Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior

Mark Chan, National University of Singapore
Irene Woon, National University of Singapore
Atreyi Kankanhalli, National University of Singapore

ABSTRACT

A large number of information security breaches in the workplace result from employees' failure to comply with organizational information security guidelines. Recent surveys report that 78% of computer attacks appear in the form of viruses embedded in email attachments. Employees who open e-mail attachments from unknown sources risk infecting their own computers as well as other computers sharing the same network. Therefore, more attention needs to be paid to learning why non-compliant behavior takes place so that appropriate measures for curbing the occurrence of such behavior can be found. With such motivation in mind, this study examines the effects of social contextual factors on employees' compliance with organizational security policies. The research model is developed based on concepts adapted from safety climate literature that has been used to explain the safe behavior of employees in organizations. Data was collected from a sample of 140 employees from two large IT intensive organizations using a 28-item survey instrument and analyzed using structured equation modeling. Management practices, supervisory practices, and coworker's socialization were found to be positively related to employees' perception of information security climate in the organization. Perception of security climate and self-efficacy had positive impacts on compliant behavior. Implications of this study for research and practice are discussed.

INTRODUCTION

In recent years, organizations have increased spending on both physical and IT security technologies (Computer Security Institute 2004). Despite the increased expenditure, organizations encounter a number of security incidents as a result of staff errors and misdemeanors. Contrary to the general perception that organizations are mainly vulnerable to external threats, a majority of misuse incidents are in fact committed by employees. Survey reports suggest that 78 % of computer attacks occur in the form of viruses (Computer Security Institute 2004), which are activated through e-mail attachments that have been opened by employees (PriceWaterHouseCoopers 2004). Since these

information security incidents occur as a result of employees' failure to observe work procedures according to information security guidelines, it is important for organizations to identify and employ measures that facilitate employee's compliance with suggested guidelines.

Past research on employees' information security related behavior has focused mainly on employee computer abuse in the organization (Limayem, Khalifa & Chin 1999; Anandarajan 2002; Galletta & Polak 2003). However, employee computer abuse does not encompass all information security incidents that are caused by employees. For example, factors such as the lack of information security awareness or performance pressure could be contributing factors. In general, it has been suggested that the assurance of information security will require a multifaceted approach, encompassing both social and technical factors (Straub & Welke 1998; Dhillon & Backhouse 2001). Based on the above practical and theoretical motivations, this research proposes to study employees' behavior toward complying with information security guidelines in an attempt to develop a more comprehensive understanding of the causes of information security incidents.

This study is based on the social information processing approach, which suggests that contextual factors of the organization are significant in explaining job perceptions of individuals (Salancik & Pfeffer 1977). In accordance with this approach, past research suggests that organizational climate perceptions are crucial determinants of individual behavior in organizations (Campbell, Dunnette, Lawler & Wick 1970; Payne & Mansfield 1978). This study develops a model that considers organizational (climate) and individual (self-efficacy) antecedents of compliant behavior. Further, social contextual factors (management practices, supervisory practices and co-workers' socialization) that are likely to impact organizational climate perceptions are identified. The model is tested using a survey of employees in two large IT intensive organizations. The theoretical and practical implications of the findings are discussed.

CONCEPTUAL BACKGROUND

The social information processing approach (Salancik & Pfeffer 1977) suggests that contextual factors are more significant than personal predispositions in explaining job perceptions of individuals. The logic is, since people are adaptive organisms, they will have a tendency to display behaviors and beliefs which are in alignment with their social context. This reasoning suggests that one can learn most about individual behavior by studying the informational and social environment within which the behavior occurs and to which it adapts (Salancik & Pfeffer 1978; Taylor & Fiske 1978). The

perceptions of the organizational environment that are likely to influence an employee's behavior are referred to as organizational climate.

Organizational Climate

Organizational climate is defined as a set of attributes specific to a particular organization that may be induced from the way the organization deals with its members and its environment (Campbell et al., 1970). Organizational climate perceptions are seen as crucial determinants of individual behavior in organizations by mediating the relationship between objective characteristics of working conditions (organizational policies, practices, and procedures) and an individual's working behavior (Campbell et al. 1970). Perceptions of climate are assumed to act as a psychological utility, which serves as a frame of reference for guiding appropriate behavior (Schneider 1975). In other words, the events in the organization as observed by an individual can serve as signals, which indicate the key priorities valued by the organization. Therefore, climate is considered to be a perceptual medium through which the effects of the organizational context are translated into an employee's behavior.

The objective characteristics of the organization have been considered as the antecedents of organizational climate. The individual's interpretive perception of these characteristics ascribes meaning to the organizational context (James & Jones 1974). The effects of top-down (vertical) and cross-level (horizontal) contextual factors on individual perceptions, attitudes, and behavior have been studied (James & Jones 1976). Thus group and organization factors provide the context for individual perceptions, attitudes, and behaviors and need to be explicitly incorporated into models of organizational behavior.

Although the concept of culture is not adopted in this study, there is a need to distinguish between culture and climate for the sake of clarity. Organizational culture refers to values, beliefs and assumptions found in the deep structure of organizations, which are held by its members. Climate, in simple terms, refers to the perceptions of organizational policies, practices, and procedures both formal and informal (Reichers & Schneider 1990). Although both concepts are similar, they are not identical. Previous research views climate as organizational members' perceptions of "observable" practices and procedures that are closer to the "surface" of organizational life and are a manifestation of culture (James & Jones 1974). Culture, on the other hand, is deeply embedded within the organizational environment and viewed as a deeper, less consciously held set of meanings compared to climate (Reichers & Schneider 1990). Climate, being more apparent and visible, could provide researchers with a glimpse of the underlying, less observable culture that resides within the organization.

Safety Climate

In recent years, there has been a paradigm shift in the area of climate research. Earlier studies took a more generic perspective of organizational climate while recent climate studies have focused on the specific facets of climate within the organization (Schneider 2000). There is emerging evidence that specific climates are predictive of specific outcomes (Carr, Schimdt, Ford & DeShon 2003). For example, studies (Zohar 1980) showed that employees complied with safety guidelines when working in organizations with a strong safety climate. Similarly, studies conducted for motivation climate (Litwin & Stringer 1968) and creativity climate (Taylor 1972) derived similar results in their respective fields. The concept of safety climate is considered useful for this study since information security can be considered as a form of safety in the organization.

There are a number of characteristics of safety programs common to information security programs in organizations. First, information security and safety share non-functional characteristics. In other words, both safety and information security are essentially non-value adding components of an organization's operations but nonetheless remain critical to the business. Second, success of safety and information security programs is achieved through the non-occurrence of incidents, in part due to employee compliance of appropriate work procedures. Both types of programs try to reduce potential loss through a reduction in occurrences of accidents. Although information security incidents do not normally result in physical harm to the individual (unlike safety-related mishaps), employees still face potential loss as a result of valuable work information being irretrievable in the event of an incident. Last, the observance of both safety and information security guidelines usually creates inconveniences and, more often than not, are in direct conflict with work efficiency and productivity.

Safety Climate Dimensions	
• Perceived importance of safety training programs • Perceived effects of safe conduct on promotion • Perceived effects of required work pace on safety • Perceived effects of safe conduct on social issues	• Perceived management attitudes toward safety • Perceived level of risk in work place • Perceived status of safety officer • Perceived status of safety committee

Table 1. Dimensions of Safety Climate adapted from Zohar (1980)

The concept of safety climate was first proposed by Zohar (1980) who identified the various dimensions that constitute safety climate (see Table 1). The results of this study showed that employees who perceived a strong safety climate in the organization worked safer. As a consequence, these organizations were observed to report fewer accidents. In line with this research, the concept of safety climate has been popular in subsequent studies in the field of safety although the dimensions used to measure safety climate varied. However, results from these studies indicate strong evidence of the presence of a positive relationship between safety climate and employee behavior in contexts as varied as the manufacturing, mining, construction, and armed forces (Dejoy 1996; Zohar & Luria 2004).

RESEARCH MODEL AND HYPOTHESES

The definition for our dependent variable compliant information security behavior has been adapted from Griffin & Neal's (2000) definition of safety compliant behavior. Compliant information security behavior refers the set of core information security activities that need to be carried out by individuals to maintain information security as defined by information security policies. To be able to carry out a recommended (compliant) behavior, an employee need not only be influenced by a conducive information security climate, but also needs the skills to perform the required actions. Previous studies have shown that individuals with self-efficacy i.e., who believe that they have the ability to perform a behavior, would be motivated toward that behavior (Bandura 1977; Chambliss & Murray 1979). Therefore, in addition to perception of information security climate, self-efficacy is considered an antecedent of compliant behavior in our model.

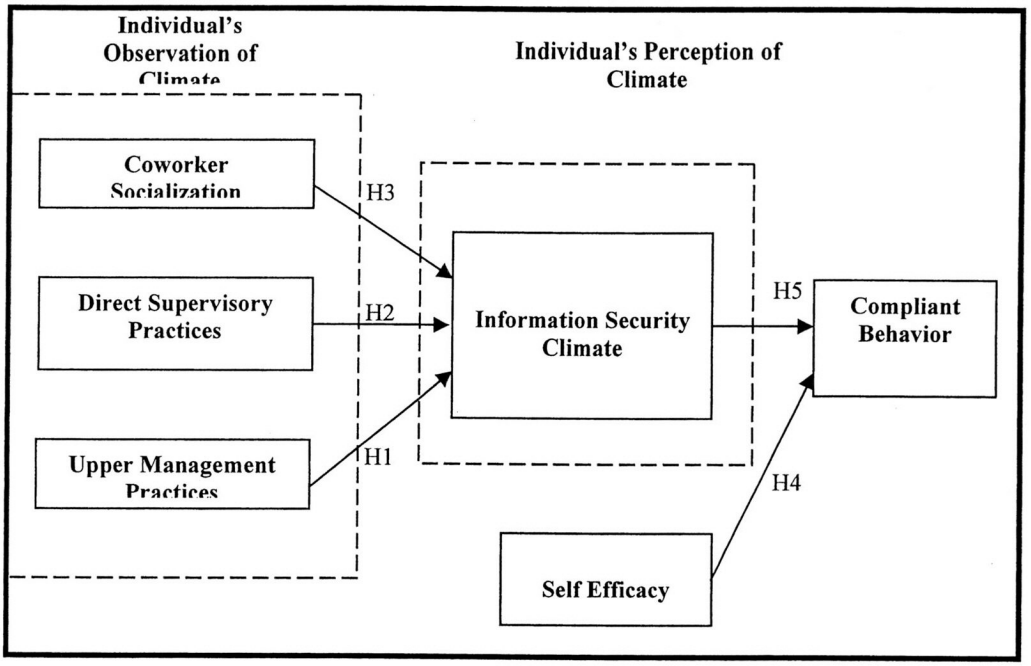


Figure 1: Research Model for Employee Compliant Behavior

Further, the perception of organizational climate by an employee can be influenced by cross-level (horizontal) and top-down (vertical) characteristics (James & Jones 1976). Cross-level characteristics include socialization with coworkers and peers. Top-down characteristics include supervisory practices of direct supervisors as well as practices of upper management. It is this aggregate view of organizational climate perception that makes up the single measure, which best estimates the general effect (Payne & Mansfield 1978). Adopting this view, our model considers co-worker socialization, direct supervisory practices, and upper management practices, as antecedents of an employee's perception of the information security climate. The research model is shown in Figure 1.

Upper Management Practices

Upper management practices refer to the customary actions of management as observed by the individual employee. Research has shown that upper management commitment is a critical element in successful safety programs (e.g., Cohen 1977; Zohar 1980). The role of upper management in providing a safe organizational climate has been indicated in a variety of industries (Barling, Loughlin & Kelloway 2002). Management commitment toward safety is demonstrated through practices such as outlining a written safety policy as well as providing training and awareness programs. Previous

studies have shown that policies (Schneider 1975; Mullen 2004) and training are strong predictors of climate (Diaz & Cabrera 1997; Dejoy, Schaffer, Wilson, Vanderberg & Butts 2004). While past research has focused on upper management practice in safety programs, we also expect that supportive upper management practices will have a positive effect on individual employee's perception of the information security climate.

H1: There is a positive relationship between upper management practices and employee's perception of the information security climate.

Direct Supervisory Practices

Direct supervisory practices refer to the repeated actions of direct supervisors as observed by the individual employee. Supervisors as official agents of the organization have the most frequent interaction with direct subordinates. This makes them ideal candidates for communicating and enforcing organizational goals to employees. Studies have shown that an improvement in supervisory practices significantly enhances an employee's perception of safety climate and consequently leads to higher levels of safety (Zohar 2002; Zohar & Luria 2003; Zohar & Luria 2004). For example, employees who observe their supervisors as giving greater emphasis to performance over the observance of prescribed safety procedures would perceive lower priority for these procedures. This can happen even when upper management policy places top priority on safety. Hence, we hypothesize a positive link between direct supervisory practices and an employee's perception of the information security climate.

H2: There is a positive relationship between direct supervisory practices and an employee's perception of the information security climate.

Coworker Socialization

Coworker socialization refers to the daily interactions that the individual has with coworkers. Socialization includes conversations, observing behavior of coworkers and the consequences of a certain behavior (Barling et al. 2002). Previous research indicates that socialization has an effect on a worker's perception of climate in several industries including police, healthcare, and utilities (Mullen 2004). Socialization may affect perception of climate since it can indicate to employees how organizational policies and procedures are actually enacted with reference to their peers. Hence we expect

that co-worker socialization will have a positive influence on employee's perception of the organization's information security climate.

H3: There is a positive relationship between co-worker socialization and the employee's perception of the information security climate.

Self-Efficacy

Self-efficacy refers to an individual's belief in his/her own ability to perform a specific task (Bandura 1977). Self-efficacy in information security is developed through the ongoing acquisition of knowledge related to information security possibly from the training that one receives. Previous studies have shown the link between self-efficacy and behavior (Bandura 1977; Chambliss & Murray 1979). Hence self-efficacy in information security is expected to influence compliant behavior.

H4: There is a positive relationship between self-efficacy and the employee's willingness to exhibit compliant behavior.

Perceived Information Security Climate

Perceived information security climate is defined as the employee's perception of the current organizational state in terms of information security as evidenced through dealings with internal and external stakeholders (Campbell & Beaty 1971). Perceptions of the climate are derived from observance of organizational management, superior, and peer attitudes. Studies have shown that a positive change in safety climate perceptions results in a corresponding change in physical safety behavior (Zohar 2000; Zohar & Luria 2004). Extending this logic to the information security context, we expect that employees who perceive a strong information security climate in the organization would be more likely to exhibit compliant behavior.

H5: There is a positive relationship between the employee's perception of the information security climate and compliant behavior.

METHODOLOGY

Operationalization and Data Collection

The proposed research model was empirically tested through the use of survey methodology. The survey instrument was developed through a systematic procedure suggested by Churchill (1979). This process involved specifying the domain of the construct, delineating what is included and what is excluded, generating sample of items from past literature, iteratively refining the instrument through data collection, and assessing the reliability and validity of the data. Table 2 shows the construct items used in the survey after these were verified through interviews with domain experts as well as labeled and unlabeled sorting (Moore & Benbasat 1991). All items were measured using a 7 point Likert scale anchored from Strongly Disagree to Strongly Agree.

Data was collected from employees working in two IT intensive organizations in the logistics and petrochemical industries. The target respondents for this study were employees who have worked for a year or more in their current place of work and have easy access to computer systems at their workplace. The survey was administered at their place of work. Out of a total of 140 survey forms distributed, 119 responses were returned giving a response rate of 85%. Out of these, 15 incomplete or invalid responses were removed leaving behind a final sample of 104 for analysis. Interviews with the IT managers and perusal of the security policies in both organizations indicated that the two organizations were similar in terms of information security policies and procedures. Also, a T-test was conducted to check for significant difference between the two organizations. As there was no significant difference at the 0.001 level, the two sets of data were pooled together for analysis. Descriptive statistics relating to respondents' demographics are shown in Table 3.

Upper Management Practices		***Source***
Mgmt1	My organization gives me specific training about the information security procedures that I need to follow when performing my daily work	Martins & Eloff 2001
Mgmt2	My organization educates me on the importance of information security	
Mgmt3	Corporate information security policies are readily available for my reference	Barling et al. 2002
Mgmt4	Corporate information security policy contains a comprehensive set of written rules and procedures guiding appropriate information security behavior	Self Developed
Mgmt5	There is strict enforcement of written corporate information security rules	Straub 1990
Direct Supervisory Practices		
Sup1	My supervisor updates me on changes to information security procedures. e.g. through direct verbal communication or via communication tools	Hayes et al. 1998
Sup2	My supervisor discusses information security issues with me and my co-workers	
Sup3	My supervisor praises me when I adopt proper information security practices	Beland & Dedobbeleer 1991
Sup4	My supervisor considers information security compliance as a key factor in assessing my overall performance	Self Developed
Co-Worker Socialization		
Cowork1	Co-workers tend to ignore information security procedures when rushing deadlines ***(reverse)***	Hayes et al. 1998
Cowork2	Co-workers discuss information security issues with me	
Cowork3	Co-workers would report breaches of information security to superiors	
Perception of Information Security Climate		
Perp1	The organization sets high standards for the protection of its information assets	Schnake 1983

Perp2	Management is concerned with information security of the organization	Neal & Griffin 1997
Perp3	My supervisor is concerned with information security of the organization	
Perp4	My coworkers are concerned with information security of the organization	
Self Efficacy		
Effi1	I am able to identify a breach in information security even if there is no one to help me	Compeau & Higgins 1995
Effi2	I am able to identify a breach in information security, even if I do not have a copy of written procedures and rules to refer to	
Effi3	I am able to identify a breach in information security even if I have not seen a similar situation occurring before	
Effi4	I am aware of what to do in the event of a information security breach even if there is no one to tell me what to do	
Effi5	I am aware of what to do in the event of a information security breach, even if I do not have a copy of written procedures and rules to refer to	
Compliant Behavior		
Comply1	I will comply with information security procedures when performing my daily work	Neal & Griffin 1997
Comply2	I tend to ignore information security procedures that I think are not necessary ***(reverse)***	Hayes et. al 1998
Comply3	I tend to ignore information security procedures in order to complete my work quickly ***(reverse)***	
Comply4	Sometimes I do not comply with information security procedures when it affects the performance / productivity of my work ***(reverse)***	Self Developed
Comply5	I tend to comply with information security procedures only when it is convenient to do so ***(reverse)***	Self Developed
Comply6	I tend to ignore information security procedures when I am busy ***(reverse)***	Self Developed

Table 2: Survey Items

	Frequency	Percentage
Age		
20-30	34	32.69
30-40	48	46.15
40-50	19	18.27
>50	3	2.88
Gender		
Male	81	77.88
Female	23	22.12
Education Level		
Diploma	16	15.38
Bachelors	35	33.65
Masters	15	14.42
Doctorate	12	11.54
Others	4	3.85
No of years in the current organization		
1-6	74	71.15
7-12	21	20.19
> 13	9	8.65
Total number of years of working experience		
1-6	51	49.04
7-12	27	25.96
> 13	26	25.00

Table 3: Demographic Profile of Respondents

Data Analysis

Partial least squares (PLS), a structural equation modeling tool, was used to analyze the data. Structural equation modeling enables researchers to examine the structural component (path model) and measurement component (factor model) simultaneously (Gefen, Straub & Boudreau 2000). PLS was used in our analysis for several reasons. First, PLS is able to handle both formative (e.g., upper management practices in our study) and reflective variables (e.g., remaining constructs in our study) that exclusively or jointly exist in a single structural model. Second, PLS supports exploratory studies such as ours. Last, PLS makes less rigid assumptions compared to other methods (Compeau, Higgins & Huff 1999) in that it accepts latent constructs

under conditions of non-normality in small to medium sample sizes (Chin 1998).

RESULTS

Measurement Model

The measurement model consists of relationships between the constructs and the items used to measure them. Testing the measurement model involves assessing the convergent validity and discriminant validity of the instrument items. Convergent validity is the degree to which two or more items measuring the same constructs agree (Cook & Campbell 1979). Discriminant validity is the degree to which items differentiate between constructs or measures distinct concepts. The model under study consists of five reflective constructs (direct supervisory practices, co-worker socialization, perception of information security climate, self-efficacy, and compliant behavior) and one formative construct (upper management practices). Items measuring reflective constructs represent the effects of the construct under study whereas items under a formative construct are representative of the construct in question (Bollen 1984). Since the various items of formative constructs are indicative of different dimensions, unlike items of reflective constructs, they are not required to exhibit convergent validity (Chin 1998). Instead, the level of contribution and relevance of the formative items to their respective constructs can be determined by looking at the absolute value of the item weights (Chin & Sambamurthy 1994).

Constructs and Items	Cronbach's Alpha	Alpha if Deleted	Item Loadings *	Composite Reliability	Average Variance Extracted (AVE)
Direct Supervisory Practices	0.91			0.93	0.71
Sup1		0.88	0.88		
Sup2		0.86	0.91		
Sup3		0.91	0.83		
Sup4		0.89	0.88		
Co-worker Socialization	0.79			0.87	0.63
Cowork1		0.70	0.88		
Cowork2		0.69	0.80		
Cowork3		0.77	0.78		
Perception of climate	0.87			0.91	0.73
Perp1		0.81	0.90		
Perp2		0.83	0.89		
Perp3		0.84	0.87		
Perp4		0.86	0.82		
Self-Efficacy	0.90			0.92	0.71
Effi1		0.87	0.87		
Effi2		0.86	0.81		
Effi3		0.86	0.79		
Effi4		0.87	0.77		
Eff5		0.90	0.77		
Compliant Behavior	0.90			0.87	0.57
Comply1		0.90	0.72		
Comply2		0.89	0.60		
Comply3		0.84	0.80		
Comply4		0.84	0.78		
Comply5		0.85	0.82		
Comply6		0.86	0.80		

Table 4: Convergent Validity for Reflective Constructs

Convergent validity of reflective constructs can be assessed through: (i) internal consistency, (ii) item reliability, (iii) composite reliability, and (iv) average variance extracted. Internal consistency of a scale refers to the degree of homogeneity among the items within the scale and is measured using Cronbach's alpha coefficient (Cronbach 1951). A level of 0.7 for the coefficient, as recommended by Nunnally (1978), would indicate adequate internal consistency. All reflective constructs in our model have their Cronbach's alphas above the recommended level (see Table 4). Item reliability indicates the amount variance in a measure due to the construct rather than to error and is determined by the item loadings of the individual items. Values of the standardized item loading should be greater than 0.5 indicating that the shared variance between each item and its construct exceeds the error variance (Chin 1998). All items had loadings above the accepted threshold. Composite reliability of each construct was evaluated based on the guideline for assessing the reliability coefficient recommended by Fornell & Larcker (1981). Composite reliability values of at least 0.7 are considered to be acceptable. All constructs in the model achieved reliability coefficient values above the recommended value. The average variance extracted (AVE) by each construct is defined as the amount of variance in the item explained by the construct relative to the amount as a result of measurement error (Fornell & Larcker 1981; Grant 1989). Values of the average extracted variance should be above 0.5 as recommended by Fornell & Larcker (1981). All reflective constructs under study have average extracted variance above 0.5 (see Table 4).

For formative constructs, the values of item weights are examined to determine the relative contributions of items constituting the construct (Chin & Gopal 1995). There is a single formative construct in our study, upper management practices. It is based on two dimensions: provision of (i) security policies and (ii) education in information security. Results shown in Table 5 indicate that employees regard the two dimensions as equally important factors in determining whether upper management is committed to information security

Upper Management Practices	Item Weight
Mgmt1	0.78*
Mgmt2	0.87*
Mgmt3	0.78*
Mgmt4	0.81*
Mgmt5	0.81**
* $p < 0.05$, ** $p<0.01$	

Table 5: Item Weight for Formative Constructs

Construct and Items	Component 1	2	3	4	5
Direct Supervisory Practices					
Sup1	0.30	0.13	**0.84**	0.15	0.13
Sup2	0.25	0.07	**0.86**	0.19	0.20
Sup3	0.04	-0.05	**0.76**	0.08	0.40
Sup4	0.21	0.00	**0.75**	0.26	0.28
Coworker Socialization					
Cowork1	0.25	0.09	0.38	0.31	**0.64**
Cowork2	0.16	-0.08	0.25	0.23	**0.77**
Cowork3	0.10	0.04	0.33	0.16	**0.74**
Perception of Climate					
Perp1	0.18	0.16	0.08	**0.87**	0.18
Perp2	0.26	0.06	0.50	**0.63**	0.25
Perp3	0.28	0.05	0.25	**0.62**	0.46
Perp4	0.17	0.15	0.23	**0.75**	0.18
Self Efficacy					
Effi1	**0.82**	0.00	0.21	0.25	0.07
Effi2	**0.86**	-0.00	0.21	0.13	0.09
Effi3	**0.87**	-0.01	0.20	0.03	0.16
Effi4	**0.82**	0.01	0.21	0.15	0.07
Eff5	**0.64**	0.27	-0.05	0.09	0.21
Compliant Behavior					
Comply1	0.51	**0.82**	0.07	0.32	0.02
Comply2	0.02	**0.71**	0.21	-0.06	-0.07
Comply3	0.09	**0.90**	0.03	0.10	0.08
Comply4	-0.01	**0.92**	0.04	0.07	-0.00
Comply5	0.10	**0.86**	0.03	0.15	0.01
Comply6	0.10	**0.85**	-0.18	0.13	0.03
Eigenvalue	4.05	3.91	3.52	2.69	2.27
Variance (%)	18.42	17.76	16.00	12.23	10.34
Cumulative Variance (%)	18.42	36.18	52.19	64.41	74.76

Table 6: Factor Analysis for Reflective Constructs

Fornell and Larcker (1981) suggested two tests for the assessment of discriminant validity of reflective constructs: (i) the examination of item loadings, and (ii) the examination of item correlations. Factor analysis was carried out to examine the item loadings (see Table 6). This was done using principle components analysis with varimax rotation. A total of 5 factors were extracted with eigen values above 1[1], which explained about 74.8% of the total cumulative variance. Items of all reflective constructs registered loading values above the threshold of 0.5 as stipulated by Hair, Anderson, Tatham and Black (1998). The factors extracted corresponded to the model constructs as expected.

Constructs	Perp	Mgmt	Sup	Cowork	Comply	Effi
Perp	**0.73**					
Mgmt	0.64	NA				
Sup	0.60	0.56	**0.71**			
Coworker	0.69	0.58	0.69	**0.63**		
Comply	0.41	0.38	0.27	0.23	**0.57**	
Effi	0.49	0.47	0.45	0.43	0.40	**0.71**

Table 7: AVE vs. Square of Correlations among Constructs

The test of item correlation involves examining the correlations between the measures of two constructs (Grant 1989). As shown in Table 7, the diagonals represent the average variance extracted while the off-diagonal values are the shared variances, i.e., the square of the correlations. For discrimination, the values of the correlations should be lower than the average variance extracted of the items measuring each construct. Since the diagonal values exceed the non-diagonal entries, the discriminant test for constructs is satisfied. Having sufficient confidence in the convergent and discriminant validity of the measurement model, the structural model was evaluated.

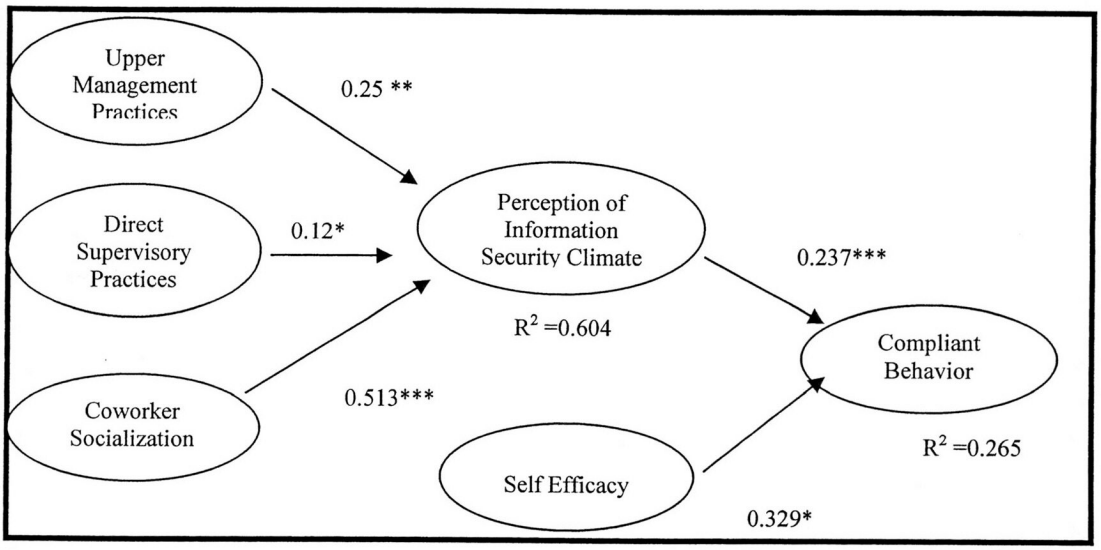
Structural Model

The structural model was tested for hypotheses, significance and explanatory power. Path coefficients indicate the strength and direction of the relationships between dependent and independent constructs. The values of path coefficients should be significant and directionally consistent with the hypotheses. Jackknife resampling method was used to assess the significance

[1] An eigenvalue above 1 is indicative that the construct is stable and that the items will load well into the factor (Johnson & Wichern 1998).

of the path estimates. This procedure builds resamples by deleting a case at a time from the original sample. The sign (positive or negative) and the statistical significance of the values are assessed for support of the hypotheses. A statistical level of 0.5 (t-value of 1.67) is considered acceptable for an exploratory study. The R^2 value is representative of the amount of variance in the dependent variable explained by the model. A larger R^2 indicates better predictive power of the model.

The results of the data analysis are shown in Figure 2. The exogenous variables comprising upper management practices, direct supervisory practices, and coworker socialization accounted for 60.4% of the variance in the perception of information security climate. Perception of information security climate and self-efficacy in turn explained 26.5% of the variance in compliant behavior. All paths were significant at the 0.05 level with three paths significant at the 0.01 level. As predicted, upper management practices, direct supervisory practices, and coworker socialization, were positively related to the employee's perception of the information security climate within the organization (H1, H2, and H3 were supported). Perceptions of information security climate and self-efficacy in turn were positively related to employee's compliant behavior with security guidelines and policies (H4 and H5 were supported).



* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Figure 2: Graphical Display of Results

DISCUSSION AND CONCLUSION

Based on our findings, perception of information security climate and self-efficacy positively impact employee's compliant behavior. This result indicates that compliant behavior is dependent on a combination of organizational and personal factors. However, the two antecedents explained 26.5% of the variance in compliant behavior. Therefore additional antecedents need to be included to increase explanatory power. For example, factors such as habit, suggested by the Theory of Interpersonal Behavior (Triandis 1980) could be incorporated into the model in the future in an attempt to better explain compliant behavior. In practice, this result suggests that compliant behavior can be promoted by increasing employees' self-efficacy and enhancing perception of information security climate.

Upper management practices, direct supervisory practices, and co-worker socialization, were found to be positively related to employees' perception of information security climate. The three antecedents explained 60.4% of the variance in employees' perception of the climate. This finding suggests that a strong information security climate can be created by engaging all levels of the organization i.e., top management, middle management (intermediate supervisors), and junior employees. However, in order to increase the explanatory power for perception of information security climate, other factors apart from socio contextual ones need to be considered in future research.

As expected, coworker socialization is significantly related to employees' perception of the information security climate. This finding indicates that employees themselves have considerable influence on their peers' perception of the information security climate. This implies that in addition to implementing policies and conducting security awareness programs, management should ensure that policy guidelines and lessons learned in these programs are actively applied and observed by employees when they are carrying out their work. By demanding work practices consistent with those prescribed in information security policies, management can help create a strong information security climate in the organization.

Several limitations of our study can be addressed in future work. First, objective measures of compliant behavior though obtrusive can be considered. For instance, 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 in the organization. Additionally, future studies could examine the behavior of employees before and after the implementation of new security policies. Second, additional factors could be included in the model to better explain compliant behavior and perception of information security climate. In particular, dispositional factors of the individual toward information security could be added to extend the model. Third, the proposed model was tested in a

single country context and results might not be representative of the generalized global population. Therefore, the study could be replicated in other countries, different organizational settings, and with larger sample groups for more generalizable findings.

In conclusion, this study makes several contributions to theory and practice. First, it applies concepts from safety literature for the first time to the context of information security. Second, the study uses the concept of information security climate, which serves as a mediator between objective characteristics of the organization and the behavior of employees. Results of the study have demonstrated support for the climate perspective and thus provide an alternative framework in studying employee behavior in organizations. Last, the results of the study provide industry practitioners insights on how employee compliance to security guidelines can be addressed and managed effectively. As information security continues to be a major concern for organizations, studies of this nature can aid in the implementation of security policies and guidelines.

REFERENCES

Anandarajan, M. (2002). Classifying web usage behavior in the workplace: An artificial neural network approach. *Managing web usage in the workplace: A social, ethical and legal perspective*, Anandarajan M. & Simmers C.A. (Eds.) Hershey, PA: Idea Publication.

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change, *Psychological Review, 84(2)*, 191-215.

Barling, J., Loughlin, C. & Kelloway, K. (2002). Development and test of a model linking safety specific transformational leadership and occupation safety. *Journal of Applied Psychology, 87(3)*, 488-496.

Beland, F. & Dedobbeleer, N. (1991). A Safety Climate Measure for Construction Sites, *Journal of Safety Research, 22(2)*, 97-103.

Bollen, K.A. (1984). Multiple Indicators: Internal Consistency or No Necessary Relationship? *Quality & Quantity, 18*, 377-385.

Campbell, J.P. & Beaty, E.E. (1971). *Organizational Climate: Its Measurement and Relationship to Work Group Performance*. Paper presented at the Annual meeting of the American Psychological Association, Washington D.C.

Campbell, J.P., Dunnette, M.D., Lawler, E.E. III. & Weick, K, Jr. (1970). *Managerial behavior, performance and effectiveness*. New York, McGraw-Hill.

Carr, Z.J., Schimdt, M.A., Ford, K.J. & DeShon, P.R (2003). Climate Perceptions Matter: A Meta-Analytic Path Analysis Relating Molar Climate, Cognitive and Affective States and Individual Level Work Outcomes, *Journal of Applied Psychology, 83(4)*, 605-619.

Chambliss, C. & Murray, E.J. (1979). Cognitive procedures for smoking reduction: Symptom attribution versus efficacy attribution, *Cognitive Therapy and Research, 3(1)*, 91-95.

Chin, W.W. (1998). Issues and Opinion on Structural Equation Modeling, *MIS Quarterly, 22(1)*, vii-xv.

Chin, W.W. & Gopal, A. (1995). Adoption intention in GSS: Relative importance of beliefs, *Database, 26(2&3)*, 42-64.

Chin, W.W. & Sambamurthy, V. (1994). The Effects of Group Attitudes toward Alternative GDSS Designs on the Decision-making Performance of Computer-Supported Groups, *Decision Sciences, 25 (2)*, 215-241.

Churchill, G.A. (1979). A paradigm for developing better measures of marketing constructs, *Journal of Marketing, 16(1)*, 64-73.

Cohen, A. (1977). Factors in successful occupational safety programs, *Journal of Safety Research, 9(4)*, 168-178.

Compeau, D. & Higgins, C.A. (1995). Computer Self Efficacy: Development of a measure and Initial Tests, *MIS Quarterly, 19(2),* 189-211.

Compeau, D., Higgins, C.A. & Huff, S. (1999). Social Cognitive Theory and Individual Reactions to Computing Technology: A Longitudinal Study, *MIS Quarterly, 23(2)*, 145-158.

Computer Security Institute. (2004). *Issues, Trends 2004: CSI/FBI Computer Abuse and Security Survey*, CSI, San Francisco, CA

http://gocsi.com/forms/fbi/csi_fbi_survey.jhtml;jsessionid=GFCCKGZ2LGROKQSNDBCCKHSCJUMEKJVN

Cook, T. & Campbell, D. (1979). *Quasi-experimentation: Design and analysis issues for field settings*. Boston: Houghton Mifflin.

Cronbach L.J. (1951). Coefficient Alpha and the Internal Structure of Tests, *Psychometrika, 16*, 297–334.

Dejoy, D.M. (1996). Theoretical models of health behavior and workplace self-protection, *Journal of Safety Research, 27(2),* 61-72.

Dejoy, D.M., Schaffer, B.S., Wilson, M.G., Vandenberg, R.J. & Butts, M.M. (2004). Creating safer workplace: Assessing the determinants and role of safety climate, *Journal of safety Research, 35(1),* 81-90.

Dhillon, G. & Backhouse, J. (2001). Current direction in IS Security research: towards socio-organizational perspective, *Information Systems Journal, 11(2),* 127-153.

Diaz, R.I. & Cabrera, D.D. (1997). Safety climate and attitude as evaluation measures of organizational safety, *Accident, Analysis and Prevention, 29(5),* 643-650.

Fornell, C. & Larcker, V.F. (1981). Evaluating structural equation models with unobservable variables and measurement error, *Journal of Marketing Research, 18(3)*, 39-50.

Galletta, D.F. & Polak, P. (2003). An Empirical Investigation of Antecedents of Internet Abuse in the Workplace, *Proceedings of the Second Annual Workshop on HCI Research in MIS*, Seattle, WA, December, 47-51.

Gefen, D., Straub, D.W. & Boudreau, M.C. (2000). Structural Equation Modeling and Regression: Guidelines for Research Practice, *Communications of the AIS, 4*, 1-77.

Grant, R.A. (1989). Building and Testing a Causal Model of an Information Technology's Impact, *Proceedings of the Tenth International Conference on Information Systems*, December 4-6, Boston, MA, 173-184.

Griffin, M.A. & Neal, A. (2000). Perceptions of Safety at Work: A Framework for Linking Safety Climate to Safety Performance, Knowledge and Motivation, *Journal of Occupational Health Psychology, 5(3),* 347-358.

Hair, J.F., Anderson, R.E., Tatham, R.L. & Black, W.C. (1998). *Multivariate Data Analysis*. Prentice-Hall, Fifth Edition.

Hayes, B.E., Perander, J., Smecko, T. & Trask, J. (1998). Measuring Perceptions of workplace safety: Development and validation of work safety scale, *Journal of Safety Research 29(3)*, 145-161.

James, R.L. & Jones, P.A. (1974). Organizational Climate: A review of theory and research, *Psychological Bulletin, 81(12),* 1096-1112.

James, R.L. & Jones, P.A. (1976). Organizational Structure: A review of structural dimensions and their conceptual relationships with individual attitudes and behavior, *Organizational Behavior & Human Decision Processes*, *16*, 74-113.

Johnson, R.A. & Wichern, D.W. (1998). *Applied Multivariate Statistical Analysis*, 4 ed. Englewood Cliffs, New Jersey, USA: Prentice-Hall.

Limayem, M., Khalifa, M. & Chin, W.W. (1999). Factors motivating software piracy: A longitudinal study, *IEEE Transactions on Engineering Management, 51(4),* 1-12.

Litwin, G.H. & Stringer, R.A. Jr (1968). *Motivation and Organizational Climate*, Boston, Harvard University.

Martins, A. & Eloff, J.H.P. (2001). Measuring Information Security, Proceedings of Workshop on Information Security – System Rating and Ranking, Virginia.
http://philby.ucsd.edu/~cse291_IDVA/papers/rating-position/Martins.pdf

Moore, G.C. & Benbasat, I. (1991). Development of an Instrument to measure the perceptions of adopting an information technology innovation, *Information Systems Research,* 2(3), 192-222.

Mullen, J. (2004). Investigating factors that influence individual safety behavior at work, *Journal of Safety Research, 35(3)*, 275-285.

Neal, A. & Griffin, M.A. (1997). *Perceptions of Safety at Work: Developing a Model to Link Organizational Safety Climate and Individual Behavior.* Paper presented to the 12th Annual Conference of the Society for Industrial and Organizational Psychology, St. Louis, MO.

Nunnally, J.C. (1978). *Psychometric Theory*, McGraw-Hill, New York.

Payne, R. & Mansfield, R. (1978). Correlates of individual perceptions of organizational climate, *Journal of Occupational Psychology, 51*, 209-218.

PriceWaterHouseCoopers (2004). *Information Security Breaches Survey 2004.*
http://www.information security.co.uk/files/DTI_Survey_Report.pdf

Reichers, A.E. & Schneider, B. (1990). Organizational climate and culture: Evolution of constructs, *Organizational climate and culture*, Schneider, B. (ed), San Francisco: Jossey-Bass.

Salancik, G.R. & Pfeffer, J. (1977). An examination of need-satisfaction models of job attitudes, *Administrative Science Quarterly, 22(3),* 427-456.

Salancik, G.R & Pfeffer, J. (1978). A Social Information Processing Approach to Job Attitudes and Task Design, *Administrative Science Quarterly, 23(2),* 224-253.

Schnake, M.E. (1983). An empirical assessment of the effects of affective response in the measurement of organizational climate, *Personnel Psychology, 36(4)*, 791-807.

Schneider, B. (1975). Organizational climates: an essay, *Personnel Psychology, 28(4)*, 447-479.

Schneider, B. (2000). *The psychological life of organizations*, Handbook of organizational culture and climate, Ashkanasy, N.M., Wilderom, C.P.M. & Peterson, M.F. (eds.), Thousand Oaks, CA: Sage.

Straub, D.W. (1990). Effective IS security: An Empirical Study, *Information Systems Research, 1(3),* 255-276.

Straub, D.W. and Welke, R.J. (1998). Coping with systems risks: Security planning models for management decision making, *MIS Quarterly, 22(4),* 441-469.

Taylor, C.W. (1972). *Climate for creativity*, N.Y., Pergamon Press.

Taylor, S. & Fiske, S. (1978). Salience, Attention and Attribution: Top of the Head Phenomena, *Advances in Experimental Social Psychology, 11*, 249-288, New York Academic Press, L Berkowitz (ed.).

Triandis, H.C. (1980). Values, Attitudes, and Interpersonal Behavior, *Nebraska Symposium on Motivation*, M.M. Page (ed.) The University of Nebraska Press, Lincoln, 159-259.

Zohar, D. (1980). Safety Climate in Industrial Organizations: Theoretical and Applied Implications, *Journal of Applied Psychology, 65(1)*, 96-102.

Zohar, D. (2000). A Group-level Model of Safety Climate: Testing the Effect of Group Climate on Micro-accidents in Manufacturing Jobs, *Journal of Applied Psychology, 85(4)*, 587-596.

Zohar, D. (2002). Modifying Supervisory Practices to Improve Subunit Safety: A Leadership-Based Intervention Model, *Journal of Applied Psychology, 87(1),* 156-163.

Zohar, D. & Luria, G. (2003). The use of supervisory practices as leverage to improve safety behavior: A cross-level intervention model, *Journal of Safety Research, 34(5),* 567-577.

Zohar, D. & Luria, G. (2004). Climate as a Social-Cognitive Construction of Supervisory Safety Practices: Scripts as Proxy of Behavior Patterns, *Journal of Applied Psychology, 89(2)*, 322-333.