Study of Ethical Ideology

Ahmad Al-Omari
Dakota State University

Amit Deokar
Dakota State University

Omar F. El-Gayar
Dakota State University

Jack Walters
Dakota State University

Recommended Citation

Al-Omari, A., Deokar, A., El-Gayar, O., Walters, J., & Aleassa, H. (2013, January). Information security policy compliance: an empirical study of ethical ideology. In 2013 46th Hawaii International Conference on System Sciences (pp. 3018-3027). IEEE.

2013 46th Hawaii International Conference on System Sciences

Information Security Policy Compliance: An Empirical Study of Ethical Ideology

Ahmad Al-Omari
Dakota State University
Ahmad.Al-Omari@dsu.edu

Amit Deokar
Dakota State University
Amit.Deokar@dsu.edu

Omar El-Gayar
Dakota State University
Omar.El-Gayar@dsu.edu

Jack Walters
Dakota State University
Jack.Walters@dsu.edu

Hasan Aleassa
Yarmouk University
Omar.El-Gayar@dsu.edu

Abstract

Information security policy compliance (ISP) is one of the key concerns that face organizations today. Although technical and procedural measures help improve information security, there is an increased need to accommodate human, social and organizational factors. Despite the plethora of studies that attempt to identify the factors that motivate compliance behavior or discourage abuse and misuse behaviors, there is a lack of studies that investigate the role of ethical ideology per se in explaining compliance behavior.

The purpose of this research is to investigate the role of ethics in explaining Information Security Policy (ISP) compliance. In that regard, a model that integrates behavioral and ethical theoretical perspectives is developed and tested. Overall, analyses indicate strong support for the validation of the proposed theoretical model.

1. Introduction

Information security and data protection have become important concerns and challenges facing organizations and users. Despite the effort and money that organizations spend to secure their assets, many incidents of data breaches and information loss continue to happen every year. Today, organizations realize that securing information is a continuous and complex task. The burden of keeping information secure rests on the shoulders of all organizational functions and members [1]. On this view, users must be aware of their roles and responsibilities in protecting information assets and of how to respond to any potential threat [2]. As a result, security awareness programs should focus on enlightening users on how to effectively protect information assets [3].

To secure information assets and to reduce the risk associated with these systems, organizations typically concentrate on technical and procedural security measures [e.g. 4]. Although these solutions help improve information security [5], relying on them alone is not enough to eliminate risk [6]. Even though organizations are investing more in technology-based information security solutions [6], evidence from empirical surveys found that respondents reported large increases in information security incidents in 2009 [7]. Accordingly, organizations need to effectively manage and control security threats, beyond reliance on deployment of security software and hardware [8]. In addition, human, social and organizational factors must be considered as well [9]. Technology is an important factor but inadequate, acting alone, to create successful security. Technology is dependent on users' behavior [10].

Information security researchers have recently emphasized that management's attention is required to secure information resources [11] to design effective security policies [12, 13], and to enhance users' security awareness to comply with information security policies [14]. People are recognized as the weakest link in the information security chain, but are considered abundant assets in the effort to reduce information security threats [6]. Therefore, ISPs must be designed to provide employees with guidelines on how to address the integrity, availability, and confidentiality of information resources they use in performing their jobs [5, 12]. Despite creating comprehensive ISPs and guidelines to control employees' behavior, compliance has been found to be lacking because employees violation of ISPs [15]. This might be due to the fact that ISPs fail to impact users at all levels, or due to users' ignorance of ISPs' existence [16]. Developing robust security systems, guidelines, and policies will ensure better protection of an organization's information assets [12, 17], but is not sufficient to guarantee employees' compliance [1, 6] and will not eradicate threats if policies are not used properly.

Plethora of studies in recent years identified factors that motivate compliance behavior [e.g. 6, 13, 15] or discourage abuse and misuse behaviors [e.g. 5, 18, 19]. These studies used different underlying theories including planned behavior (TPB) [e.g. 6, 8], general

1530-1605/12 $26.00 © 2012 IEEE
DOI 10.1109/HICSS.2013.272

deterrence (GDT) [e.g. 5, 18], and protection motivation (PMT) [20]. Most of these studies investigated misuse behavior from a criminological perspective or rational choice perceptions of cost and benefits of deviant behaviors. Stafford and Warr [21] argued that punishments might have worked in the past, but today work only if an organization is serious about enforcing the policy. Thus deterrence, as discussed by Ruighaver, et al. [22], should be used only when high risk behavioral patterns can be identified without officious monitoring. Although literature on information security often refers to the importance of considering ethics as part of a holistic approach [22-24], and given that organizations practice deterrence rather than positive motivation to induce employees to meet ISPs requirements [22], relevant literature search reveals very few studies that investigate the role of ethical ideology in shaping compliance behavior or changing misuse behavior. Ethical theories are relevant to ISPs because the decision to comply or violate ISPs can be understood as an ethical conflict. Therefore, ethics in information security can serve two purposes [25]: identify criteria that distinguish good and bad, and promote good over bad. This study contributes to the extant body of knowledge by investigating the role of ethical ideology *per se.* This is done by developing an integrated model combining behavioral theory and ethics theory.

Specifically, we draw on the TPB [26] to propose a model that explains users' intentions to comply with ISPs. It is postulated that employees' intention to comply with the requirements of an organization's ISPs is influenced by subjective norms, self-efficacy, and attitudes toward compliance. Deontological and teleological ethics are hypothesized to impact attitude and subjective norms toward compliance. In essence, the study addresses the following questions:

1. What is the role of employee's deontological ethical ideology in shaping his/her behavior toward compliance with ISPs?
2. What is the role of employee's teleological ethical ideology in shaping his/her behavior toward compliance with ISPs?
3. What is the role of social pressure on employees' compliance intention regarding ISPs?

The rest of the article is arranged as follows. The next section (2) presents a brief review of the relevant literature and highlights the gaps that this study aims to address. Section 3 presents our theoretical foundation, discusses the research model, and presents hypotheses to be tested. Section 4 describes our research methodology, survey instrument, sample, and data collection methods. Section 5 presents analyses and results. Section 6 highlights contributions, limitations and future directions or this area of research.

2. Literature Review

Information and computer ethics have been a major concerns for researchers and practitioners for a long time [e.g.19, 27], and both groups have increasingly realized the importance of promoting ethical behavior [28]. Software and digital piracy literature widely investigated ethical behavior and information systems codes [29-31]. Yoon [32] integrated the TPB, ethics theory, deontological and teleological theories and found that ethical perspectives significantly reduce behavioral intentions to commit digital piracy. Higgins and Makin [33] tested the correlation of low self-control with software piracy and found that it correlated more strongly with software piracy for those who had associations with deviant peers. Building on TPB, Cronan and Al-Rafee [34] examined the factors that influence individual's intention to pirate digital material. They found that moral obligation and past piracy behavior significantly affect behavioral intentions. Seale, et al. [35] examined the predictors of software piracy, building on TPB, and found that social norms, expertise required, gender, and computer usage affect behavioral intentions to pirate. Wagner and Sanders [29] investigated the relationship between religion and theoretical ethical decision making processes in ethical or unethical situations, and found a significant relationship to software piracy. Chan and Lai [30] examined the impact of ethical ideology on Chinese computer users' software piracy attitude and behaviors, and found that ideological relativism exerted a stronger influence on attitudes and behaviors than did idealism. Moores and Chang [31] proposed a model of ethical decision making based on an adaptation of a four-component model of morality. The results suggested that moral recognition determines moral judgment, which determines moral intention, which determines buyer behavior, which influences use behavior. Building on the Theory of Reasoned Action (TRA), Aleassa, et al. [36] investigated the moderating effect of ethical ideology, religiosity, public self-consciousness, and low self-control on attitudes toward software piracy and found that all but religiosity acted as moderators.

In the information security environment, Myyry, et al. [15] explored the ability of moral reasoning and values to encourage compliance with ISPs. They argued that theories of moral reasoning are related to ISPs, and the intention or decision to violate an ISP can be interpreted in terms of moral conflict. They found that pre-conventional moral reasoning, which focuses on negative consequences for violators, is positively related to both hypothetical and actual compliance, while conventional moral reasoning, which focuses on acts to please others and on following the laws and norms for their own sake,

correlates negatively with compliance behavior. Harrington [19] assessed whether general and IS-specific codes of ethics affect computer abuse judgments and employees intentions to abuse information systems. The study found that general codes of ethics had no effect on abuse intentions of all employees, but it was found to affect those IS personnel who tend to deny responsibility. As compared to general codes, IS-specific codes of ethics had a direct effect on computer sabotage judgments and intentions, but had no contrasting effect on those with strong tendencies to deny responsibility.

North, et al. [37] compared the levels of information security and ethics awareness of students in diverse university environments, and found that technology universities' students were more aware of information systems security and ethics than those who attended a liberal arts university. Munro and Cohen [28] examined the effect of code communication on ethical behavior through its effects on code awareness and understanding and found that code understanding by IS professionals was a significant determinant of their ethical behavior. Workman and Gathegi [38] investigated why ethics and/or punishment may or may not serve to deter people from breaching information security measures. The study found that punishment and ethics training can be effective in reducing threats to information security. Other studies proposed frameworks for teaching information security ethics [e.g. 17]. The few studies found in security research investigated the role of ethics with other constructs. This study investigates the role of ethics in explaining compliance behavior.

3. Research Model

Drawing on the TPB [26], we propose an integrated model (refer Figure 1) to understand employees' behavioral compliance intentions with ISPs requirements from an ethical perspective.

3.1. Behavioral Theoretical Constructs

The TPB, an extension of the theory of reasoned action (TRA) [39], describes individual's intention to perform a given behavior over which they have incomplete volitional control. The TPB and TRA have been a framework for several studies in the information systems and information security fields [e.g. 36, 40]. TPB suggests that intentions are highly influenced by individuals' attitudes toward the behavior, subjective norms, and perceived behavioral control surrounding the performance of behavior. These intentions explain a high percentage of the variance in the actual behavior [26]. Our theory postulates that intentions are expected to capture the motivational factors that influence the behavior and the amount of effort planned to exert in order to perform the behavior [26].

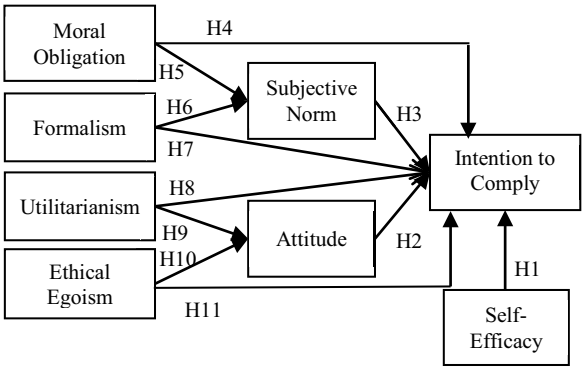

Figure 1. Research Model - Security Ethical Model

In consonance with the existing literature, we propose that an employee's intention to comply with the requirements of the organization's ISPs is associated with attitudes toward compliance, subjective norms, and self-efficacy. Self-efficacy is used instead of perceived behavioral control as it captures the same latent factor [41], and this is consistent with the literature [6, 42]. Based on the literature that investigated TPB constructs, we hypothesized in the context of ISPs compliance:

Hypothesis 1: An employee's self-efficacy toward compliance with the organization's ISPs positively affects intentions to comply with the requirements of the ISPs.

Hypothesis 2: An employee's attitude toward compliance with the organization's ISPs positively affects intention to comply with the requirements of the ISPs.

Hypothesis 3: An employee's subjective norms about compliance with the organization's ISPs positively affect intention to comply with the requirements of the ISPs.

3.2. Ethical Theoretical Constructs

Ethics can be defined as "inquiry into the nature and grounds of morality, where the term morality is taken to mean moral judgments, standards, and rules of conduct" [43, p. 1]. In our study, ethical theories were classified as either deontological or teleological according to Murphy and Laczniak [44]. The main difference between the two theories is that deontological theories focus on the specific actions or behaviors of an individual; the inherent righteousness of a behavior --, while teleological theories focus on the consequences of the actions or behaviors -- the amount of good or bad embodied in those consequences [45].

3.2.1. Deontological Theory. Deontological theories of ethics are based on the view that certain acts are wrong in themselves, and thus are morally unacceptable, even if the consequences pursued are morally remarkable [46]. This approach conceives of

morality as a duty, or a moral rule that should be followed. It is about following universal norms that describe what people should do, how they should behave, and what is right or wrong [47]. According to Gopal and Sanders [48], deontological ethics theories focus on the central role of moral obligation and duty. This view includes the theories of moral obligation, justice, and formalism [24, 32, 49].

Moral obligation as a deontological concept refers to the feeling of guilt or the personal obligation to perform or not to perform a behavior [34]. Ajzen [26] suggested that moral obligation could be added to the TPB as a separate determinant of intention in parallel with attitudes, subjective norms, and behavioral control. Also it can be a good predictor of ethical/unethical intentions [50]. Moral obligation has been used in the IT literature to predict ethical intentions [34]. According to Ajzen [26] moral obligation has a direct impact on intention, as investigated in the field of psychology. Further, moral obligation as a form of normative ethical standards, will help to shape employees' normative beliefs. Consequently, moral obligation could play an essential role in contexts where ethics are involved [34]. Furthermore, subjective norms are a function of one's normative beliefs and motivation to comply with the referent in question [26, 39]. Therefore, moral obligation as a normative ethical standard may play a role in forming personal normative beliefs [32]. Greater perceived obligation to comply with the requirements of the organization's ISPs is associated with higher compliance intentions. Hence, we hypothesize:

Hypothesis 4: An employee's moral obligation toward compliance with the organization's ISPs positively affects intentions to comply with the requirements of the ISPs.

Hypothesis 5: An employee's moral obligation positively affects subjective norms toward complying with the requirements of the ISPs.

Formalist ethics as a deontological concept looks to a set of rules or principles for guiding behavior, while actions are viewed as ethical/unethical to the degree that they conform to these rules [24]. Thus, the acts themselves are ethical or not, regardless of their outcomes, to the extent they conform to rules or principles [49]. This approach represents a human tendency to evaluate ethical situations in the context of compliance with rules and formal features [49]. Furthermore, the same concept of subjective norms in moral obligation applies to formalism in the sense that it is a function of person's normative beliefs concerning referent and motivation to comply with that referent [26]. Thus, we postulate that formalism as a normative ethical standard plays a role in forming personal normative beliefs. Therefore, we hypothesize:

Hypothesis 6: Formalism will positively affect subjective norms toward complying with the requirements of the ISPs.

Hypothesis 7: Formalism will positively affect employees' intentions to comply with the requirements of the ISPs.

3.2.2. Teleological Theory. These theories involve valuing goals or ends that are "good" [23], and they differ on the question of whose good it is that one ought to try to promote [45]. Teleologists "believe that there is one and only one basic or ultimate right-making characteristic, namely, the comparative value of what is, probably will be, or is intended to be brought into being" [51, p. 14]. According to this approach, people should identify the outcomes of various behaviors and evaluate the advantages and disadvantages of all outcomes [45]. Accordingly, a behavior is ethical if the outcomes are good and evil if otherwise. Teleological theories include utilitarianism and ethical egoism.

Utilitarianism posits that an act is right only if produces a greater balance of good outcomes over bad outcomes than other alternatives for all people [45]. It assumes that an individuals have moral preferences and evaluate consequences of actions as ethical or not [24] and act in the interest of others [47]. TRA, according to Fishbein and Ajzen [39], postulates that attitudes toward behavior are determined by a person's salient beliefs, that performing the behavior will lead to certain outcomes, and the evaluation of those outcomes. As perceived consequences are factors influencing attitudes toward the behavior, Yoon [32] argued that perceived benefits will have impact on attitudes toward the behavior. Likewise, Hunt and Vitell [45], contend that teleological evaluation influences behavior through ethical judgments which contain the perceived consequences. The Technology Acceptance Model (TAM) proposed and tested the relationship between perceived benefit (usefulness) and behavioral intention [52]. Accordingly, we argue that if an employee perceives that outcomes derived from compliance are higher than outcomes derived from noncompliance, a favorable attitude toward compliance will be formed. This argument is congruent with the findings of Tyler and Blader [53], where compliance with ISPs behavior is positively correlated with reaction to behavior captured by personal values. Therefore we hypothesize:

Hypothesis 8 Utilitarianism will positively affect employees' intentions to comply with the requirements of the ISPs.

Hypothesis 9 Utilitarianism will positively affect employees' attitudes toward complying with the requirements of the ISPs.

The second teleological theory is ethical egoism, under which the consequences of an act are evaluated exclusively in terms of their damage or benefit to the individual considering the action. It holds that employees should always try to promote their own greatest good [45]. If an act will benefit him/her but harm others, an ethical egoist will choose to perform that act [54]. Also, the act is right for an individual if the outcomes of that act for him or her are more favorable than the outcomes of any other act [45]. Therefore, if the outcomes of compliance with the requirements of the organization's ISPs for an employee are more favorable than the outcomes of noncompliance, then s/he will comply or form a favorable attitude toward compliance. According to Hunt and Vitell [45] teleological evaluation independently affects the intention, as an individual may perceive a particular alternative as the most ethical alternative and, nevertheless, intend to choose another alternative because of certain preferred consequences. An egoist is a person who acts in a way that promotes the greatest good for him- or herself, but only as long as others are not likely to be unjustly harmed [55]. Accordingly, we hypothesize:

Hypothesis 10: Ethical egoism will negatively affect employees' attitudes toward complying with the requirements of the ISP.

Hypothesis 11: Ethical egoism will negatively affect employees' intentions to comply with the requirements of the ISPs.

4. Research Methodology

Our Security Ethical Model is based on the Theory of Planned Behavior (TPB). The basic premise of the TPB is that behavioral intention is a function of perception, attitude, and perceived behavioral control. Such constructs are hard to observe and measure directly, as they represent an internal state, and therefore are "measured through indirect indicators, such as verbal expressions or overt behaviors" [56, p. 308]. Considering it "is difficult to get accurate information about internal states, such as attitudes or emotions, with anything other than self-reports" [57, p. 229], and since "self-reports of participants via surveys, questionnaires, and interviews are a very common way to gather data in almost all of the social sciences" [58], self-reports were utilized to measure all study constructs. People are expected to be able to report various relevant internal states, including attitudes, emotions, perceptions, and values [57]. Based on a comprehensive literature review, an initial survey instrument was developed by identifying and creating appropriate measurement items.

4.1. Item Development

An investigation of theoretical and empirical literature was conducted as the first step to develop survey items. The measurement items were based on existing scales in the literature that have proven reliable. The survey instrument is based on constructs validated and tested in prior research [1, 6, 20, 32, 36, 49, 59, 60], standardized and adapted to the context of this study. The survey instrument (refer Tables 1 and 3) was refined based on the feedback obtained from information security experts in the United States and Jordan as well as from a number of employees working at a variety of banks in Jordan. Based on that feedback, several items were reviewed and modified. The instrument also collected key demographic information including gender, age, education, years of experience, functional area of work, and average computer usage each day.

4.2. Data Collection

The research study participants were employees working at seven banks in Jordan. All of these banks have formal ISPs in place. The survey questionnaire was distributed on paper to 850 randomly-selected employees at different managerial levels in all bank departments participating in the study. The participants were given one week to complete and return the questionnaire. The identities of participants were kept confidential. Participants were asked about their awareness of the existence of ISPs and about their fluency in the English language. Only those participants that indicated some awareness of ISPs and those that were fluent in English were included in the data analyses. In total, 525 questionnaires were returned. 35 of them indicated that they were unaware of their banks' ISPs, so they were excluded. Another 27 questionnaires were later eliminated because of incomplete answers, and 18 were eliminated because of unreliable responses. For the purpose of data analysis, 445 usable responses were received, and the effective response rate was 52.3 percent.

Table 1 summarizes respondents' descriptive statistics. Participants reported using different computer software such as spreadsheets, e-mail, programming languages, database applications and their banks' special tailored software. The sample was quite evenly distributed in terms of the responsibilities of the respondents and in terms of their managerial levels. The data collected represents a diverse employee population because it includes employees from local as well as international banks in Jordan.

5. Data Analysis

Exploratory Factor Analysis (EFA) was conducted as a first step because relationships among observed indicators and underlying factors were not tested or investigated beforehand. EFA produced eight factors with eigenvalues greater than 2.0, which matches with the number of factors investigated in the study.

Component-based partial least squares (PLS), a structural modeling technique, was used to test and evaluate the psychometric properties of the constructs and to test the study hypotheses. PLS was chosen as the data analysis technique because it is better than traditional first-generation statistical methods (e.g., regression), in that it tests the measurement model (relationships between constructs and measurement indicators) and the structural model (theoretical relationships among constructs) simultaneously. Also, PLS was chosen because it focuses on prediction and is more suitable for exploratory research and theory building. The SmartPLS software package (version 2.0.M3) [61] was used for the estimation. In order to assess the measurement quality of the eight reflective constructs, factorial validity (convergent validity and discriminant validity), individual item reliability, and composite reliability were computed.

Table 1. Descriptive statistics of respondents

	Item	Freq.	Percent
Gender	Male	245	55.1
	Female	200	44.9
Age	20-29 years	179	40.2
	30-39 years	152	34.2
	40-49 years	88	19.8
	≥ 50 years	26	5.8
Education	High School	30	6.7
	Collage	51	11.5
	Bachelor's Degree	282	63.4
	Master	63	14.1
	PhD	19	4.3
Experience	1-5	150	33.7
	6-10	131	29.4
	11-15	75	16.9
	16-20	52	11.7
	> 20	37	8.3
Computer Use at Work (hrs./day)	Mean	10.52	
	Std. Deviation	6.21	
Using the computer (years)	Mean	11.00	
	Std. Deviation	7.72	

5.1. Measurement Model Testing

Table 3 summarizes the questionnaire items and their descriptive statistics; including means, standard deviations, and item loadings.

Table 2. Discriminant validity, AVE, and CR

	CR	AVE	1	2	3	4	5	6	7	8
ATT	.99	.97	**.98**							
EEG	.97	.78	-.32	**.88**						
FOR	.94	.77	.25	-.35	**.87**					
IC	.97	.84	.14	.08	.18	**.92**				
MO	.95	.80	.17	-.46	.25	.19	**.89**			
SE	.95	.76	.22	-.31	.34	.31	.27	**.87**		
SN	.95	.80	.19	-.36	.28	.21	.29	.37	**.89**	
UTI	.96	.76	.21	-.33	.29	.19	.31	.38	.31	**.87**

As noted in Table 3, all item loadings exceeded the recommended minimum value of 0.789, indicating that at least 50 percent of the variance was accounted for by the corresponding construct. As shown in Table 2, the AVE was higher than the minimum recommended value of 0.5 for each construct, indicating that the items had convergent validity.

Next, discriminant validity was assessed. The square root of the AVE for each construct was noted to be higher than the inter-construct correlations (refer Table 2). Also, from the cross-loading matrix, it was found that, as recommended, all measurement items loaded higher than 0.789 on their underlying construct, and loaded very low, less than 0.40, on other constructs. All constructs in the model satisfied these criteria for discriminant validity.

Scale reliability and internal consistency were also assessed. Composite reliability (CR) for each construct was noted to be more than 0.952 (see Table 2), and Cronbach's alpha was higher than 0.925, demonstrating that all constructs had adequate reliability assessment scores and all construct measures were considered to be reflective. We also conducted a series of confirmatory factor analyses using different extraction methods to test dimensionality of the constructs. The results of these analyses indicated that all constructs were unidimensional.

5.2. Structural Model Testing

PLS was used to estimate our measurement model. The PLS algorithm and the bootstrapping re-sampling method with 445 cases and 890 re-samples were used to estimate the structural model. Figure 2 shows the results of the model estimation, path coefficients, path significance based on a two-tailed t-test, and the variance explained by the independent variables (R^2).

Based on the significant path coefficients (refer to Figure 2), all hypotheses were supported ($p < 0.001$) except H8. The structural model explained approximately 32.1 percent of the variance for the "intention to comply", whereas 41.1 percent of the variance was explained for attitude and 23.7 percent of the variance was explained for subjective norms.

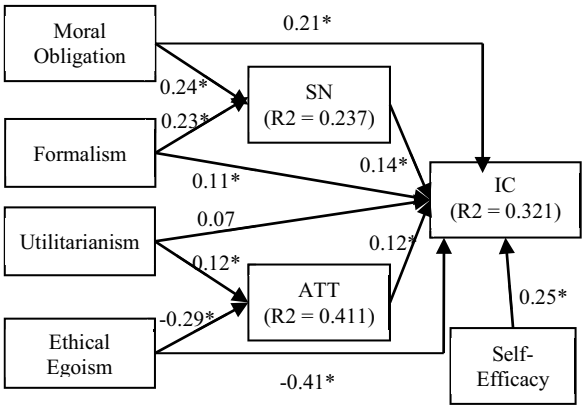

Figure 2. Structural Model Testing Results

6. Discussion

Our proposed Security Ethical Model underscores the user dimension in addressing ISP compliance issues. The model tries to explain users' compliance behavior with ISPs in the context of TPB, and the users' ethical ideology (deontology and teleology). Conceptually, employees who are aware of their organizations' ISPs, yet deliberately violate those policies, are a significant threat to the organization. Awareness and training programs are likely to have little impact on their behavior [62]. The results of our study supported the validity of the model as a useful theoretical framework to predict and enhance compliance behavior with ISPs.

We found, as hypothesized in H2 and H3, that attitude, subjective norms, and self-efficacy are significantly related to an employee's intention to comply. Consistent with the proposed reference model, we found that deontological ethical ideology, moral obligation, and formalism exerted significant influence on employees' intention to comply. Thus, hypotheses 4, 5, 6, and 7 were fully supported. Our findings also indicated that both deontological theories had almost equal influence on an employee's social pressure about compliance, suggesting no specific norms has a predominant effect on employee's perceived social pressure about compliance. Furthermore, moral obligation was found to have stronger influence on intention to comply, suggesting that compliance behavior is an ethical behavior and employees with higher feelings of guilt or moral obligation have higher intention to comply.

Constructs of utilitarianism and ethical egoism were found to have significant influence on employee attitudes toward compliance, suggesting increased compliance from employees who value goals or ends that are good for their (or others) personal interests. Thus hypotheses 9, and 10 were fully supported. Utilitarianism was found to exert no significant influence on intention to comply. This suggests that employees are more interested in achieving personal goals or ends by complying with the organization's ISPs than in acting in the interest of others if it conflicts with ISPs. However, ethical egoism was found to have a significant and a negative influence on intention to comply suggesting that persons promoting the greatest goods for themselves are less likely to comply.

7. Contributions, Limitations and Future Research

In this study, an integrated model that combines the TPB and ethics theory was proposed. Our goal was to identify ethical factors that can influence employees' intentions to comply with organizations' ISPs. Using established research from psychology, information technology, and business ethics, four ethical ideologies were identified. Although previous literature advocated the crucial influence of individual ethical beliefs on behavioral intentions [15, 19, 32, 36], it failed to scrutinize how users with different ethical ideologies might diverge in making compliance/abuse/piracy decisions. This study represents the first attempt to investigate the influence of various types of ethical ideology on compliance attitudes and behaviors. This study offers a new venue to scout the decision process underlying compliance/abuse behavior.

Our study makes important theoretical contributions to the emerging body of knowledge about ethical behavior as it relates to information security. The existing literature has investigated factors rooted in GDT, PMT, and RCT, among others, to explain compliance but, to the best of our knowledge, this is the first study that offers a theoretical explanation and empirical support for the impact of an employee's ethical ideology (deontologist or teleologist) on compliance intention with ISPs.

The results suggest that employees' attitudes toward compliance with ISPs may be shaped and enhanced by their ethical ideology. This provides evidence of the significant impact of a person's moral and ethical background on compliance behavior, specifically when we know that the decision to comply or violate ISPs can be viewed as an ethical conflict.

We acknowledge the limitations that relate to this study. First, the study sample was collected in Jordan, which will restrict the generalizability of the results based on cultural dimension. Also, the study sample is confined to the bank employees. We plan to address these limitations by replicating the study in other contexts and cultures. Another limitation could arise from a possible loss of meaning that might have occurred because the questionnaire was written in English, which is a second language in Jordan. A third limitation could arise from measuring "intention" via self-report. Siponen and Vance [63] have proposed using scenarios describing a hypothetical situation to capture detailed explanations about specific policies, rules, and guidelines. Future work based on hypothetical scenarios is planned.

Study of ethical issues in information security is in its infancy. Integrating perspectives from different ethical theories into the field of information security can lead us to better understand and predict employees' security behaviors.

8. References

[1] T. Herath and H. R. Rao, "Protection motivation and deterrence: a framework for security policy compliance in organisations," *European Journal of Information Systems,* vol. 18, pp. 106-125, 2009.

[2] M. Wilson, K. Stine, and P. Bowen, "Information Security Training Requirements: A Role- and Performance-Based Model," 2009.

[3] C. C. Chen, R. Shaw, and S. C. Yang, "Mitigating information security risks by increasing user security awareness: a case study of an information security awareness system," *Information Technology, Learning, and Performance Journal,* vol. 24, pp. 1-15, 2006.

[4] T. Schlienger and S. Teufel, "Analyzing information security culture: increased trust by an appropriate information security culture," in *Proceedings of the 14th International Workshop on Database and Expert Systems Applications (DEXA'03)*, 2003, pp. 405–409.

[5] D. Straub, "Effective IS security," *Information Systems Research,* vol. 1, pp. 255-276, 1990.

[6] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness," *MIS Quarterly,* vol. 34, pp. 523-548, 2010.

[7] R. Richardson. (2009, Dec. 10). *2009 CSI Computer Crime and Security Survey*. Available: **http://www.personal.utulsa.edu/~james-childress/cs5493/CSISurvey/CSISurvey2009.pdf**

[8] J. Zhang, B. J. Reithel, and H. Li, "Impact of perceived technical protection on security behaviors," *Information Management & Computer Security,* vol. 17, pp. 330-340, 2009.

[9] R. Werlinger, K. Hawkey, and K. Beznosov, "Human, organizational and technological challenges of implementing IT security in organizations," in *Proceedings of the Second International Symposium on Human Aspects of Information Security & Assurnace (HAISA 2008)*, Plymouth, UK, 2008, pp. 35-47.

[10] B. Y. Ng and Y. Xu, "Studying Users' Computer Security Behavior Using the Health Belief Model," in *11th Pacific-Asia Conference on Information Systems* 2007, pp. 423-437.

[11] A. Dutta and K. McCrohan, "Management's Role in Information Security in a Cyber Economy," *California Management Review,* vol. 45, pp. 67-87, 2002.

[12] M. E. Whitman, A. M. Townsend, and R. J. Aalberts, "Information systems security and the need for policy," in *Information Security Management: Global Challenges in the New Millennium*, G. Dhillon, Ed., ed Hershey, PA, USA: Idea Group Publishing, 2001.

[13] M. Siponen, S. Pahnila, and A. Mahmood, "Employees' adherence to information security policies: an empirical study," in IFIP International Federation for Information Processing, Volume 232, New Approaches for Security, Privacy and Trust in Complex Environments, H. Venter, Eloff, M., Labuschagne, L., Eloff, J., von Solms, R., Ed., ed: Boston: Springer, 2007, pp. 133-144.

[14] S. R. Boss, L. J. Kirsch, I. Angermeier, R. A. Shingler, and R. W. Boss, "If someone is watching, Ill do what Im asked: mandatoriness, control, and information security," *European Journal of Information Systems,* vol. 18, pp. 151-164, 2009.

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

[16] R. O. Mason, "Four Ethical Issues of the Information Age," *Mis Quarterly,* vol. 10, pp. 5-12, 1986.

[17] E. Cohen and L. Cornwell, "A question of ethics: Developing information system ethics," *Journal of Business Ethics,* vol. 8, pp. 431-437, 1989.

[18] J. D'Arcy, A. Hovav, and D. Galletta, "User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach," *Information Systems Research,* vol. 20, pp. 79-98, 2009.

[19] S. J. Harrington, "The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions," *MIS Quarterly,* vol. 20, pp. 257-278, 1996.

[20] M. Siponen, S. Pahnila, and M. A. Mahmood, "Compliance with Information Security Policies: An Empirical Investigation," *Computer,* vol. 43, pp. 64-71, 2010.

[21] M. C. Stafford and M. Warr "Reconceptualization of General and Specific Deterrence," *Journal of Research in Crime and Delinquency,* vol. 30, pp. 123-135, 1993.

[22] A. B. Ruighaver, S. B. Maynard, and M. Warren, "Ethical decision making: Improving the quality of acceptable use policies," *Computers & Security,* vol. 29, pp. 731-736, 2010.

[23] R. M. Davison, "Professional ethics in information systems: A personal perspective," *Communications of the AIS,* vol. 3, pp. 4-es, 2000.

[24] G. Alder, M. Schminke, T. Noel, and M. Kuenzi, "Employee Reactions to Internet Monitoring: The Moderating Role of Ethical Orientation," *Journal of Business Ethics,* vol. 80, pp. 481-498, 2008.

[25] J. Leiwo and S. Heikkuri, "An analysis of ethics as foundation of information security in distributed systems," in *Proceedings of the Thirty-First Hawaii International Conference on System Sciences*, 1998, p. 213.

[26] I. Ajzen, "The theory of planned behavior," *Organizational behavior and human decision processes,* vol. 50, pp. 179-211, 1991.

[27] B. C. Stahl, "The ethical nature of critical research in information systems," *Information Systems Journal,* vol. 18, pp. 137-163, 2008.

[28] K. Munro and J. Cohen, "Ethical Behavior and Information Systems Codes: The Effects of Code Communication, Awareness, Understanding, and Enforcement," ICIS 2004 Proceedings. Paper 74. **http://aisel.aisnet.org/icis2004/74**, 2004.

[29] S. C. Wagner and G. L. Sanders, "Considerations in ethical decision-making and software piracy," *Journal of Business Ethics,* vol. 29, pp. 161-167, 2001.

[30] R. Y. K. Chan and J. W. M. Lai, "Does ethical ideology affect software piracy attitude and behaviour? An

empirical investigation of computer users in China," *European Journal of Information Systems,* vol. 20, pp. 659-673, 2011.

[31] T. T. Moores and J. C. J. Chang, "Ethical decision making in software piracy: Initial development and test of a four-component model," *Mis Quarterly,* vol. 30, pp. 167-180, 2006.

[32] C. Yoon, "Theory of Planned Behavior and Ethics Theory in Digital Piracy: An Integrated Model," *Journal of Business Ethics,* pp. 1-13, 2011.

[33] G. E. Higgins and D. A. Makin, "Self-Control, Deviant Peers, and Software Piracy," *Psychological reports,* vol. 95, pp. 921-931, 2004.

[34] T. P. Cronan and S. Al-Rafee, "Factors that influence the intention to pirate software and media," *Journal of Business Ethics,* vol. 78, pp. 527-545, 2008.

[35] D. A. Seale, M. Polakowski, and S. Schneider, "It's not really theft!: personal and workplace ethics that enable software piracy," *Behaviour & Information Technology,* vol. 17, pp. 27-40, 1998.

[36] H. Aleassa, J. Pearson, and S. McClurg, "Investigating Software Piracy in Jordan: An Extension of the Theory of Reasoned Action," *Journal of Business Ethics,* vol. 98, pp. 663-676, 2011.

[37] M. North, D. A. Perryman, S. Burns, and S. North, "A comparative study of information security and ethics awareness in diverse university environments," *Journal of Computing Sciences in Colleges,* vol. 25, pp. 223-230, 2010.

[38] M. Workman and J. Gathegi, "Punishment and ethics deterrents: A study of insider security contravention," *Journal of the American Society for Information Science and Technology,* vol. 58, pp. 212-222, 2007.

[39] M. Fishbein and I. Ajzen, Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research: MA: Addison-Wesley, 1975.

[40] C. L. Anderson and R. Agarwal, "Practicing Safe Computing Special Issue Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions," *MIS Quarterly,* vol. 34, pp. 613-643, 2010.

[41] M. Fishbein, "A reasoned action approach to health promotion," *Medical Decision Making,* vol. 28, p. 834, 2008.

[42] P. Y. K. Chau, "Influence of computer attitude and self-efficacy on IT usage behavior," *Journal Of End User Computing,* vol. 13, pp. 26-33, 2001.

[43] P. W. Taylor, *Principles of Ethics: An Introduction*. Encino, CA: Dickenson Publishing Company, Inc., 1975.

[44] P. Murphy and G. R. Laczniak, "Marketing Ethics: A Review with Implications for Managers, Educators and Researchers," *in Enis, B. M., & Roering, K. J. (1981). Review of Marketing, 1981: American Marketing Association.,* pp. 251-266, 1981.

[45] S. D. Hunt and S. Vitell, "A General Theory of Marketing Ethics," *Journal of Macromarketing,* vol. 6, pp. 5-16, 1986.

[46] G. Walsham, "Ethical theory, codes of ethics and IS practice," *Information Systems Journal,* vol. 6, pp. 69-81, 1996.

[47] I. Van Staveren, "Beyond Utilitarianism and Deontology: Ethics in Economics," *Review of Political Economy,* vol. 19, pp. 21-35, 2007/01/01 2007.

[48] R. D. Gopal and G. L. Sanders, "Preventive and Deterrent Controls for Software Piracy," *Journal of Management Information Systems,* vol. 13, pp. 29-47, Spring97 1997.

[49] F. N. Brady and G. E. Wheeler, "An empirical study of ethical predispositions," *Journal of Business Ethics,* vol. 15, pp. 927-940, 1996.

[50] S. H. Schwartz and R. C. Tessler, "A Test of a Model for Reducing Measured Attitude-Behavior Discrepancies," *Journal of Personality and Social Psychology,* vol. 24, pp. 225-236, 1972.

[51] W. Frankena, *Ethics*. Englewood Cliffs, NJ: Prentice-Hall, Inc, 1963.

[52] Y. Lee, K. A. Kozar, and K. R. T. Larsen, "The technology acceptance model: Past, present, and future," *Communications of the Association for Information Systems,* vol. 12, p. 50, 2003.

[53] T. R. Tyler and S. L. Blader, "Can Businesses Effectively Regulate Employee Conduct? The Antecedents of Rule Following in Work Settings," *Academy of Management Journal,* vol. 48, pp. 1143-1158, 2005.

[54] E. R. Foxman and P. Kilcoyne, "Information Technology, Marketing Practice, and Consumer Privacy: Ethical Issues," *Journal of Public Policy & Marketing,* vol. 12, pp. 106-119, 1993.

[55] K. Rallapalli, S. Vitell, and J. Barnes, "The Influence of Norms on Ethical Judgments and Intentions: An Empirical Study of Marketing Professionals," *Journal of Business Research,* vol. 43, pp. 157-168, 1998.

[56] W. G. Zikmund, *Business Research Methods*. Mason, Ohio: Thomson/South-Western, 2003.

[57] P. E. Spector, "Method Variance in Organizational Research : Truth or Urban Legend?," *Organizational Research Methods,* vol. 6, pp. 221-232, 2006.

[58] T. J. B. Kline, L. M. Sulsky, and S. D. Rever-Moriyama, "Common Method Variance and Specification Errors: A Practical Approach to Detection," *Journal of Psychology,* vol. 134, pp. 401-421, 2000.

[59] G. Casali, "Developing a Multidimensional Scale for Ethical Decision Making," *Journal of Business Ethics,* vol. 104, pp. 485-497, 2011.

[60] J. B. Cullen, B. Victor, and J. W. Bronson, "The Ethical Climate Questionnaire: An Assessment of Its Development and Validity," *Psychological Reports,* vol. 73, pp. 667-674, 1993/10/01 1993.

[61] C. M. Ringle, S. Wende, and S. Will, "SmartPLS Release 2.0 (M3) Beta," ed. University of Hamburg, Hamburg, Germany: **http://www.smartpls.de**, 2005.

[62] M. Siponen, "Critical analysis of different approaches to minimizing user-related faults in information systems

security: implications for research and practice," *Information Management & Computer Security,* vol. 8, pp. 197-209, 2000.

[63] M. Siponen and A. O. Vance, "Neutralization: New Insights into the Problem of Employee Systems Security Policy Violations," *MIS Quarterly,* vol. 34, pp. 487-502, 2010.

Appendix

Table 3. Measures items and item loading

Items	Dimensions/Questions	Mean	STD	Loading
IC	**Intention to Comply**			
	I intend to comply with the requirements of the ISP of my organization	5.517	1.347	0.940
	I intend to protect information resources according to the requirements of the ISP of my organization.	5.463	1.408	0.908
	I intend to protect technology resources according to the requirements of the ISP of my organization.	5.315	1.552	0.954
	I intend to carry out my responsibilities prescribed in the ISP of my organization when I use information resources.	5.285	1.551	0.946
	I intend to carry out my responsibilities prescribed in the ISP of my organization when I use technology resources.	5.578	1.298	0.920
	I intend to recommend that others comply with ISP.	5.688	1.202	0.825
	I intend to assist others in complying with ISP.	5.443	1.398	0.948
SE	**Self-Efficacy**			
	I have the necessary skills to fulfill the requirements of the ISP.	5.079	1.671	0.861
	I have the necessary knowledge to fulfill the requirements of the ISP.	5.121	1.729	0.893
	I have the necessary competencies to fulfill the requirements of the ISP.	5.038	1.724	0.888
	I would feel comfortable following my organization's ISP on my own.	5.171	1.634	0.875
	If I wanted to, I could easily comply with my organization's ISP on my own.	4.989	1.724	0.891
	I would be able to follow most of the ISP even if there was no one around to help me	5.036	1.739	0.851
SN	**Subjective Norm**			
	Upper level management thinks I should comply with the requirements of my organization's ISPs.	5.209	1.682	0.894
	My boss thinks that I should comply with the requirements of my organization's ISPs.	5.258	1.700	0.899
	My colleagues think that I should comply with the requirements of my organization's ISPs.	5.202	1.679	0.898
	The information security/technology department in my organization thinks that I should comply with the requirements of my organization's ISPs.	5.184	1.657	0.902
	Other computer technical specialists in the organization think that I should comply with the requirements of my organization's ISPs.	5.128	1.653	0.880
MO	Moral Obligation			
	I would feel guilty if I violate the requirements of ISPs	5.375	1.626	0.887
	Violating the requirements of ISPs goes against my principles	5.411	1.559	0.937
	It would be morally wrong for me to violate the requirements of ISPs	5.402	1.488	0.879
	Moral actions are those which closely match ideals of the most "perfect" action.	5.375	1.594	0.868
	There are no ethical principles important enough that they should be a part of any code of ethics.	2.515	1.518	0.909
UTI	**Utilitarianism**			
	Compliance with the requirements of ISPs creates the greatest overall benefit for the organization.	5.299	1.645	0.856
	Compliance with the requirements of ISPs creates the greatest overall benefit for the department.	5.371	1.645	0.875
	Violation of the requirements of ISPs has no effect or harm on the organization	2.739	1.683	0.877
	Respecting organizational rules and regulations that have been created for the greatest benefit for all stakeholders	5.400	1.661	0.880
	Compliance with the requirements of ISPs minimizes the costs for the organization.	5.274	1.700	0.876
	Compliance with the requirements of ISPs optimizes resources of the organization.	5.373	1.629	0.899
	It is never necessary to sacrifice the welfare of others by violating the requirement of the ISPs.	5.254	1.553	0.866
	One should not violate the requirements of ISPs that might in any way threaten the dignity and welfare of another individual.	5.346	1.592	0.856
	A person should make certain that violating the requirements of ISPs never intentionally harm others even to small degree.	5.324	1.633	0.858
FOR	**Formalism … … How important are the following personal characteristics to you, being**			
	dependable	5.337	1.608	0.789
	trustworthy	5.097	1.794	0.897
	honest	5.146	1.702	0.906
	noted for integrity	5.213	1.622	0.908
	law abiding	5.238	1.625	0.889
EEG	**Ethical Egoism**			
	In this company, people are mostly out for themselves.	2.888	1.732	0.881
	The major responsibility for people in this company is to consider efficiency first.	2.897	1.815	0.895
	People are expected to do anything to further the company's interests.	2.939	1.752	0.909
	There is no room for one's own personal morals or ethics in this company.	2.861	1.788	0.901
	Work is considered sub-standard only when it hurts the company's interests.	2.816	1.738	0.892
	In this company, people protect their own interest above other considerations.	2.845	1.750	0.880
	People are concerned with the company's interests to the exclusion of all else.	2.915	1.731	0.870
	Decisions here are primarily viewed in terms of contribution to profit.	2.834	1.758	0.856
	People in this company are very concerned about what is best for themselves.	2.813	1.683	0.863
ATT	**Attitude … … To me, complying with the requirements of my organization's ISP is _____**			
	Not necessary … Necessary	5.613	1.484	0.981
	Not beneficial … Beneficial	5.613	1.488	0.989
	Not important … Important	5.580	1.517	0.995
	Not useful … Useful	5.613	1.488	0.989
	Not exciting … Exciting	5.620	1.479	0.978