

Accepted Manuscript

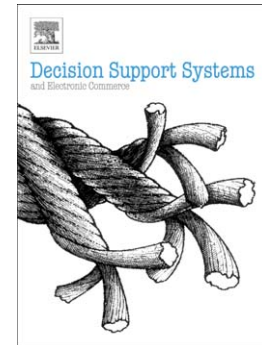
Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness

Tejaswini Herath, H.R. Rao

PII: S0167-9236(09)00053-0
DOI: doi: [10.1016/j.dss.2009.02.005](https://doi.org/10.1016/j.dss.2009.02.005)
Reference: DECSUP 11586

To appear in: *Decision Support Systems*

Received date: 22 October 2007
Revised date: 6 February 2009
Accepted date: 16 February 2009



Please cite this article as: Tejaswini Herath, H.R. Rao, Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness, *Decision Support Systems* (2009), doi: [10.1016/j.dss.2009.02.005](https://doi.org/10.1016/j.dss.2009.02.005)

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

ENCOURAGING INFORMATION SECURITY BEHAVIORS IN ORGANIZATIONS: ROLE OF PENALTIES, PRESSURES AND PERCEIVED EFFECTIVENESS

Tejaswini Herath

Assistant Professor, Department of Finance, Operations and Information Systems
Faculty of Business, Brock University, St. Catharines, Ontario, Canada

H. R. Rao

Professor, Management Science and Systems, School of Management and
Adjunct Professor Computer Science and Engineering, College of Engineering
State University of New York at Buffalo

ABSTRACT

Secure management of information systems is crucially important in information intensive organizations. Although most organizations have long been using security technologies, it is well known that technology tools alone are not sufficient. Thus, the area of end-user security behaviors in organizations has gained an increased attention. In information security observing end-user security behaviors is challenging. Moreover, recent studies have shown that end-users have divergent security views. The inability to monitor employee IT security behaviors and divergent views regarding security policies, in our view, provide a setting where the principal agent paradigm applies. In this paper, we develop and test a theoretical model of the incentive effects of penalties, pressures and perceived effectiveness of employee actions that enhances our understanding of employee compliance to information security policies. Based on 312 employee responses from 77 organizations, we empirically validate and test the model. Our findings suggest that security behaviors can be influenced by both intrinsic and extrinsic motivators. Pressures exerted by subjective norms and peer behaviors influence employee information security behaviors. Intrinsic motivation of employee perceived effectiveness of their actions was also found to play an important role in security policy compliance intentions. In analyzing the penalties, certainty of detection was found to be significant while surprisingly, severity of punishment was found to have a negative effect on security behavior intentions. We discuss the implications of our findings for theory and practice.

Keywords: Principal agent theory, Information security, End-user security behaviors, Security policy compliance

1.0 INTRODUCTION

In information intensive organizations secured management of information has become an important issue. Organizations have been actively using security technologies. Extant research in information security has been focused on the use technology (e.g., [27, 69]). However more recently, practitioners and academics have started to realize that information security can not be achieved through only technological tools and effective organizational information security depends on all three components, namely: people, processes and technology [34]. However, empirical research on end user security behaviors and factors influencing them is still in its infancy.

With the advances in security technologies, many computing behaviors such as patch management and antivirus updates are now being automated to reduce the task knowledge and time burdens on end users. However, behaviors such as appropriate use of computer and network resources, appropriate password habits etc., that can not be addressed by security technologies are often dealt through organizational computer security policies. Recent security breach incidents [3] show that employee negligence and noncompliance often cost organizations millions of dollars in losses. Mishra and Dhillon [44] contend that failures to prevent or minimize security breaches due to end-user noncompliance are indicators of failed IS security governance programs which do not address the means to encourage conformity with policies. Although, appropriate computer use policies in organizations have been recognized to be important for a long time, the empirical research in this area is still embryonic.

Our paper focuses on security policy compliance in organizations. In information security context, the inability to monitor employee IT security policy compliance and divergence in management and employee views provides a setting where the principal agent paradigm can be applied. Our paper makes two main contributions to theory and practice. First, we draw upon and synthesize the rich literature in agency theory and apply it in the context of information security where, to our knowledge, it has not yet been applied. We propose an empirically testable theoretical model which considers several extrinsic and intrinsic motivators that may encourage security policy compliance in organizations. Specifically, this study investigates the impact of penalties (extrinsic incentive), social pressures (extrinsic

incentive) and perceived value or contribution (intrinsic incentive) on the organizational security policy compliance. To the best of our knowledge, this is one of the earliest studies that evaluate mechanisms by which the information security policy compliance can be encouraged in organizations. Second, using responses from 312 employees from 77 organizations we empirically validate and test the model providing insightful findings that have implications for both theory and practice. Our findings suggest that both the intrinsic and extrinsic motivators influence employee intentions of security policy compliance in organizations. Surprisingly, contrary to our expectation we find that severity of penalties had significant but negative impact on policy compliance while as expected certainty of detection had positive effect on policy compliance. These results provide important implications for practice as well as further research.

This paper is organized as follows. First, we discuss the relevant gaps in the literature and illustrate the applicability of the principal agent paradigm to information security governance. Next, based on a detailed review of relevant information security, economic, sociological, and psychological literatures we develop a theoretical model. We then discuss the instrument development process, validation, and empirical test of the theoretical model. We conclude the paper with a discussion of our findings, their implications for theory and practice, and avenues for future research.

2.0 RESEARCH MOTIVATION AND THEORETICAL BACKGROUND

2.1 Prior Research related to Employee Information Security Behaviors

A survey of literature shows that research on technical controls for securing the information systems is abundant but policy compliance and informal controls have rarely been emphasized in the security literature [44]. Although the importance of security governance that entails the end-user behaviors has been stressed by the practitioners and academics alike, there has been only limited attention devoted to behavioral information security.

There are some empirical studies that evaluate organizational security practices and their effectiveness. However, the respondents are typically IT administrators or top-level managers (e.g., [21, 38, 43, 62]), and there have been hardly any representation from the end-user community. The fact that the respondents in prior studies were largely those responsible for setting up and running technical

security initiatives raises the question as to whether their views are likely to be representative of an organization at large [28]. For example, even though an IT administrator might indicate that there is a formal security policy; this does not necessarily mean that the end-users would take any notice of it. A recent empirical study [52] evaluating perceptions regarding access controls reports that employees perceive increase security conformity as greater job interference. Such perception may lead employees to ignore security policies to achieve efficiency in their day to day job routines.

Most participants of an ICIS 1993 conference panel reported that organizational information security policies are necessary, however, they perceived them to be ineffective [42]. In an empirical study, Frank et al. [29] found that user knowledge and informal department norms were related with the security-related behavior while the existence of formal policies regarding PC security was not associated with security-related behavior. Almost fifteen years later, the Knapp [38] security manager opinion study indicates that employee perceptions about security policies are still unclear and varied. Recent information security surveys (such as eCrime Survey [1]) reveal that, although, the policies and procedures are in place, many employees as well as outside contractors in majority of the instances tend to ignore them.

Although, the literature focusing on information security policy compliance in organization is sparse, we identify some of the representative literature in the area of behavioral security (Table 1) that provides guidelines and motivation for this study. The review of literature indicates the possibility of various theories that can be used in examination of information security related behaviors. It also shows the framework considered in this study that has not until now been empirically evaluated in the literature.

Insert Table 1 Here

2.2 Security Policy Compliance and Agency Paradigm

The objective of any organizational policy is to influence and determine employees' course of action. While the defined policies may be crystal clear and detailed, the result may not turn out to be as desired, especially with regard to information security [44]. The aim of behavioral aspects of security governance

is to ensure that employees show conformity with the rules and policies [58]. Previous research and field surveys, however, suggest that employees seldom comply with information security procedures. Policies, especially those involving information security, are viewed as mere guidelines [33] or general directions to follow rather than “hard and fast rules” that are specified as standards [47, 60]. Due to the relatively discretionary nature of adherence to these policies, organizations find enforcement of security a critical challenge. Thus more recently, research in behavioral information security has started focusing attention to employee intentions to follow security policies [14, 47].

In influencing the employee behavior we can draw upon agency theory which has been widely studied in organizational context. Agency theory or principal agent paradigm [26] is mainly concerned with the efforts provided by the individual members and of motivating them to obtain the desired effort input. An agency relationship exists whenever one party (principal) entrusts some decision making authority to another party (agent). This paradigm assumes that agents incur personal costs as they devote their time, knowledge and effort to the firm; and given an opportunity they can retract the level of effort, skill, and knowledge they provide (shirking). When a member's effort is not observable or monitoring is very costly, and goals are incongruent it creates a principal agent problem. The principal's goal is to effectively motivate the agent's effort through incentives that recognizes the member's effort as well as environmental factors that have a bearing on the output. Since the early evaluation of employer-employee relationships, agency theory has been extended to virtually all types of transactional exchanges that occur in a socio-economic system where information asymmetry, fears of opportunism, and bounded rationality exist ([48, 54], among others).

In an information security setting, the uncertainty of employee actions arises when employees and management (IT management) have conflicting interests. In organizational information security, responsibility of whether to adhere to organizational security policies or ignore them is delegated to employees. Employees may choose to break security policies for malicious purposes or choose to evade security policies for mere convenience. A recent study in context of access controls [52] found that employees believe that higher level of information security restricts their ability to follow flexible

operation routines, and perceive it as counter productive. In addition, employee actions related to security policy compliance may also be difficult to monitor. Monitoring of employee performance of security behaviors requires surveillance. Surveillance control techniques are now becoming more common in social spaces including workplaces [8]. While organizational surveillance techniques can be used to monitor and control employee behaviors, monitoring every information security related action of each end-user is extremely costly and may not even be practically possible. For instance, one can employ network monitoring to track on-line behaviors or install cameras to attain certain level of physical security; however, behaviors such as writing down the passwords or sharing passwords with friends can not be monitored.

Agency theory can provide a systematic way to think about incentive/disincentive mechanisms to encourage higher level of policy conformance. The incentives to achieve security behaviors can be investigated from the perspective of imposing penalties (negative incentives) for harmful behaviors (e.g. see [30]). Alternative incentive mechanisms based on environmental factors may also play a useful role in encouraging desired behaviors. In information security, practitioners have acknowledged that when surveillance may not be possible, for various reasons, creating a general environment or culture that fosters security is a better strategy [2]. Economists have also discussed and considered the role of social norms (see [40]). Although, some social psychologists and sociologists have considered norms as somewhat general rules of voluntary behavior, Kreps [40] suggests that social pressure can provide implicit and vague but still valuable extrinsic incentives. While whether social pressures act in an intrinsic or an extrinsic way can be disputed [40], they have been shown to have effects on employee behaviors in prior literature including IT use in organizational setting. In this research, we adopt a view similar to the one described by Benabou and Tirole [7] to characterize the motivations: extrinsic motivations are rewards contingent on external factors while intrinsic motivations are based on individual's desire to perform the task for its own sake. Since social pressures are factors external to an individual, we consider them as extrinsic influencing factors.

Much of the agency literature assumes that an agent bears no moral burden, and therefore they are perfectly willing, given an opportunity, to renege on the level of effort, skill, or knowledge they provide the firm. However, in recognizing the importance of other incentive mechanisms researchers have incorporated moral motivations (intrinsic incentives) in analytical models [7, 12, 45]. Information security literature has also considered such intrinsic motivations in the context of knowledge sharing. In our study, we consider motivation in terms of feeling of contribution from one's actions. If the employees believe that their actions can contribute to greater good, such as organizational betterment, it is likely to have a positive impact on their decision to carry out such actions.

3.0 THEORETICAL DEVELOPMENT

In this section we lay the theoretical framework for empirical testing. Based on the arguments presented in the preceding section, we propose a theoretical model presented in Figure 1 which summarizes the proposed hypotheses as well as the nature of each relationship. Specifically, the framework evaluates the relative importance of three incentive mechanisms: (1) penalties; (2) social pressures; and (3) perceived effectiveness. We propose that penalty effects are created by two mechanisms – perceived severity of punishment and perceived certainty of detection - in promoting the security policy compliance. We hypothesize that social pressures exerted by subjective norms (perceived expectation) and descriptive norms (observation) positively influence the compliance intentions. Lastly we propose employee perceived effectiveness of their actions will have positive effect on their compliance intentions. We describe these in more detail in the following subsections.

INSERT Figure 1 HERE

3.1 Penalty – Extrinsic Incentive

Crime and deterrence have been researched from an economic viewpoint for decades. More recently, the analysis of optimal punishment has been applied in the agency theory context. For example, Garoupa [30] models penalties in the context of corporate crime, while, Oliver [46] considers the role of penalties in the case of collective actions. The role of penalties has been considered in many pro-social acts. This stream of research suggests that sanctions against committing a deviant act inhibit potential offenders from

conducting anti-social acts. Ehrlich [24] considers offenders, potential victims, buyers of goods and law enforcement roles based on rules of optimizing behavior in evaluating both positive and negative incentives. His empirical findings suggest that punishment exerts a deterrent effect on offenders. Punishments, alternatively called as penalties or sanction, may include mechanisms such as denunciation, fine, dismissal from job, jail time and others. The deterrence doctrine suggests that perceived threat of sanctions influence personal behaviors through the certainty and severity of punishment; i.e., as punishment certainty and punishment severity are increased, the level of illegal behavior should decrease. Deterrence theory has also been used to study pro-social employee behaviors [35]. There is considerable prior research related to deterrence in organizational settings including information technology. In IT context, Straub [61] notes that deterrence measures are a useful primary strategy for reducing computer abuse.

In the consideration of severity of punishment, the literature suggests that as the level of punishment increases, an individual is less likely to be inclined to carry out a deviant act. In the IS research, specifically in the context of software piracy, Peace et al. [49] found that punishment severity was significantly related to software piracy attitudes in organizations. Similar logic can also be applied to information security context where employees' harmful activities such as non-adherence to security policies can be deterred by imposing penalties. For instance, if employee is caught violating the organizational security policy, the organization can punish the agent by imposing a penalty. If individuals perceive high levels of penalties for non-compliance such as loss of job, heavy fines or other disciplinary actions, their intention to commit undesired behaviors is likely to decrease. Hence we anticipate:

Hypothesis 1 a: Increased severity of penalty will be positively associated with intention to comply with organizational information security policies.

Not only severity but also certainty of organizational action against employees is an important aspect of enforcement. The low probability of being caught is listed as one of the important reasons in a decision to illegally copy software [61]. Deterrence theory, assumes that potential violators are made aware of efforts to control anti-social behaviors. Peace et al. [49] emphasize that simply having the rules

on the books will do little to create change, if the rules are not enforced. In their empirical investigation they found that the certainty of penalty was negatively related to piracy attitudes.

In information security context, enforcing penalties is possible if the organization is able to detect the employee misbehavior. Researchers and practitioners have stressed the importance of auditing mechanisms to inspect end user security behaviors. In general, auditing mechanisms are considered to be a deterrent to a deviant act and is used in variety of context such as tax and corporate reporting. As Vroom and Solms [70] argue to enhance the effectiveness of security policies it is crucial that the employees behave and act responsibly in line with the prescribed security policies of the organization. Achieving this requires some form of investigation and evaluation of the security behavior of the individual.

Thus some kinds of monitoring and detection mechanisms are necessary to make certain that employees are acting in accordance with the security policies. Organizations can deploy various processes and technologies to observe whether the end-user behaviors are in accordance with the policies. These can include random walks through the workplaces, checking computer history logs, network logs, among others. If the employees are aware of monitoring and detection efforts they are more likely to obey the policies with the fear of getting caught and penalized. We expect that with higher awareness of existing detection mechanisms in workplace, employees are more likely to comply with the security policies. Hence we hypothesize

Hypothesis 1b: Increased certainty of detection will be positively associated with intention to comply with organizational information security policies.

3.2 Social Pressures - Extrinsic Incentive

From an incentive perspective, economists have argued that social influences play a significant role in social exchanges taking subtle forms of banishment and withholding of favors [40]. Kreps [40] argues that, if employee fears discharge resulting from low level of effort or fears censure from fellow employees, extrinsic motivations to comply are in play. A norm, or social norm, can be the reason to act, believe or feel. Social influence which is the extent to which one member's social network influences

another member's behavior is exerted through messages and signals that help form perceptions of the value of an activity [67]. There is a long standing distinction in the literature on social influence between the *is* (descriptive) and the *ought* (subjective) meaning of social norms [56]. Individuals are influenced by both - messages about expectations as well as the observed behavior of others. Much of the research in IS has considered the role of social influence in terms of normative beliefs, subjective, peer and descriptive norms. Venkatesh et. al. [68] discuss various constructs that have been considered in the literature and point out that the role of social influence in technology acceptance decisions is complex and could depend on a wide range of contingent influences as well.

Subjective norms are based on normative beliefs and motivation to comply –which is based on the belief as to whether or not a significant person wants the individual to perform the behavior in question. The view that individuals are more likely to comply with relevant others' expectations when those others have the ability to reward the desired behavior or punish non-compliance behavior, is consistent with findings in the technology acceptance literature. While the IT use literature has used variety of labels for subjective norm constructs, each of these constructs contain the notion that the individual's behavior is influenced by what the relevant others expect her/him to do. In consideration of norms in an organizational setting, studies have considered the perception of the expectations of superiors, managers, peers in relevant IS departments [37]. In information security context, if the employee believes that the managers, IT personnel or his peers expect information security policy compliance from her, she is more likely to undertake security actions. Hence we propose,

Hypothesis 2a: Normative beliefs will be positively associated with intention to comply with organizational information security policies.

Subjective norms motivate the individual behavior through the possibility of gaining approval from the significant others. Descriptive norms, on the other hand, refer to the extent to which one believes others are performing the behavior. It focuses on the propensity that an individual may have to indirectly reciprocate the believed behavior of others [56]. Here the individual's behavior is motivated by observing what the typical or normal thing to do is. It is what most people do and "if everyone is doing it, it must be

sensible thing to do” [16]. People often do (or believe) in certain actions or non-actions because many other people do (or believe) the same. Information technology literature has found support for the role of peer behaviors as a motivational source for performing a behavior in question [66, 68]. In the context of security policy compliance, if the employees see their coworkers routinely following the information security practices as directed by the organization they are likely to be inclined to carry out similar behaviors with the fear of being left out. Thus we can expect,

Hypothesis 2b: Peer behavior will be positively associated with intention to comply with organizational information security policies.

3.3 Perceived effectiveness - Intrinsic Incentive

Although, much of agency literature has focused mainly on an agent’s value of extrinsic rewards, individuals value both intrinsic and extrinsic rewards. In recent years, economists have discussed the role of intrinsic value. Researchers have argued that “no artificial incentive can ever match the power of intrinsic motivation” [39]. Benabou and Tirole [7], with a formal analysis that helps reconcile the economic and psychological views, show that the central role played by the phenomena of intrinsic motivation in many social and economic interactions are often quite rational.

Davis [19] argues that subordinates are reinforced by intrinsic intangible rewards such as self actualization and are motivated to work harder. Wasko and Faraj [71] and Ardichvili et al. [6] empirically find that individuals wish for good outcomes not only for themselves but also for the community, other employees and the entire organization. Many social exchanges are motivated by moral obligation and community interest, not by a narrow self-interest [71]. Indeed, employees engage in activities that are beneficial to the organization because they feel a commitment to the organization, and believe that their actions will improve organizational outcomes.

In security behavior context recently some researchers have considered a similar concept [5, 18]. In a survey dealing with citizen information security behaviors in context of home computer use Culnan [18] considered perceived citizen effectiveness; which also was used by Anderson [5] in a study related to security behaviors in the home computing environment. In these studies perceived citizen effectiveness

represented an individual's belief that his individual actions can make a difference in a securing the Internet. With such perceptions, individuals were found to be more likely to undertake favorable security behaviors[5]. Similarly, in the context of security policy compliance in organizations, if employees believe that their actions can make a difference and have an impact on the overall organizational information security goal, they are more likely to undertake security behaviors. Thus we hypothesize

Hypothesis 3: Employee perceived effectiveness of his/her security behavior will be positively associated with the intention to comply with organizational information security policies.

Based on the above discussion in the previous two sections, Table 2 provides a brief summary of the three motivators we use in this study and the supporting literatures.

| Table 2: Constructs and Relevant Agency Literature | | | |
|---|-----------------------------|---|---|
| Motivator | | Related Agency Literature | |
| Extrinsic | Penalty | Severity of Penalty Certainty of Penalty | Penalties: Garoupa [30] Rewards and Punishments: Oliver [46] |
| Extrinsic | Social Pressure | Normative Beliefs Peer Behavior | Conformity: Bernheim [9] Norms: Kreps [40] Socio-economic theory of compliance: Sutinen and Kuperan [64] |
| Intrinsic | Intrinsic Motivation | Perceived Effectiveness | Intrinsic motivation: Benabou and Tirole [7] Moral motivation: Brekke et al. [12] Why incentives plans can't work: Kohn [39] Intrinsic motivations: Murdock [45] |

4.0 RESEARCH METHODOLOGY

4.1 Measurement

In order to maximize the measurement reliability with respect to constructs considered in our study, we selected items that have been tested in extant literatures. The use of pretested and validated questions improves the reliability of the results. The survey instrument was primarily adapted from a variety of previously validated scales. Where necessary, terms were explicitly defined (e.g. IS security, security policies, security precautions) so that each respondent had a common understanding of each term.

Policy compliance intention (CompInt), was considered as a dependent variable in this study.

Although, the information security related behaviors can be diverse, the trend to use appropriate computer

security policies to deal with the issues that can not be handled by automated security systems or IS security personnel continues. Organizations continue to struggle with enforcement of end-user policy. Recognizing the important role of information security policy compliance in achieving information security objectives in organizations, researchers have initiated studies on policy compliance intentions [14, 47]. In our study, the items for policy compliance intention were adapted from a security related study by Anderson [5] on security behaviors in home computer use. Recent studies considering the security policy compliance [14, 47] also gave us insight into the questions. Each item involved a 7-point Likert scale to indicate a respondent's level of agreement with the statements regarding likelihood of complying with the information security policies in their organizations.

To understand the role of penalties, two constructs were used in our study. *Punishment severity (PunSev)* and *certainty of detection (DetCert)* items were adopted from a piracy related study by Peace et al. [49] and information security related study by Knapp [38] which considered policy enforcement dimension by managers. The questions attempted to gauge the level of agreement for the statements related to the likelihood of detection and possible penalty with a set of 7-point Likert scale questions.

In order to understand the role of social pressures, we used *normative beliefs (NormBel)* and *peer behavior (PeerBeh)*. Normative belief questions were taken from the study by Karahanna et al. [37]. Peer behavior questions were adapted from the descriptive norm questions from Anderson study [5]. Items for *Employee perceived effectiveness of his/her security behavior (Eff)* were adapted from the studies by Culnan [18] and Anderson [5]. These items capture individual's belief that her/his individual actions can make a difference in a securing the organizational information systems.

Moreover, to control for explanation of results due to extraneous factors, several control variables were added. These included demographic characteristics such as gender, age and education, as well as size of the company and participant job role. A large, well-organized company and its IT department is likely to have a set of well specified policy and practices in place. Hence size of the company was added as a control variable. Size of the company was measured with reflective measures of the number of computers and number of end-users. Job affiliation of IT or non-IT job was also added as a control

variable since varied participant roles in their organization may show different expectations and appreciation with respect to security policy compliance.

4.2 Instrument Development

When most of the constructs are adopted from earlier studies, although validation may be sound, additional content validation using a multi-stage iterative procedure is recommended [17]. The instrument was pre-tested with field experts through interviews. We sought comments to reduce ambiguity and increase the reliability and validity of survey instrument. A group consisting of MIS, Sociology and Computer Science faculty, three IT professionals from Banking industry and three FBI experts working in cyber security were solicited to achieve content validity and clarify the wording for each item. Items were added, reworded, and deleted in the pretest. The instrument was examined several times by this panel (twice by some experts while three times by others).

We incorporated several procedural remedies to control for common method bias as recommended by Podsakoff, et al. ([51] pp. 888).

1. Increasing validity: concise and clear questions; removing ambiguity of terms used; removing vagueness of questions; avoiding double barreled questions. This was achieved through multi-iterative pretest with the panel. To remove the ambiguity of the terminology used, the participants were given clear instructions on what the terms such as ‘information security policy’ meant.
2. Protecting respondent anonymity and reducing evaluation apprehension: The variables were chosen such that they were informative, but at the same time did not beg sensitive data; so, participants could answer the questionnaire without requiring any special clearance. Furthermore, all precautionary measures were adopted in the survey process to ensure the confidentiality of data.

A pilot test was conducted with a group of undergraduate students, graduate students and employees of a large northeast American university to ensure the initial reliability of the scales and the general mechanics of the questionnaire, such as survey instructions, completion time, and appropriate wording. Consistent placement of items into a particular category demonstrates convergent validity with the related construct, and discriminant validity with the other constructs (as discussed in detail later).

Items that consistently did not match the corresponding construct or were reported to be ambiguous were deleted from the item pool. This process resulted in 18 items finally considered in the instrument for this study (The survey instrument is attached as an Appendix). Responses to all the measurement items ranged from 1 (strongly disagree) to 7 (strongly agree).

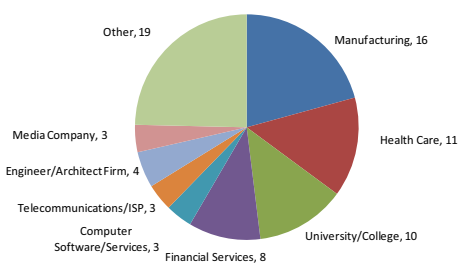
4.3 Survey Administrations and Participants

The study was carried out in collaboration with Cyber Task Force, Buffalo Division, Federal Bureau of Investigation (FBI). Employees from several organizations were requested to participate in the web based survey (10 employees from each organization). Due to the nature of the study, a permission to carry out the employee survey from the top management in each respective organization had to be sought. High level information systems managers in approximately 690 organizations were contacted of which 120 indicated their interest in participation. Subsequently, invitations were distributed to the employees who work in diverse roles but use computers and internet as a part of their daily work routine. Our dataset shows that employees from 77 organizations in Western New York area participated in this study.

Due to the relative sensitive nature of the information sought, many safeguards were put in place to solicit honest responses and encourage participation. Variables were chosen such that they were informative but were not sensitive in nature. Due to the sensitive nature of the study, additional precautionary measures were adopted to ensure the anonymity of survey responses which were reviewed and approved by the university Ethics Review Board. Participants were directed to a survey website hosted on a secure university server. The raw data collected was not available to anyone other than the primary investigator. Moreover, to boost the confidence the survey respondents were assured that no personal information was attached to their responses and data collected was for research purposes only. Code numbers were used to ensure that each respondent completed only one survey. If the participants wished to participate in a draw, they were directed to enter their information on a separate website. Incentives were also offered in the form of draw for several gift certificates of \$25 and \$50 value.

The consideration of various types of organizations as well as participants working in different roles introduces heterogeneity in the sample. The 312 responses represent employees from 77

organizations. The average age of a participant was 42.3 yrs, but ranged from 18 yrs to 70 yrs. The participants worked in varied roles from IT personnel to non-IT personnel, engineer, technician, accounting manager, medical professional, administrative assistant etc. 46% of respondents were female while 54% of the respondents were male. The average education reported was “completed a university or bachelor's degree”. The demographic information about the sample is provided in the Table 3 below.

| Table 3: Demographic Information | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|-------|-------|---|-------|-------|-------|--|--------------------------------|---|--------------|---|--------------|---|----------------|---|-----------------------|---|---------------------|---|---------------------|---|-----------|---|---------|---|-------------------------|---|-----------|---|-----------------------|---|----------------------------|---|
| | Count | % | | Count | % | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Gender | | | Education | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Female | 142 | 46% | Grade school or some high school | 3 | 1.0% | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Male | 168 | 54% | Completed high school | 13 | 4.2% | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Age | | | Some community college or university - did not complete | 43 | 13.8% | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Under 20 | 4 | 1.3% | Completed technical school or a community college | 61 | 19.6% | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 20-29 | 41 | 13.1% | Completed a university or Bachelor's degree | 120 | 38.5% | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 30-39 | 79 | 25.3% | Completed a post-graduate degree such as a Master's or Ph.D. | 71 | 22.8% | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 40-49 | 100 | 32.1% | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 50-59 | 77 | 24.7% | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 60 and above | 11 | 3.5% | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Organization (Sector) Information | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|  | | | <table><tr><th>Other</th><th></th></tr><tr><td>Chemical/Chemical Distribution</td><td>2</td></tr><tr><td>Construction</td><td>2</td></tr><tr><td>Power/Energy</td><td>2</td></tr><tr><td>Transportation</td><td>2</td></tr><tr><td>Beverage Distribution</td><td>1</td></tr><tr><td>Defense Contracting</td><td>1</td></tr><tr><td>Government Facility</td><td>1</td></tr><tr><td>Nonprofit</td><td>1</td></tr><tr><td>Oil/Gas</td><td>1</td></tr><tr><td>Pharmaceutical Research</td><td>1</td></tr><tr><td>Aerospace</td><td>2</td></tr><tr><td>Service_Legal Service</td><td>2</td></tr><tr><td>Service_Personnel Staffing</td><td>1</td></tr></table> | | | Other | | Chemical/Chemical Distribution | 2 | Construction | 2 | Power/Energy | 2 | Transportation | 2 | Beverage Distribution | 1 | Defense Contracting | 1 | Government Facility | 1 | Nonprofit | 1 | Oil/Gas | 1 | Pharmaceutical Research | 1 | Aerospace | 2 | Service_Legal Service | 2 | Service_Personnel Staffing | 1 |
| Other | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Chemical/Chemical Distribution | 2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Construction | 2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Power/Energy | 2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Transportation | 2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Beverage Distribution | 1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Defense Contracting | 1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Government Facility | 1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Nonprofit | 1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Oil/Gas | 1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Pharmaceutical Research | 1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Aerospace | 2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Service_Legal Service | 2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Service_Personnel Staffing | 1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

5.0 DATA ANALYSIS

We use SmartPLS 2.0 for measurement validation and testing the structural model. Created by Ringle, Wende and Will [55], SmartPLS 2.0, is a relatively easy to use software application that allows graphical path modeling with latent variables. SmartPLS uses a Partial Least Square (PLS) regression technique which employs a component-based approach for estimation. It places minimal restrictions on sample size and residual distributions. Randomly selected 100 responses were used to conduct principal components factor analysis. Remaining 212 responses were used to carry out the confirmatory analysis. Bootstrapping of the 212 cases was done with 500 samples for significance testing.

5.1 Measurement Validation

Before testing the hypothesized structural model, the psychometric properties of the measures were evaluated. The normative beliefs was modelled as a formative (aggregate or composite) latent construct, following Karahanna et al. [37] since the indicators theoretically may be seen to employ different themes and may not be interchangeable. For the formative constructs, the examination of weights in the principal component analysis is suggested rather than the evaluation of loadings in common factor analysis [11]. The results indicate that item weightings for three of the five normative beliefs measures were found to be significant. However, to retain content validity [50] all of the indicators were kept in the model. Excessive multicollinearity between the construct items in formative constructs can destabilize the model. Hence a variance inflation factor (VIF) test was used to determine whether the formative measures are highly correlated and to ensure that multicollinearity was not present. VIF statistics for the formative measures were below 3.3 thresholds, suggesting that a high multicollinearity was not present [50].

Although, the issue regarding ‘does the common method variance really bias the results?’ has been debated [23], we conducted the Harman’s single factor test to investigate common method bias [51]. Principal component analysis without rotation revealed five distinct components while the varimax rotated solution showed six factors. Evidence for common method bias exists when one factor accounts for most of the covariance in all factors. Since one factor did not explain much of the variance we can be reasonably assured that the data do not indicate evidence of severe common method bias. Additionally, we conducted a test with an unmeasured latent methods factor¹. In absence of preconceived and directly measured (social desirability or marker) variable, one of the suggested approaches by Podsakoff et al. ([51] pp. 891 and 894) is to test for method bias using a single unmeasured latent method factor. This method involves adding a first order factor to the theoretical model with all of the measures as indicators. The modeling of a latent common method variance factor (LCMV) in PLS was carried out using the approach discussed by Liang et al.[41]. In this approach each indicator is converted into a single-indicator

¹ We are thankful to anonymous reviewers for suggesting that we carry out additional common method bias test and include detailed discussion. We have provided a further discussion on the method bias in the limitations and future research section.

construct making all major constructs of interest second-order constructs. A LCMVF is added by creating a second order construct by linking all the first order constructs. Normative beliefs construct was modeled as a formative construct when we tested our theoretical model. However, to ensure interpretability of results it was modeled as a reflective construct when assessing the common method bias. We tested the theoretical model with the normative beliefs as a formative construct as well as a reflective construct. We found that there were no substantive differences in statistical results. No paths gained or lost statistical significance and no significant paths changed signs. According to Podsakoff et al. [51], in using a latent common methods variance factor test, “items are allowed to load on their theoretical constructs, as well as on a latent common method variance factor (LCMVF), and the significance of the structural parameters is examined both with and without the LCMVF in the model”. As shown in Table 4 our results indicate that the factor loadings in both the models, with and without the LCMVF, are significant and of similar magnitude. Additionally, the path coefficients showed same directions and remained significant.

| Table 4: Common Method Test with Latent Common Method Variance Factor | | | | |
|--|-------------|--|---------|---|
| Construct | Item | Loadings (t value) without LCMVF in the model | | Loadings (t value) with LCMVF in the model |
| Punishment Severity (PunSev) | PunSev1 | 0.889 | (17.02) | 0.871 (45.79) |
| | PunSev2 | 0.743 | (6.22) | 0.853 (35.42) |
| | PunSev3 | 0.778 | (9.41) | 0.730 (13.84) |
| Certainty of Detection (DetCert) | DetCert1 | 0.888 | (28.84) | 0.885 (52.45) |
| | DetCert2 | 0.883 | (25.82) | 0.885 (51.45) |
| Normative Beliefs (NormBel) | NormBel1 | 0.715 | (7.61) | 0.869 (29.51) |
| | NormBel2 | 0.909 | (15.31) | 0.922 (43.64) |
| | NormBel3 | 0.877 | (16.38) | 0.859 (28.94) |
| | NormBel4 | 0.884 | (14.51) | 0.893 (36.52) |
| | NormBel5 | 0.745 | (7.34) | 0.839 (14.95) |
| Peer Behavior (PeerBeh) | PeerBeh1 | 0.927 | (51.20) | 0.940 (81.14) |
| | PeerBeh 2 | 0.912 | (50.70) | 0.933 (86.17) |
| | PeerBeh 3 | 0.897 | (31.69) | 0.870 (23.48) |
| Perceived Effectiveness (Eff) | EFF1 | 0.874 | (13.93) | 0.870 (24.41) |
| | EFF2 | 0.907 | (27.08) | 0.873 (27.14) |
| Compliance Intention (CompInt) | INT1 | 0.931 | (36.04) | 0.948 (50.47) |
| | INT2 | 0.872 | (14.56) | 0.900 (17.76) |
| | INT3 | 0.941 | (60.99) | 0.952 (65.47) |
| Note: All factor loadings are significant at 0.001 level | | | | |

Reliability was calculated using the PLS Internal Consistency Scores which indicate that all principal constructs seem adequate since they exceed the 0.70 threshold. Cronbach alpha values also show adequate reliability -- all exceeding the threshold value of 0.70.

Table 5: Reliability Scores and Cross Correlations

| Constructs | Cronbach Alpha | Composite Reliability Scores | AVE | Cross Correlations of Constructs | | | | | |
|----------------|----------------|------------------------------|-------|----------------------------------|--------------|---------|--------------|--------------|--------------|
| | | | | PunSev | DetCer | NormBel | PeerBeh | EFF | INT |
| PunSev | 0.750 | 0.857 | 0.668 | 0.817 | | | | | |
| DetCer | 0.723 | 0.878 | 0.783 | 0.695 | 0.885 | | | | |
| NormBel | -- | -- | -- | 0.294 | 0.277 | -- | | | |
| PeerBeh | 0.902 | 0.938 | 0.835 | 0.473 | 0.366 | 0.514 | 0.914 | | |
| Eff | 0.714 | 0.862 | 0.758 | 0.160 | 0.093 | 0.296 | 0.072 | 0.871 | |
| CompInt | 0.926 | 0.953 | 0.872 | 0.248 | 0.315 | 0.595 | 0.412 | 0.324 | 0.934 |

Note: The diagonal elements represent the square root of AVE. Normative Belief was formative construct.

Convergent and discriminant validity was tested rigorously using the following five tests: First, the square root of the Average Variance Extracted (AVE) of all constructs is much larger than all other cross-correlations (Table 5). Second, all AVEs are well above 0.50, suggesting that the principal constructs capture much higher construct-related variance than error variance. Third, the correlations among all constructs are all well below the 0.90 threshold, suggesting that all constructs are distinct from each other. Fourth, a principal component factor analysis was performed (Table 6), where all items were loaded on their respective constructs. These were found to be much higher than all cross loadings. Lastly, similar to the principal component factor analysis, a PLS confirmatory analysis also showed an excellent loading pattern which differentiated among the study's principal constructs. Items should load high (>0.7) on their respective constructs and no item should load higher on constructs other than the one it was intended to measure [15]. Cross loadings of items on other latent constructs than their own were found to be at least one magnitude smaller [31]. Jointly, these tests suggest good convergent and discriminant validity. The items and factors presented in tables 4, 5 and 6 were used for further testing of the structural model.

INSERT Figure 2 HERE

5.2 Testing the Model

Results of the structural model testing are presented in Figure 2 and Table 7. Figure 2 presents the path coefficients and their significance levels. The model explained approximately 42 percent variance in the compliance intentions. Contrary to our expectations, severity of penalty ($b = -0.209$, $p < 0.01$) is found to have negative effect on security policy compliance intentions. Certainty of detection ($b = 0.260$, $p < 0.001$) is found to have positive impact on intentions to follow security policies as hypothesized. Thus findings support H1b, but found significant but opposite relationship for H1a.

In evaluating various social pressures, we found that normative beliefs, the pressure from significant others, had a large and significant impact on security policy compliance intentions ($b = 0.395$, $p < 0.001$). Descriptive norm, the behavior of similar others/colleagues, is also found to have a significant impact on security policy compliance intentions ($b = 0.163$, $p < 0.05$). These findings support H2a and H2b. Perceived contribution is found to have significant impact on the security behavior intentions ($b = 0.223$, $p < 0.001$) supporting hypothesis 3. No significant relationships between security behavior intentions and the control variables of age, education, IT or nonIT job affiliation were found. Organizational size of the employee organization was also not found to have a significant effect on employee policy compliance intentions. However, gender was found to have a significant relationship ($b = 0.125$, $p < 0.001$) indicating females have higher policy compliance intentions.

Table 7: Summary of Effects of Motivators on Security Behavior Intention and Hypotheses Testing

| Type | Motivator | Path Coefficient | Hypotheses | Support |
|-------------------------|-------------------------|------------------|------------|--|
| Penalty | Severity of Penalty | - 0. 209 | H1a | No –significant effect in opposite direction |
| | Certainty of Detection | 0.260 | H1b | Supported |
| Social Pressures | Normative Beliefs | 0.395 | H2a | Supported |
| | Peer Behavior | 0.163 | H2b | Supported |
| Perceived Effectiveness | Perceived Effectiveness | 0.223 | H3 | Supported |

6.0 DISCUSSION

6.1 Implications for Theory and Practice

The behavioral research in information security addressed in this article has several theoretical and practical implications. In this paper drawing from the literature in principal agent paradigm we attempt to

understand information security specific employee behaviors in organizations. In general, the principal's goal is to effectively motivate the agent's effort through incentives that recognizes the member's effort as well as environmental factors that have a bearing on the output. Raghu et al. [54]) suggest that an employee behavior is affected by two types of phenomenon: (1) explicit incentives that both agents and organizations understand and (2) implicit psychological contracts governing the perception of obligation and expectations of agents and principal. In this context, theoretically this research evaluates the role of various extrinsic and intrinsic incentive mechanisms in encouraging security behaviors in organizations. Emphasis on behavioral research in information security is just beginning and to the best of our knowledge the role of various extrinsic and intrinsic incentive mechanisms have not been evaluated or empirically tested previously in the context of information security policy compliance.

Our study has several key findings. Our results indicate that both the intrinsic and extrinsic motivators influence employee intentions of security policy compliance in organizations. First, our results show that intrinsic motivation plays a role in employee behaviors related to information security policy compliance. We find that if the employees perceive their security compliance behaviors to have a favorable impact on the organization or benefit an organization, they are more likely to take such actions.

Second, we find that social influence also plays a role in security behaviors. Our results show that normative beliefs have a significant impact on employee behaviors suggesting that the beliefs regarding expectations of superiors, IT management and peers seem to have the most impact on employee security behaviors. Employee perceptions of others complying with the security policies were also found to be significant contributor in employee intentions to comply with the policies themselves.

Certainty of detection was found to have a positive impact on security behavior intention. If the employees perceive that there is higher likelihood of them getting caught if they violate security policies, they are more likely to follow the security policies. Surprisingly, severity of penalty was found to have a negative impact on the security behavior intentions. Some researchers have suggested that incentives and penalties can also play a negative role [7]. In studying the role of penalties, Oliver [46] suggests that negative incentives are effective in motivating unanimous cooperation, but their use is often uneven,

cyclical and may generate hostilities which disrupt that cooperation they enforce. In using the deterrence theory Hollinger [35] notes that empirical research shows evidence that among the three factors of deterrence - severity, certainty and celerity of punishment - perceived certainty of punishment is the most effective in shaping the behavior.

Findings of this study are in line with recent prior research in information security. Although, representing the opinions of the IS managers, Kankanhalli et al. [36] found that deterrent severity in the form of punishments meted out to IS abusers did not seem to affect the security effectiveness. They argue that enforcing more severe penalty for IS abusers does not seem to deter IS abuse. In a more recent study on information security by Pahnilla et al. [47] similarly found that sanctions did not significantly affect employee intentions to comply with security policies. Experts in the field suggest that, this may be due to employees associating terminations for breaking security rules as “one time” issue versus a repeated issue. To understand issues related to this finding, we carried out a post-hoc discussion session in graduate executive level MIS course where all the students had at least three years prior work experience in the IS field. While some pointed out that till the time a penalty action such as dismissal happens most people believe that it is unlikely and do not take it seriously; others suggested that perhaps it has to do with the feeling that penalties really may not apply to them but they may apply to people around them. Some participants suggested stepped approach of evaluation as they had experienced in their workplaces may be a better alternative: sanctions and rewards for their behaviors in point rewards which were in due course considered at the employee annual performance evaluation.

From a practical point, our research provides implications for design, development and implementation of secured systems and security policies. Our results suggest that employee perceived likelihood of getting caught if they violate the security policies was more likely to result in compliance. The existence and visibility of detection mechanisms is perhaps more important than the severity of penalties imposed. Managers need to adopt mechanisms to investigate and evaluate security performance of their employees. These can include informal walk-in checks to monitor the workplace to evaluation of

logs. Although auditing of the employee behavior is suggested, there is very little evidence that it occurs in practice [70].

Findings from the study suggest that the normative beliefs regarding expectations of superiors or managers play an important role in employee behaviors. Not only the expectations of others but the behavior of similar others was found to have significant impact on employee compliance to security policies. This suggests that managers can enhance the security compliance by enhancing appropriate security climate in the organizations. Moreover, if employees perceive that their actions make a difference and aid in achieving overall security, they are more likely to follow the security policies. Overall, it is important for IT management to make efforts to convey to employees that information security is important to an organization and employee actions make a difference in achieving the overall goal of secured information.

6.2 Limitations and Avenues for Future Research

There are several limitations in this study that create opportunities for further research. First, the evaluation of incentives from the principal agent perspective may have limitations. Critics suggest that “agent’s behavioral norms in the principal agent models deviate from commonly held ethical values in society, from models of man in conventional economic theory, and also from behavioral foundations of related business schools fields like corporate strategy, business ethics and human resource management”[10]. While some have expressed concerns regarding agency models due to its cynical model of human nature [13]; Eisenhardt [25] suggests organizational approaches and agency theory can be complementary and evaluated in an integrative manner.

The model considered in this study explained roughly 42 percent of the variance. Additional antecedents may be considered to further increase the explanatory power. Additional factors such as personal or dispositional factors could be included in the model to better understand policy compliance in organizations. The role of the penalties still remain unclear and further research may be needed to evaluate the role of penalty and reward systems in shaping information security behaviors.

This study evaluated the influence of several incentive mechanisms on security policy compliance. In general, extrinsic and intrinsic motivations can be classified as positive (incentive) and negative (disincentive). However, this study considered only positive intrinsic motivations and negative extrinsic motivations. Additional research is needed to evaluate positive extrinsic mechanisms such as reward systems or recognitions and negative intrinsic mechanisms such as perception of loss inflicted by individual action.

Surprisingly much of the research in the information security area has not rigorously tested for the method bias. In information security studies, specifically studies that evaluate behaviors such as piracy behaviors, malicious behaviors, compliance behaviors, social desirability is likely to play a role. Social desirability refers to the need for social approval, acceptance and belief that it can be attained by means of culturally acceptable and appropriate behaviors. Although, we carried out two tests to check for the method bias, caution in interpreting and generalizing the results is necessary. Future studies can consider capturing the social desirability, negative affectivity or other unrelated marker variables as controls. This study uses a cross sectional survey method to understand policy compliance. It is possible that there is a halo effect since the respondents could look retrospectively in answering the survey questions. Future studies, if possible, can consider capturing the information regarding compliant behavior from third party sources. Also researchers could observe the behavior of employees at their work place over a period of time to obtain an assessment of the level of compliance.

7.0 CONCLUSION

End-user security behaviors are an important part of enterprise-wide information security. Our research is an effort to examine various motivating factors that encourage information security behaviors in organizations. In particular, this study explores the role of penalties, pressures and perceived contribution as motivating factors in information security behaviors. For information security researchers, this study makes an important contribution towards understanding the problem of encouraging employee information security behaviors using a theoretically well grounded approach based on micro-economic, sociology and psychology principles. The paper integrates various motivation mechanisms in an

empirically testable model for encouraging security behaviors in organizations. By simultaneously testing the relationships between the penalties, social influence, perceived contribution by employee actions and policy compliance intentions, this study assesses the effectiveness of these motivators and offers suggestions on how managers can enhance the information security policy compliance in their organizations. Our findings suggest that security behaviors can be influenced by both intrinsic and extrinsic motivators. Thus, from the standpoint of information security research, this study is an important contribution to theory as well as practice and fills an important gap in the literature.

ACKNOWLEDGEMENTS

We appreciate the support and collaboration on this project by the Cyber Task Force, Buffalo Division, FBI. Part of this research is funded by NSF under grant # 0402388, grant #0802062 and MDRF grant #F0630. The usual disclaimer applies. We would like to thank the Editor and the three anonymous reviewers for the valuable suggestions during the review process which has helped improve this paper tremendously.

REFERENCES

- [1] 2004 E-Crime Watch Survey Summary of Findings, Computer Emergency Response Team Coordination Center (CERT/CC), (2004).
- [2] 2005 E-Crime Watch Survey Summary of Findings, Computer Emergency Response Team Coordination Center (CERT/CC), (2005).
- [3] Privacyrights.org, A Chronology of Data Breaches, accessed on July 2007. <http://www.privacyrights.org/ar/ChronDataBreaches.htm>.
- [4] E. Albrechtsen, A qualitative study of users' view on information security, Computers & Security, (2006).
- [5] C. Anderson, Creating Conscientious Cybercitizen: An Examination of Home Computer User Attitudes and Intentions Towards Security, presented at Conference on Information Systems Technology (CIST)/INFORMS, (San Francisco, California, 2005).
- [6] A. Ardichvili, V. Page, and T. Wentling, Motivation and Barriers to Participation in Virtual Knowledge-Sharing Communities of Practice., Journal of Knowledge Management, 7 (1), (2003).
- [7] R. Benabou and J. Tirole, Intrinsic and Extrinsic Motivation, Review of Economic Studies, 70, (2003).

- [8] C. J. Bennet and P. M. Regan, Editorial: Surveillance and Mobilities, *Surveillance & Society*, 1 (4), (2004).
- [9] D. Bernheim, A Theory of Conformity, *Journal of Political Economy*, 102 (5), (1994).
- [10] O. Bohren, The Agent's Ethics in the Principle-Agent Model, *Journal of Business Ethics*, 17 (7), (1998).
- [11] K. Bollen and R. Lennox, Conventional Wisdom on Measurement: A Structural Equation Perspective, *Psychological Bulletin*, 110 (2), (1991).
- [12] K. A. Brekke, S. Kverndokk, and K. Nyborg, An Economic Model of Moral Motivation, *Journal of Public Economics*, 87, (2003).
- [13] M. Brennan, Incentives, Rationality, and Society, *Journal of Applied Corporate Finance*, (1994).
- [14] M. Chan, I. Woon, and A. Kankanhalli, Perceptions of Information Security at the Workplace: Linking Information Security Climate to Compliant Behavior, *Journal of Information Privacy and Security*, 1 (3), (2005).
- [15] W. W. Chin, Issues and Opinion on Structure Equation Modeling, *MIS Quarterly*, 22 (1), (1998).
- [16] R. B. Cialdini, R. R. Reno, and C. A. Kallgren, A focus theory of normative conduct: Recycling the concept of norms to reduce littering in public places, *Journal of Personality and Social Psychology*, 58 (6), (1990).
- [17] L. Cronbach, Test validation, in *Educational Measurement*, R. L. Thorndike, Ed., 2 ed, Washington, DC: American Council on Education, 1971)
- [18] M. Culnan, Bentley Survey on Consumers and Internet Security: Summary of Findings, (2004).
- [19] J. Davis, Toward a Stewardship Theory of Management, *Academy of Management Journal*, 22 (1), (1997).
- [20] G. Dhillon and J. Backhouse, Current Directions in IS Security Research: Towards Socio-Organizational Perspectives, *Information Systems Journal*, 11, (2001).
- [21] G. Dhillon and G. Torkzadeh, Value-focused assessment of information system security in organizations, *Information Systems Journal*, 16 (3), (2006).
- [22] T. Dinev, J. Goo, Q. Hu, and K. Nam, User Behavior toward Preventive Technologies – Cultural Differences between the United States and South Korea, *Information Systems Journal*, (Forthcoming).
- [23] D. H. Doty and W. H. Glick, Common Methods Bias: Does Common Methods Variance Really Bias Results? *Organizational Research Methods*, 1 (4), (1998).
- [24] I. Ehrlich, Crime, punishment, and the market for offenses, *Journal of Economic Perspectives*, 10 (1), (1996).

- [25] K. M. Eisenhardt, Control: Organizational and Economic Approaches, *Management Science*, 31 (2), (1985).
- [26] K. M. Eisenhardt, Agency Theory: An Assessment and Review, *The Academy of Management Review*, 14 (1), (1989).
- [27] E. Ferná'ndez-Medina, J. Trujillo, R. Villarroel, and M. Piattini, Access control and audit model for the multidimensional modeling of data warehouses, *Decision Support Systems*, 42, (2006).
- [28] J. Finch, S. Furnell, and P. Dowland, Assessing IT Security Culture: System Administrator and End-User Perspectives, presented at Proceedings of ISOneWorld 2003 conference and convention, (Las Vegas, Nevada, USA, 2003).
- [29] J. Frank, B. Shamir, and W. Briggs, Security-related behavior of PC Users in Organizations, *Information and Management*, 21 (3), (1991).
- [30] N. Garoupa, Corporate Criminal Law and Organization Incentives: A Managerial Perspective, *Managerial and Decision Economics*, 21, (2000).
- [31] D. Gefen and D. Straub, A Practical Guide to Factorial Validity Using PLS-Graph: Tutorial and Annotated Example, *Communications of the Association for Information systems*, 16, (2005).
- [32] A. Gupta and D. Zhdanov, Role of Performance Incentives in Compliance with Information Security Policies, presented at Conference on Information Systems and Technology, (Pittsburgh, PA, 2006).
- [33] M. Gupta, Information Security Manager- M&T Bank, Personal Communication (2007).
- [34] J. T. Hamill, R. F. Deckro, and J. M. K. Jr., Evaluating information assurance strategies, *Decision Support Systems*, 39, (2005).
- [35] R. Hollinger and J. Clark, Deterrence in the Workplace: Perceived Certainty, Perceived Severity, and Employee Theft, *Social Forces*, 62 (2), (1983).
- [36] A. Kankanhalli, H.-H. Teo, B. C. Y. Tan, and K.-K. Wei, An Integrative Study of Information Systems Security Effectiveness, *International Journal of Information Management*, 23, (2003).
- [37] E. Karahanna, D. W. Straub, and N. L. Chervany, Information Technology Adoption Across Time: A Cross-Sectional Comparison of Pre-Adoption and Post-Adoption Beliefs, *MIS Quarterly*, 23 (2), (1999).
- [38] K. J. Knapp, T. E. Marshall, R. K. Rainer Jr, and F. N. Ford, (ISC)2 Inc., Palm Harbor, Florida and Auburn University, Auburn, Alabama., Managerial Dimensions in Information Security: A Theoretical Model of Organizational Effectiveness, accessed on January 2006. https://www.isc2.org/download/auburn_study2005.pdf.
- [39] A. Kohn, Why Incentives Plans Cannot Work, *Harvard Business Review*, (1993).

- [40] D. M. Kreps, The Interaction Between Norms and Economic Incentives, AEA Papers and Proceedings, (1997).
- [41] H. Liang, N. Saraf, Q. Hu, and Y. Xue, Assimilation of Enterprise Systems: The Effect of Institutional Pressures and Mediating Role of the Top Management, MIS Quarterly, 31 (1), (2007).
- [42] K. Loch, S. Conger, and E. Oz, Ownership, Privacy and Monitoring in the Workplace: A Debate on Technology and Ethics, Journal of Business Ethics, 17, (1998).
- [43] Q. Ma and J. M. Pearson, ISO 17799: "Best Practices" In Information Security Management? Communications of the Association for Information Systems, 15, (2005).
- [44] S. Mishra and G. Dhillon, Information Systems Security Governance Research: A Behavioral Perspective, presented at 1st Annual Symposium on Information Assurance, Academic track of 9th Annual NYS Cyber Security Conference, (New York, USA, 2006).
- [45] K. Murdock, Intrinsic motivation and optimal incentive contracts, The Rand Journal of Economics, 33 (4), (2002).
- [46] P. Oliver, Rewards and Punishments as Selective Incentives for Collective Action: Theoretical Investigations, The American Journal of Sociology, 85 (6), (1980).
- [47] S. Pahnla, M. Siponen, and A. Mahmood, Employees' Behavior Towards IS Security Policy Compliance, presented at 40th Hawaii International Conference on System Sciences (HICSS 07), (Hawaii, USA, 2007).
- [48] P. Pavlou, H. Liang, and Y. Xue, Understanding and Mitigating Uncertainty in On-line Exchange Relationships: A Principal-Agent Perspective, MIS Quarterly, 31 (1), (2007).
- [49] A. G. Peace, D. Galletta, and J. Thong, Software Piracy in the Workplace: A Model and Empirical Test, Journal of Management Information Systems, 20 (1), (2003).
- [50] S. Petter, D. Straub, and A. Rai, Specifying Formative Constructs in Information Systems Research, MIS Quarterly, 31 (4), (2007).
- [51] P. M. Podsakoff, S. B. MacKenzie, J.-Y. Lee, and N. P. Podsakoff, Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies, Journal of Applied Psychology, 88 (5), (2003).
- [52] G. V. Post and A. Kagan, Evaluating Information Security Tradeoffs: Restricting Access Can Interfere With User Tasks, Computers & Security, (2006).
- [53] S. Posthumus and R. von Solms, A framework for the governance of information security, Computers & Security, 23 (8), (2004).

- [54] T. S. Raghu, B. Jayaraman, and H. R. Rao, Toward an Integration of an Agent and Activity Centric Approaches in Organizational Process Modeling: Incorporating Incentive Mechanisms, *Information Systems Research*, 15 (4), (2004).
- [55] C. M. Ringle, S. Wende, and A. Will, Institution, SmartPLS 2.0 Beta, accessed on <http://www.smartpls.de>.
- [56] P. Sheeran and S. Orbell, Augmenting the Theory of Planned Behavior: Roles for Anticipated Regret and Descriptive Norms, *Journal of Applied Social Psychology*, 29 (10), (1999).
- [57] M. T. Siponen, A Conceptual Foundation for Organizational Information Security Awareness, *Information Management and Computer Security*, 8 (1), (2000).
- [58] R. v. Solms and B. v. Solms, From Policies to Culture., *Computers & Security*, 23, (2004).
- [59] J. M. Stanton, K. Stam, I. Guzman, and C. Caldera, Examining the Linkages between Organizational Commitment and Information Security, presented at IEEE Systems, Man, and Cybernetics Conference, (Washington, DC, USA, 2003).
- [60] J. M. Stanton, K. R. Stam, P. Mastrangelo, and J. Jolton, Analysis of end user security behaviors, *Computers & Security*, 24 (2), (2005).
- [61] D. Straub, Effective IS Security: An Empirical Study, *Information Systems Research*, 1 (3), (1990).
- [62] D. Straub and R. W. Collins, Key information issues facing managers: Software piracy, proprietary databases, and individual rights to privacy., *MIS Quarterly*, 14 (2), (1990).
- [63] D. W. Straub, Jr. and W. D. Nance, Discovering And Disciplining Computer Abuse In Organization, *MIS Quarterly*, 14 (1), (1990).
- [64] J. G. Sutinen and K. Kuperan, A socio-economic theory of regulatory compliance, *International Journal of Social Economics*, 26 (1/2/3), (1999).
- [65] M. Theoharidou, S. Kokolakis, M. Karyda, and E. Kiountouzis, The Insider Threat to Information Systems and the Effectiveness of ISO17799, *Computers and Security*, 24, (2005).
- [66] R. L. Thompson, C. A. Higgins, and J. M. Howell, Influence of Experience on Personal Computer Utilization, *Journal of Management Information Systems*, 11 (1), (1994).
- [67] V. Venkatesh and S. Brown, A Longitudinal Investigation of Personal Computers in Homes: Adoption Determinants and Emerging Challenges, *MIS Quarterly*, 25 (1), (2001).
- [68] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, User Acceptance of Information Technology: Toward a Unified View, *MIS Quarterly*, 27 (3), (2003).
- [69] M. Vroblefski, A. Chen, B. Shao, and M. Swinarski, Managing user relationships in hierarchies for information system security, *Decision Support Systems*, 43, (2007).

- [70] C. Vroom and R. von Solms, Towards information security behavioural compliance, *Computers & Security*, 23 (3), (2004).
- [71] M. M. Wasko and S. Faraj, It is What One Does: Why People Participate and Help Others in Electronic Communities of Practice, *Journal of Strategic Information Systems*, 9, (2000).

APPENDIX

Survey Instrument

| | | | |
|--|------------------------------|--|---|
| Perceived Effectiveness [5, 18] | Perceived Effectiveness | EFF1 EFF2 | Every employee can make a difference when it comes to helping to secure the organization's information systems. If I follow the organization IS security policies, I can make a difference in helping to secure my organization's information systems. |
| Penalties [38, 49] | Severity of Penalty | PunSev1 PunSev2 PunSev3 | The organization disciplines employees who break information security rules. My organization terminates employees who repeatedly break security rules. If I were caught violating organization information security policies, I would be severely punished |
| | Certainty of Detection | DetCert1 DetCert2 | Employee computer practices are properly monitored for policy violations. If I violate organization security policies, I would probably be caught. |
| Pressures [5, 37] | Normative Beliefs | NormBel1 NormBel2 NormBel3 NormBel4 NormBel5 | Top management thinks I should follow organizational IS security policies. My boss thinks that I should follow organizational IS security policies. My colleagues think that I should follow organizational IS security policies. The information security department in my organization thinks that I should follow organizational IS security policies. Computer technical specialists in the organization think that I should follow organizational security policies. |
| | Peer Behavior | PeerBeh1 PeerBeh 2 PeerBeh 3 | I believe other employees comply with the organization IS security policies. I am convinced other employees comply with the organization IS security policies. It is likely that the majority of other employees comply with the organization IS security policies to help protect organization's information systems. |
| Policy Compliance Intention [5, 14, 47]. | Policy Compliance Intentions | INT1 INT2 INT3 | I am likely to follow organizational security policies. It is possible that I will comply with organizational IS security policies to protect the organization's information systems. I am certain that I will follow organizational security policies. |

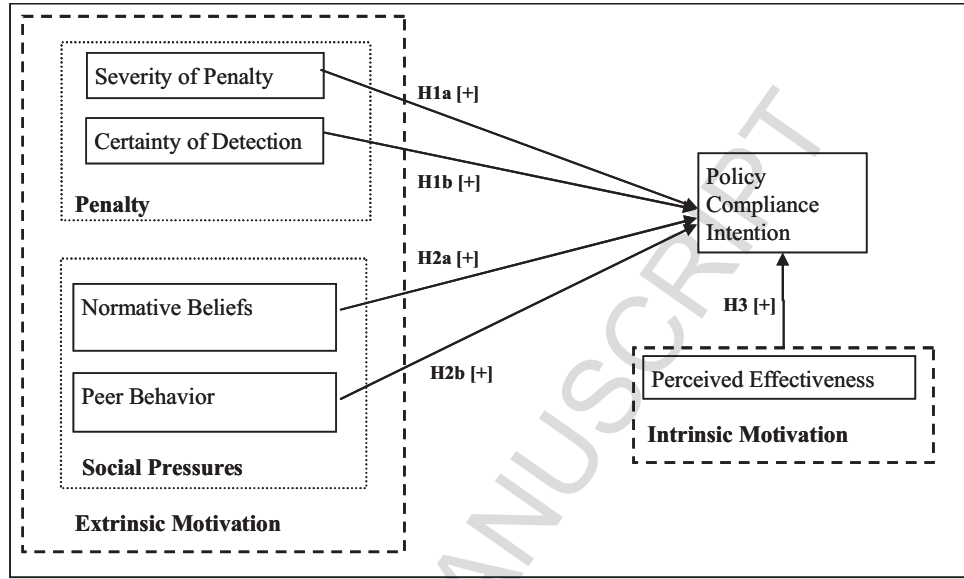


Figure 1: Intrinsic and Extrinsic Motivators in Information Security Behaviors

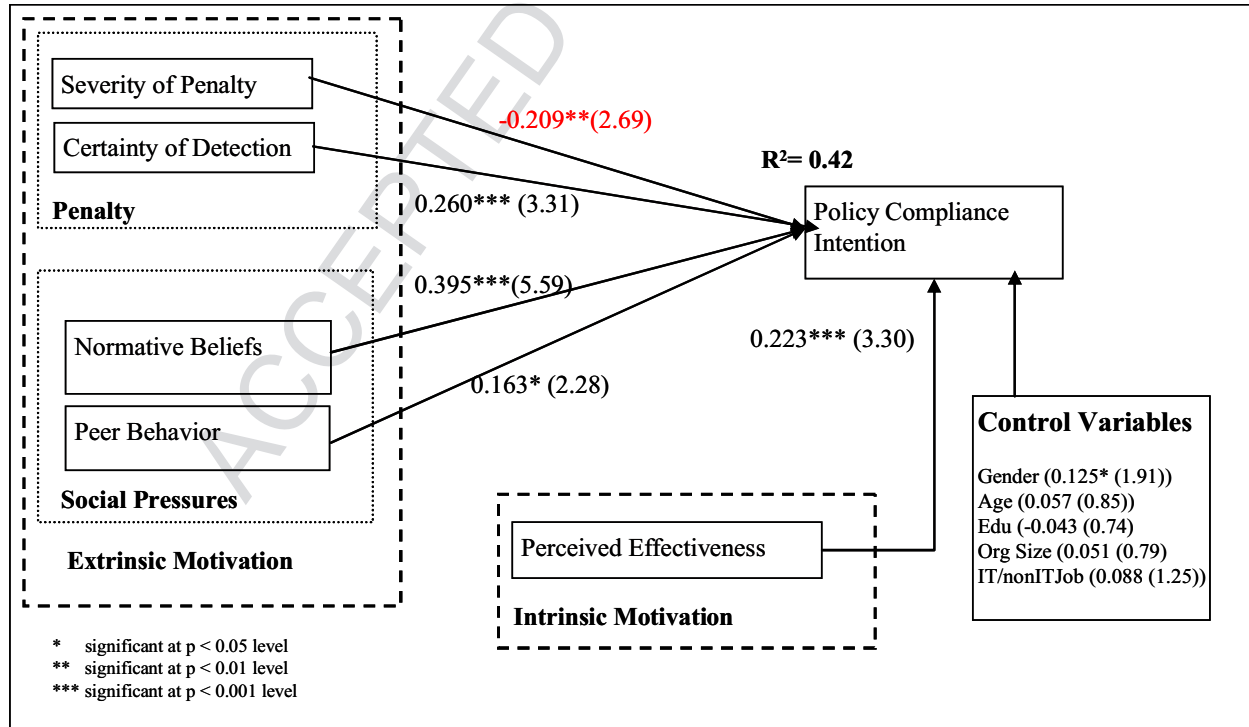


Figure 2: Intrinsic and Extrinsic Motivators in Information Security Behaviors

Table 1: Selected Prior Research in Behavioral Information Security

| Title | Related Literature with Research Focus | Theories Used/Proposed | Core of the literature |
|--|--|--|--|
| Conceptual Papers in Behavioral Security: | Posthumus and von Solms [53], Vroom and von Solms [70] | Components of effective security governance. | Papers with discussion on components of security governance and conceptual perspectives on end user behaviors |
| | Mishra and Dhillon [44] | | |
| | Dhillon and Backhouse [20] | Socio-organizational or behavioral approach to security | |
| | Straub and Nance [63] | Need for more empirical research using socio-organizational perspectives to develop key principles for the prevention of negative events that will help in the management of information security. | |
| | Siponen [57] | Factors affecting malicious use in organizations | |
| | Theoharidou et.al.[65] | Conceptual foundation for organizational information security. | |
| | Albrechtsen [4] | Insider threats to information systems and effectiveness of ISO17799. | |
| Empirically tested studies in Behavioral Security: | Anderson [5] | Qualitative study of users' view on information security. | Papers with end user behaviors in variety of contexts such as security tool use, home users, password practices etc. |
| | Dinev et.al [22] | Security behavior of internet users in the home setting | |
| | Stanton [59] | User behavior in using preventative technologies | |
| | Post [52] | Role of organizational commitment on various security related behaviors. | |
| | Peace et.al. [49] | Security perceptions in organizations - found that end users perceived security practices to be hindrance to their normal routine. | |
| | Pahnila et al. [47] | Piracy in workplaces | |
| Papers focusing on Security Policy Compliance | Chan et.al. [14] | Role of threat appraisal, facilitating conditions, and information quality on IS security policy compliance | Information security policy compliance research is still in early stages; [32]analytically evaluate incentive mechanisms, it remains empirically untested. |
| | Gupta and Zhdanov [32] | Role of security climate on security policy compliance. | |
| | | Game theory to evaluate the role of performance incentives in security policy compliance. | |

Table 6: Exploratory and Confirmatory Factor Analysis

| Construct | Item | Principal Component Analysis with Varimax Rotation (EFA) (n=100) | | | | | | | Confirmatory Factor Analysis (CFA- PLS) (n=212) | | | | | | | PLS Weight (sig p value) |
|----------------------|-----------|--|---------|---------|---------|--------|---------|--------|---|---------|---------|--------|---------|--|---------------|--------------------------|
| | | PunSev | DetCert | NormBel | PeerBeh | Eff | Complnt | PunSev | DetCert | NormBel | PeerBeh | Eff | Complnt | | | |
| PunSev (reflective) | PunSev1 | 0.786 | 0.170 | 0.107 | 0.363 | 0.075 | 0.136 | 0.889 | 0.598 | 0.262 | 0.427 | 0.190 | 0.219 | | | |
| | PunSev2 | 0.863 | 0.097 | 0.143 | 0.093 | -0.075 | 0.004 | 0.743 | 0.479 | 0.176 | 0.320 | 0.095 | 0.088 | | | |
| | PunSev3 | 0.799 | 0.182 | 0.077 | 0.281 | 0.066 | 0.011 | 0.778 | 0.553 | 0.254 | 0.354 | 0.118 | 0.185 | | | |
| DetCert (reflective) | DetCert1 | 0.186 | 0.849 | 0.130 | 0.140 | -0.043 | 0.123 | 0.585 | 0.888 | 0.228 | 0.272 | 0.109 | 0.262 | | | |
| | DetCert2 | 0.325 | 0.646 | 0.003 | 0.368 | 0.135 | 0.060 | 0.623 | 0.883 | 0.224 | 0.377 | 0.051 | 0.256 | | | |
| NormBel (formative) | NormBel1 | 0.218 | -0.050 | 0.759 | 0.317 | 0.144 | 0.181 | 0.287 | 0.268 | 0.715 | 0.454 | 0.242 | 0.401 | | -0.181 (ns) | |
| | NormBel2 | 0.082 | -0.007 | 0.812 | 0.099 | 0.163 | 0.381 | 0.249 | 0.212 | 0.909 | 0.394 | 0.254 | 0.510 | | 0.477 (<0.05) | |
| | NormBel3 | 0.269 | 0.171 | 0.700 | 0.083 | -0.082 | 0.118 | 0.335 | 0.276 | 0.877 | 0.492 | 0.238 | 0.492 | | 0.355 (<0.05) | |
| | NormBel4 | -0.010 | -0.023 | 0.809 | 0.202 | 0.146 | 0.246 | 0.262 | 0.251 | 0.884 | 0.398 | 0.252 | 0.496 | | 0.370 (<0.05) | |
| | NormBel5 | -0.069 | 0.303 | 0.629 | 0.053 | 0.260 | 0.300 | 0.187 | 0.153 | 0.745 | 0.317 | 0.197 | 0.418 | | 0.077 (ns) | |
| PeerBeh (reflective) | PeerBeh 1 | 0.208 | 0.158 | 0.233 | 0.906 | 0.027 | 0.073 | 0.437 | 0.396 | 0.404 | 0.927 | -0.018 | 0.300 | | | |
| | PeerBeh 2 | 0.207 | 0.120 | 0.177 | 0.898 | 0.025 | 0.099 | 0.450 | 0.327 | 0.383 | 0.912 | 0.065 | 0.285 | | | |
| | PeerBeh 3 | 0.290 | 0.171 | 0.155 | 0.808 | 0.071 | 0.191 | 0.391 | 0.290 | 0.439 | 0.897 | 0.097 | 0.391 | | | |
| Eff (reflective) | EFF1 | 0.053 | -0.082 | 0.086 | 0.006 | 0.885 | 0.168 | 0.137 | 0.045 | 0.247 | 0.034 | 0.874 | 0.267 | | | |
| | EFF2 | -0.023 | 0.150 | 0.228 | 0.094 | 0.815 | 0.206 | 0.176 | 0.112 | 0.235 | 0.066 | 0.907 | 0.308 | | | |
| Complnt (reflective) | INT1 | 0.122 | 0.112 | 0.275 | 0.166 | 0.114 | 0.831 | 0.195 | 0.278 | 0.555 | 0.281 | 0.298 | 0.931 | | | |
| | INT2 | 0.002 | 0.042 | 0.270 | 0.073 | 0.139 | 0.861 | 0.1644 | 0.156 | 0.443 | 0.395 | 0.295 | 0.872 | | | |
| | INT3 | 0.034 | 0.098 | 0.352 | 0.121 | 0.255 | 0.831 | 0.246 | 0.355 | 0.536 | 0.332 | 0.299 | 0.941 | | | |