Work-related groups and information security policy compliance

Teodor Sommestad, Swedish Defence Research Agency FOI

Abstract

Purpose: It is widely acknowledged that norms and culture influence decisions related to information security. This paper investigates how work-related groups influence information security policy compliance intentions and to what extent this influence is captured by the Theory of Planned Behavior, an established model over individual decision making.

Design/methodology/approach: A multilevel model is used to test the influence of work-related groups using a cluster sample of responses from 2,291 employees from 203 worksites, 119 organizations, six industries, and 38 professions.

Findings: The results suggest that work-related groups influence individuals' decision-making in the manner in which contemporary theories of information security culture posit. However, the influence is weak to modest and overshadowed by individual perceptions that are straightforward to measure.

Research limitations/implications: This study is limited to one national culture and four types of work-related groups. However, the results suggest that the Theory of Planned Behavior captures most of the influence that work-related groups have on decision making. Future research on security culture and similar phenomena should take this into account.

Practical implications: Information security perceptions in work-related groups are diverse and information security decisions appear to be based on individual perceptions and priorities rather than groupthink or peer-pressure. Security management interventions may be more effective if they target individuals rather than groups.

Originality/value: This paper tests some of the basic ideas related to information security culture and its influence on individuals' decision-making.

Keywords: information security culture, organizational policy, Theory of Planned Behavior, information security behavior, compliance, obedience

1 Introduction

The behavior of employees poses a risk to their organization's information security in a number of ways. For instance, employees may threaten the information security when they open phishing emails, surf malicious websites, connect infected USB-sticks, or move information to their private computer. A large number of studies have been devoted to identifying why employees are compliant or not compliant with organizational information security policies, and many ideas have been presented regarding how the social environment influences information security decisions. Karlsson et al. (2015) recently reviewed theories of information security culture and summarized them as ideas about "a shared pattern of values, mental models and activities that are traded among an organization's employees over time, affecting information security. (p. 247)" Thus, theories concerning information security culture suggest that individuals' perceptions and priorities are influenced by the groups to which they belong.

There is ample empirical support for ideas about group differences in decision making. For example, a meta-analysis of antecedents of a broad range of behaviors suggested that norms are more influential in cultures in which less powerful members accept and expect that power is distributed unequally (Hassan et al., 2016). Similar results have been observed in relation to national cultures and information security behaviors (Dinev et al., 2009) (Hovav and D'Arcy, 2012). However, information security is primarily governed at an organizational level, and little is known about how work-related groups influence individual employees' information security decisions.

Information security culture is a typical multilevel phenomenon, in which individuals are influenced by the different groups to which they belong (Bélanger et al., 2014). Accordingly, this research uses a multilevel model (also known as a random coefficients model or a hierarchical level model) to investigate the extent to which individuals' decision models are influenced by four types of work-related groups. The four groups are: industry, organization, worksite, and profession. A clustered sample of 2,291 employees was used to test whether these groups: a) influence the perceptions of variables known to influence individuals' decisions; b) influence how these perceived variables influence decisions; and c) influence the decisions in some other manner. These tests allow assessments of where information security cultures are formed and upheld, how much information security culture influences the decision making of individuals, and whether there is some culture-related variable missing from the models of individual decision making.

The remainder of the article is arranged as follows. The next section presents a review of models for individual decision making in information security policy compliance and theory related to information security culture. This section also presents a number of hypotheses drawn from extant theories concerning the relationships between individuals' decisions and work-related groups. This section is followed by a section describing the measurement instrument, data collection method, and statistical analysis. Thereafter, the results of the statistical analysis are presented, followed by a section discussing the implications of these results and a section concluding the paper.

2 Theory and hypotheses

This section summarizes the research on models proposed for individual decision making concerning information security policy compliance, presents theories related to information security culture, describes the limitations of the extant research, and presents twelve hypotheses related to them.

2.1 Models of individual decision making

A large number of models have been proposed for information security policy compliance decisions, and a considerable number of variables have been tested as antecedents of behavioral intentions. The observed statistical associations have been summarized in a number of reviews and meta analyses (Sommestad et al., 2015)(Sommestad et al., 2014)(Milicevic and Goeken, 2013)(Sommestad and Hallberg, 2013)(D'Arcy and Herath, 2011)(Cram et al., 2017). The more frequently studied variables are drawn from established theories from other disciplines, namely the Theory of Planned Behavior (TPB) (Ajzen, 1991), Protection Motivation Theory (PMT) (Maddux and Rogers, 1983), Deterrence Theory (DT) (Gibbs, 1975), and Rational Choice Theory (RCT) (Becker, 1968). Other theories have only been occasionally tested. For example, tests of Neutralization Theory (Siponen and Vance, 2010) (Barlow et al., 2013) and Social Control Theory (Lee et al., 2004) (Goo et al., 2013) have been performed.

Among the theories that have frequently been tested with quantitative methods, the TPB has produced the most consistent results and has explained behavioral intentions the best. The theory is relatively straightforward and posits that there are three variables explaining intentions: attitude toward the behavior, perceived norms, and perceived behavioral control. Models that adapt these variables to the context of information security compliance explain, on average, 42 percent of the intention to comply with information security policies (Sommestad and Hallberg, 2013). Although this percentage is far from all of the variance, it is more than the other models can explain. In addition, cross-correlations reported in studies including TPB-variables along with other variables suggest that the predictions of compliance intentions produced by the TPB are difficult to improve by introducing additional variables (Sommestad et al., 2017). Thus, the TPB includes components that are missing from the other theories, and tests suggests that the opposite relationship is not the case. The theory is therefore suitable as a reference model for how information security compliance decisions are made.

2.2 Information security culture and compliance decisions

There are a considerable number of theories related to culture and information systems. These theories include ideas about how culture and climate within organizations and societies influence system development, adoption, use, outcomes, and management (Leidner and Kayworth, 2006). Culture has also been explicitly related to information security behavior in a number of theoretical and empirical studies (Karlsson et al., 2015), and there has been ample evidence that the social interaction and group membership shapes decision making related to information security. Two types of relationships to information security compliance decisions have been observed: a) influence on variables that are influence policy compliance decisions; and b) influence on the relative weight of these variables.

Substantial evidence exists for the first type of relationship, i.e., links between social environment variables related to information security policy compliance decisions. A number of studies have reported strong relationships between the norms that a person perceives and the person's intention to comply with information security policy. These studies include references to norms at different levels in organizations. For example, Herath and Rao (2009b) included top management, the boss, and colleagues; Siponen et al. (2010) included top management, immediate supervisors, and peers. Some of these studies have also found links between information security policy compliance intentions and the norms expressed by friends (Jenkins and Durcikova, 2013), information security personnel (Siponen et al., 2010) (Siponen et al., 2014), IT personnel (Ifinedo, 2012) or technical specialists (Herath and Rao, 2009). Furthermore, research by Goo et al. (2013), McCoy et al. (2009), Lowry et al. (2014), Hu et al. (2012), Finch et al (2003), Chipperfield and Furnell (2010), Furnell and Thomson (2009) and Sommestad (2015)

have established or proposed various links between individuals' perception of their organization and their perceptions related to information security.

There has not been as much evidence for the second type of relationship, i.e., a social influence on the relative weight of variables determining information security policy compliance. Nevertheless, there are good reasons to believe that culture influences the relative weight of different variables explaining people's information security policy compliance intentions. First, the correlation coefficients of information security compliance intentions and the predictor variables of the TPB have differed considerably between studies. Some of this variance might be due to cultural differences among populations. Second, organizational variables (e.g., availability of resources) have been found to moderate the influence of intuitional pressure (e.g., norms within the industry) on organizations' information security management (Hsu et al., 2012). Third, studies explicitly comparing the decision models of people in the USA and the Republic of Korea have found significant differences between how relevant variables are perceived and how they influence information security compliance decisions Dinev et al. (2009) Hovav and D'Arcy (2012). Previous research at the organizational level has not included research explicitly comparing groups this way. However, there has been research suggesting that organizational culture is linked to priorities of information security aspects (Chang and Lin, 2007) and research indicating different security priorities vary among professions (Ramachandran et al., 2013). In addition, ideas about differences in philosophies tied to organizations' security policies have been presented (Siponen and Iivari, 2006).

2.3 Limitations of extant research

Information security culture is often related to organizational culture (Karlsson et al., 2015), and Yammarino and Dansereau (2011) noted that theories of organizational culture are multilevel in nature. They identified four levels/entities that can be addressed in relation to culture, namely: 1) individual differences in perceptions of culture; 2) culture in workgroups or teams; 3) culture in larger groups, such as whole organizations; and 4) culture in societies or countries. The studies described above linked information security values to all of these levels, therefore it is reasonable to assume that there is a cultural influence on individuals' decision making. However, there are few direct tests of the notion that groups within organizations share some culture that shapes their decision making, and the tests previously performed at an organizational level are associated with measurement issues due to the complexity of the concept of culture.

Schein's model (1985) is one of the more commonly cited frameworks in the research on organizational culture, information systems culture, and information security culture. According to this model, organizational cultures can be analyzed on three distinct levels: artifacts and behaviors; espoused values; and basic underlying assumptions. Artifacts, behaviors, and espoused values are relatively straightforward to observe and recognize; the underlying assumptions leading to artifacts are less so because they are related to unconscious beliefs, feelings and thoughts. Thus, measuring the third level with a questionnaire is problematic. In fact, in the safety domain, the type of expressible shared values and perceptions that can be captured by questionnaires are typically referred to as climate, while culture is reserved for something more complex and deeply hidden (Mearns and Flin, 1999) (Guldenmund, 2000).

Hofstede (2011, p. 3) succinctly described culture as "the collective programming of the mind that distinguishes the members of one group or category of people from another." With this definition and the measurement issues in mind, it is not surprising that the clearest links between culture and decision models for information security have been found in studies explicitly comparing the decision models of different groups. Both Dinev et al. (2009) and Hovav and D'Arcy (2012) found differences in how groups perceived their environments and how they prioritized variables to form their information security compliance intentions, but did so on by comparing two societies. Sommestad (2015)

performed similar analyses at the organizational level and found clear relationships between work-related groups and security perceptions, but failed to decompose the extent to which compliance decisions were mediated by security perceptions. This paper continues along this track and uses a unique dataset to assess the influence that groups related to organizations have on individuals' decisions.

2.4 Hypotheses about work-related groups and compliance decisions

There is, as noted above, plenty of research that posits that work-related groups influence individuals' decision making. Three influences from work-related groups on the decision model of the TPB are conceivable: a) as a background factor determining the predictor variables; b) as a moderator of the predictor variables; and c) as a factor that has some other, direct relationship with compliance intention. These three influences are illustrated in Figure 1.

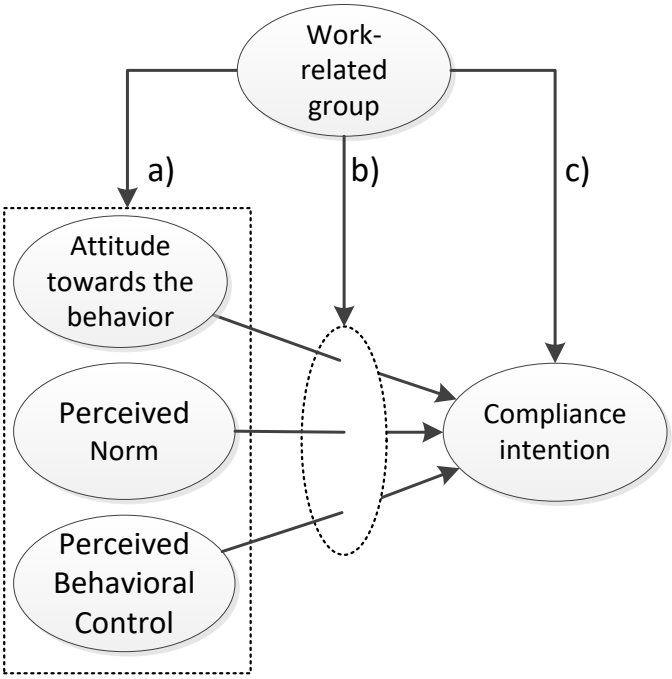

Figure 1. Potential relationships between work-related groups and the TPB.

Fishbein and Ajzen (2010), the originators of the TPB, claimed that background factors, such as social context, knowledge, and personality, have clear influences on predictor variables. As noted above, there has been ample research in the information security field supporting this notion. Thus, it should be expected that the relationship labeled a) is present. Fishbein and Ajzen (2010) also recognized that different populations assign different weights to predictor variables. Thus, they acknowledged the moderating relationship illustrated by b) in Figure 1. Research on information security policy compliance comparing respondents in different nations has supported this assumption, however, no moderating role has previously been measured at the organizational level or at the level of other work-related groups. Regarding the relationship labelled c) in Figure 1, the TPB has a clear stance. The sufficiency assumption of the TPB states that the theory is complete with respect to predictor variables and that no new variable will result in sizable improvements in explained variance (Fishbein and Ajzen, 2010). As discussed above, extant research has not been able to reject this sufficiency assumption in the context of information security policy compliance. However, relatively few studies have addressed how background factors are related to the model of the TPB in general (Fishbein and Ajzen, 2010), and no studies have tested whether group membership is a missing variable in decisions concerning information security. If relationship c) is present

and associated with a substantial effect size, this is evidence for the notion that variables related to culture are missing from the TPB.

A number of different types of groups can be studied to test the presence of the aforementioned relationships. The present research investigates the decision models of employees in different worksites, organizations, industries, and professions. These types of groups are used because they are relatively easy to link to individuals and because there are good reasons to believe that they are associated with certain underlying assumptions about the world and certain beliefs. For example:

- People who share the same worksite might socialize casually, e.g., when they meet at the water cooler to share rumors, stories, and gossip;
- People within the same organization are likely to share the same incentive structure, e.g., in terms of security policies or the priorities that their management express;
- People within the same industry share characteristics with each other; e.g., people in the government tend to stay longer with their employers than those in the private sector (U.S. Bureau of Labor Statistics, 2014); and
- People with the same profession can share certain codes of ethics, symbols, role models, and professional goals, e.g., the Hippocratic Oath sworn by people who practice medicine and the ethical codes of accountants.

There are, of course, many other reasons to believe that these groups are associated with decision models. However, the present research will not attempt to untangle the hidden assumptions and beliefs related to information security culture to investigate the underlying reasons for why different groups are influence decisions. It will instead focus on assessing the overall influence that these four groups have on people's decision making, as described in Figure 1. The three types of influence and four types of work-related groups result in twelve hypotheses, which are detailed in Table 1.

Table 1. Hypotheses on the influence of work-related groups on decisions.

	Work-related group			
Manifestation	Worksite	Organization	Industry	Profession
The group influences the values of the predictor variables	H1.A	H2.A	H3.A	H4.A
The group influences the weights of the predictor variables	H1.B	H2.B	H3.B	H4.B
The group has another relationship with intentions	H1.C	H2.C	H3.C	H4.C

It should be noted that the first three of these groups has a clear nested relationship: an organization exists within an industry, and a worksite exist within an organization. Thus, a particular culture within a worksite might exist because this particular culture exists within the organization or the industry to which the worksite belongs. A profession can be expected to be associated with the other three groups, e.g., because nurses often work in worksites of organizations in the healthcare industry. However, there is no apparent nested structure because nurses can work in other industries too.

3 Measurement instrument and data collection

A questionnaire was used to collect the data with the assistance of Statistics Sweden, a Swedish government agency producing statistics. The official records held by Statistics Sweden were used to define a three-stage clustered sample suitable for testing the hypotheses. The sections below describe the instrument used for the TPB variables, the

data collection procedures, the tests of measurement reliability, validity, and non-response bias, and the statistical analysis.

3.1 Measurement instrument

A considerable amount of knowledge concerning how best to operationalize the TPB has been accumulated through the many applications, tests, and reviews of the theory. The measurement instrument used to measure the variables of the TPB is based on the examples and a template for direct scales provided by the originators of the theory (Fishbein and Ajzen, 2010), indicating that both instrumental and experiential *attitudes* were measured, items of *perceived norms* measured both injunctive norms and descriptive norms, and *perceived behavioral control* covered both autonomy and capability dimensions. *Intentions* were measured as outright intentions or predictions of future behavior. The items used to measure the variables were associated with the same action (compliance with), target (the organization's security policy), context (at work), and time (unspecific). Thus, they followed the principle of compatibility. Each item was associated with five points ranging from completely disagree to completely agree.

The questionnaire was quality controlled by analysts at Statistics Sweden, subjected to approval from an ethical board, and tested in a pilot survey. This pilot survey was distributed to 500 randomly selected individuals in the target population, i.e., white-collar professionals. Of these people, 156 (31 percent) responded to the questions. Tests of reliability and validity of the measurement led to two types of modifications to the survey. First, when sufficient reliability could be maintained, items were omitted to reduce the length of the final questionnaire. Second, some items (e.g., related to attitude) were changed to a more pointed wording to limit ceiling effects in the measurement. In the final survey, two to four items were used for each TPB variable.

3.2 Data collection procedure

Statistics Sweden maintains various records related to individuals, government, and business organizations. The present study primarily used the "Longitudinal Integration Database for Health Insurance and Labour Market Studies" (LISA), which among other things contains information about all of the individuals in Sweden and the organizations that employ them (Statistics Sweden, 2016). More specifically, this study used records of individuals, links between individuals and professions, links between individuals and worksites, links between worksites and organizations, and links between organizations and industries.

Statistics Sweden provided structural information that could be used to identify a suitable sample frame. This structural information showed, among other things, industries with suitable numbers of organizations of the correct size and with individuals with suitable professions. A number of power analyses were also performed to identify requirements for the number of groups and the number of respondents from each group. With this input, a number of alternative sampling procedures were documented and reviewed together with experts at Statistics Sweden under the cost constraint that a maximum of 9,000 respondents could be involved. The result of this review was a sampling procedure designed as follows.

- **Industries**: Six industries were selected based on structural information and the relevance of information security to the industry. These six were chemical manufacturing, IT consulting, banking, universities and colleges, public healthcare, and social services, which were chosen because they differed in several manners, e.g., in market orientation.
- **Profession:** The third level of abstraction in the coding system SSYK (Statistics Sweden, 2011) was used, and 86 of 148 professions were included in the sample, namely those labeled 011-422, including employees of the "armed forces", "various legislators, senior officials and managers," "various professionals,"

"technicians and associate professionals" and "clerks." Excluded professions were judged to be unlikely to work with sensitive information and information systems. They included, among others, various blue-collar professions, agricultural workers, and elementary occupations.

- **Organizations**: A random sample of 20 organizations was used within each industry. To be included in the sample frame, the organization had to have 20-500 employees of the right professions at one or several worksites. The lower limit was used to ensure that a sufficient number of employees were available to measure group effects; the upper limit was set to exclude large organizations in which the information security culture might be dominated by subcultures.
- **Worksites:** Up to three randomly selected worksites were used within each organization. All of the included worksites were required to have at least 20-500 employees of the right professions included in the sample frame. Up to 70 randomly selected employees of the included professions were chosen for each worksite, i.e., up to 210 employees at each organization.

Because some organizations are involved in several industries, the industry codes of Statistics Sweden did not suffice for the accurate identification of organizations within all six industries. Supplementary records were used to ensure a high-quality sample of organizations. Social services, which in Sweden are a parts of local governments, were identified using a combination of employer, worksites, and professions of the employees; banks were identified using the records maintained by the financial regulatory authorities; chemical manufacturing organizations were identified from an industry survey conducted by Sweden's innovation agency; and IT consulting organizations, as well as universities and colleges, were identified using the industry codes together with the organizations' relationships with the government.

These constraints yielded a total sample frame of 801 organizations, 2,120 worksites, and 130,824 employees. The structure differed among the six industries. For instance, 389 IT consulting organizations met the criteria, while only 20 healthcare organizations did; 87 worksites in chemical manufacturing were included in the sample frame; and 630 were included for social services. The proportions of professions also differed among industries, organizations, and worksites. With a response rate greater than 25 percent, the random part of the sample was predicted to be sufficient to determine any sizable shared variance at the group level.

The survey was distributed and administered by Statistics Sweden. A letter to the included organizations' information security managers was distributed in early January 2016 to inform them about the upcoming survey. The questionnaire was sent to 8,968 respondents' home addresses by mail in mid-January 2016. Recipients had the option of responding by mail or using a Web site link printed on the questionnaire. Two reminders followed, which increased the return rate from 23.1 percent to 33.5 percent. After the removal of questionnaires with incomplete responses, responses from persons who were unaware of their organizations' information security policies, and responses from persons who had changed jobs since the records of LISA were updated, 2,291 (25.5 percent) responses remained.

3.3 Measurement reliability, validity, and non-response bias

The internal reliability in terms of Cronbach's Alpha was greater than 0.85 for all of the variables in the pilot survey and greater than 0.80 for all of the variables in the final survey. Thus, the items for each variable were clearly related to each other, and convergent validity was present (Peterson, 2014). All of the average inter-item correlations for the variables supposed to be different were 0.85 or less when they were attenuated for measurement error, suggesting that discriminant validity was present (Campbell and Fiske, 1959). The TPB variables had mean values of 3.83-3.98 with standard deviations of 0.74-0.88 (on a scale of 1-5). QQ-plots were used to confirm that

the responses to the survey items were approximately normally distributed. Furthermore, all of the variable relationships predicted by the TPB were found to be statistically significant. Thus, the measurement instrument successfully operationalized the TPB.

Because only one quarter of the sample responded, the threat of non-response bias was present. Already in the pilot survey, it was recognized that older people tended to return more surveys than younger people, which was a pattern Statistics Sweden recognizes for surveys in general. Overrepresentation of older respondents was also present in the final survey. Among respondents 50 years old and older, 44.4 percent returned the survey; among respondents aged 40-49 years old, 31.8 percent returned the survey; among 16- to 39-year-olds, the response rate was 25.8 percent. Respondents' ages had a weak, positive correlation (between 0.06 and 0.19) with responses related to the TPB variables. However, the age bias was even across industries, and age had no significant effect on intentions when entered after the predictor variables of the TPB. Thus, the influence of age was mediated by the TPB and was unproblematic for the analysis performed in this paper. The response rates of men (33.4 percent) and women (33.6 percent) were similar; people living in urban areas (33.5 percent) and rural areas (33.5 percent) had the same response rate; and those working in the public sector (34.3 percent) had similar response rates to those in the private sector (32.8 percent). Furthermore, very weak correlations (all -0.03) were present between the return date of the survey and the measurements of the TPB variables. Thus, the willingness or ambition to return the questionnaire did not have any problematic relationship with the responses. Finally, there were no major differences in response rates between industries (all between 31 percent and 35 percent).

The analysis was based on results from 6 industries, 119 organizations, 203 worksites, 37 professions, and 2,291 individuals. The mean responses obtained for the groups and the standard deviations of the numbers of responses obtained from the groups were 382±23 for industry, 19±13 for organization, 11±6 for worksite, and 62±75 for profession.

3.4 Statistical analysis

The hypotheses addressed in this paper can be understood in terms of the regression model predicting intentions according to the TPB. In the TPB, the responses to the TPB variables of person number *i* are calculated as the mean values of the associated items and are entered into a regression model as:

$$INT_i = B_{intercept} + B_{ATB}*ATB_i + B_{PNO}*PNO_i + B_{PBC}*PBC_i + error_i$$

Thus, the basic model based on the TPB suggests that the *i*:th person's intentions (INT_i) can be predicted based on a constant (the intercept $B_{intercept}$), the responses of the three predictor variables (ATB_i, PNO_i and PBC_i), and their weights (B_{ATB}, B_{PNO}, and B_{PBC}). If the mean of the prediction errors ($error_i$) is small, the model has a good fit in the population. In typical application of the TPB, both the intercept and the variables' weights are assumed to be the same for all of the respondents in the population. All twelve hypotheses in Table 1 can be directly related to this equation.

- Hypotheses H1.A, H2.A, H3.A and H4.A concern whether the groups influence the responses of individuals concerning the variables associated with the theory, i.e., INT_i, ATB_i, PNO_i and PBC_i. For instance, H2.A proposes that the means of responses from respondents of different organizations are different from each other.
- Hypotheses H1.B, H2.B, H3.B and H4.B concern the relationships between groups and the weights of the predictor variables, i.e., B_{ATB}, B_{PNO} and B_{PBC}. For instance, H2.B posits that the weights vary between organizations, or stated differently, it posits that the organization moderates the relationships between intentions and their predictor variables.
- Hypotheses H1.C, H2.C, H3.C and H4.C concern the term $B_{intercept}$ and its relationship with the groups in a flexible model, in which all of the variable

weights (B_{ATB}, B_{PNO}, and B_{PBC}) are allowed to vary with the work-related groups. For instance, if the term $B_{intercept}$ varies with organizations although the responses (ATB_i, PNO_i, and PBC_i) are individual, and the variable weights (B_{ATB}, B_{PNO}, and B_{PBC}) are group-specific, there must be some relationship between INT_i and the organization that is not captured by the variables of the TPB.

The hypotheses were tested using version 7 of the Hierarchical Linear and Nonlinear Modeling (HLM). HLM supports analysis of multilevel models (also known as random coefficient models or hierarchical linear models), which address situations in which the observations of individuals are not independent from each other but are related to the groups to which they belong (Garson, 2013). To test the hypotheses labeled A, a null model was used, in other words, a simple model with no other predictors than the intercept (i.e., $B_{intercept}$) in it, equivalent to a random effect ANOVA. To test the hypotheses labeled B, the significance of the influence of random slopes was tested. In other words, it assessed whether the weights of the predictors of the TPB (i.e., B_{ATB}, B_{PNO} and B_{PBC}) varied significantly between groups. To test the hypotheses labeled C, it was assessed whether there was a significant variation in the intercept (i.e., $B_{intercept}$) between the groups, although random slopes were used. A four-level hierarchical model was used to assess the individual influence of industry, organization, and worksite on individuals; a crossed model with both worksite (tied to organization and industry) and profession as independent groups was used to assess their individual effects. A p-value less 0.05 was considered statistically significant throughout the analysis.

A relevant measure of the magnitude of the aforementioned effects is how much better the predictions of individuals' intentions are in models in which coefficients are dependent on the work-related groups the individuals belong to. As a result, the variance remaining on level one of the models (i.e., mean error in within-group predictions) is used as an effect size measure. This variance is compared to the overall variance in the response variable and the variance remaining after a regular Ordinary Least Squares (OLS) regression analysis that does not consider group differences. This type of effect size is not typical in the use of random coefficients models, which are often concerned with the relative weight of specific variables on different levels. However, it fits well with the goals of the present research, which was concerned with how predictions improve when group memberships are controlled for.

4 Results

Before addressing the hypotheses more explicitly, it is worth noting that all of the predictor variables were significant in a model of the whole population. The ordinary least squares (OLS) regression coefficients (B) and unstandardized coefficients (β) were: B_{const}=0.640; B_{ATB}=0.280; B_{PNO}=0.489; B_{PBC}=0.055; β_{ATB} =0.236; β_{PNO} =0.444; β_{PBC} =0.051. The prediction with the TPB explained 41.5 percent of the overall variance in intentions.

4.1 Influence of work related groups on the value of predictor variables

Hypotheses H1.A, H2.A, H3.A and H4.A posit that measurements of the variables of the TPB are homogeneous within industry, organization, worksite, and profession. These hypotheses were tested using models with the intercept only and measurements of the variance explained by a model allowing the groups to have different mean values for the variables.

As Table 2 shows, both worksite and profession had significant relationships with TPB variables in the crossed model. However, the hierarchical (nested) model showed that much of the variance explained by worksites could be attributed to organizations and industries. In fact, worksites had no statistically significant relationship to the variables

when industry and organization were controlled for. Thus, support was not present for H1.A but was for H2.A, H3.A, and H4.A. It should be noted that, despite these significant relationships, there are substantial differences in how people perceive the world and what they intend to do. The crossed model shows that only 6.1 percent of the variance in the responses could be tied to membership in the work-related groups.

Table 2. Portion of variance in responses to questions explained at different levels. Bold values represent statistically significant relationships.

Model	Work-related group	Portion of variance explained			
		ATB	PNO	PBC	INT
Crossed null	Worksite	**0.028**	0.007	**0.030**	**0.019**
	Profession	**0.033**	**0.037**	**0.022**	**0.042**
Nested null	Industry	**0.027**	**0.040**	**0.044**	**0.025**
	Organization	**0.023**	**0.009**	**0.014**	0.010
	Worksite	0.003	0.001	0.001	0.016

ATB: Attitude toward the behavior; PNO: Perceived norms; PBC: Perceived behavioral control; INT: Intention

4.2 Influence of work-related groups on variable weights

Hypotheses H1.B, H2.B, H3.B and H4.B concern whether the weights of the predictor variables in the TPB are dependent on work-related groups, which can be tested through models with random slopes, i.e., models in which the beta-values of the regression model are allowed to vary with the groups.

As the random slopes models in Table 3 show (cf. models #5 and #9), the only type of group with a statistically significant influence on the weights of the TPB predictors was the worksite. Thus, industry, organization, and profession had no clear relationship with the relative weight of the predictor variables, but worksites did, indicating that H1.B was supported, but none of H2.B, H3.B, and H4.B were. Although not reported in the table, it should be noted that these tendencies held even if the relationships were tested one type of work-related group at a time. There were no significant differences in variable weights in a simpler model that only included industry; no significant differences in a model that only included profession; and significant differences only for PBC occurred in a model that only included organizations.

How much group-related differences in variable weights influence intentions can be estimated by comparing the variance left unexplained by the models. The crossed model (#5), including both worksites and professions, explained 45.8 percent of the within-group variance in intentions when weights were group-specific, which is 4.3 percentage points more than an OLS-model (#2) with fixed weights for the entire population. The nested random slopes model (#9) explained 44.9 percent of the variance in intentions, 3.4 percentage points more than an OLS model with the same weights for the whole population. The magnitude of differences between variables in worksites could also be seen through the standard deviations of the coefficients in the models. In the crossed model, the fixed part and standard deviations of coefficients within worksites were $B_{ATB}=0.268\pm0.131$, $B_{PNO}=0.484\pm0.147$, and $B_{PBC}=0.061\pm0.139$, respectively.

Table 3. Variance explained in different models and standard deviations for random coefficients in different models. Bold values represent statistically significant relationships.

Model	Level 1 variance	Portion of variance explained	Work-related group	Random coefficients std. deviation			
				B_{ATB}	B_{PNO}	B_{PBC}	$B_{Const.}$
1: No model	0.775	-	All	-	-	-	-
2: Fixed model (OLS)	0.453	0.415	All	-	-	-	-
3: Crossed null model	0.726	0.063	Worksite	-	-	-	**0.121**
			Profession	-	-	-	**0.181**
4: Crossed random intercept TPB	0.440	0.432	Worksite	-	-	-	0.068
			Profession	-	-	-	**0.092**
5: Crossed random slope TPB	0.420	0.458	Worksite	**0.131**	**0.147**	**0.139**	-
			Profession	0.096	0.049	0.074	-
6: Crossed random intercept and slope TPB	0.414	0.466	Worksite	**0.127**	**0.175**	**0.123**	**0.301**
			Profession	**0.127**	0.035	0.048	**0.389**
7: Nested null model	0.737	0.050	Industry	-	-	-	**0.139**
			Organization	-	-	-	0.086
			Worksite	-	-	-	0.112
8: Nested random intercept TPB	0.445	0.426	Industry	-	-	-	0.017
			Organization	-	-	-	0.037
			Worksite	-	-	-	0.071
9: Nested random slope TPB	0.428	0.449	Industry	0.027	0.014	0.018	-
			Organization	0.059	0.050	0.049	-
			Worksite	**0.118**	0.127	**0.137**	-
10: Nested random intercept and slope TPB	0.423	0.455	Industry	0.040	0.007	0.002	0.025
			Organization	0.044	0.104	0.043	0.249
			Worksite	**0.117**	**0.110**	**0.143**	**0.267**

ATB: Attitude toward the behavior; PNO: Perceived norms; PBC: Perceived behavioral control; INT: Intention

4.3 Other relationships between work-related groups and intentions

The hypotheses labeled H1.C, H2.C, H3.C, and H4.C concern the sufficiency assumption of the TPB, which can be addressed by allowing the intercept to vary with groups in a model that has variable-weights that are group-specific. A statistically significant difference in the intercepts of different groups would suggest that the work-related groups have relationships with intentions that are not mediated by the variables of the TPB nor that express themselves by moderating the variables' influence.

The models with both a random intercept and a random slope (#6 and #10) in Table 3 show that there was something associated with workgroups and professions not covered by the TPB. Thus, H1.C and H4.C were supported, but neither H2.C nor H3.C was. That being said, the effect was small. The reduction in variance on level one was only 0.8 percentage points when a random intercept was added to the random slope model, i.e., when models #5 and #6 were compared.

5 Discussion

Information security culture is a thorny subject that is interpreted in many ways and is related to a number of theories. This section aims to untangle some of the questions related to information security culture based on the empirical results at hand. First, the way in which information security culture manifests itself in the present study are addressed. Second, the relative weight of different work-related groups is discussed. Third, the significance of information security culture for information security compliance is addressed. The limitations of the study and suggestions for future research are provided within these sections.

5.1 The manifestations of information security compliance culture

In this paper, shared characteristics in work-related groups are used as measures of information security culture. This operationalization of culture is in agreement with the definition of culture as "the collective programming of the mind that distinguishes the members of one group or category of people from another" (Hofstede, 2011). It is also straightforward and concrete, and there has been a call for a more concrete operationalization of culture (Schein, 2012). Multilevel analysis made it possible to identify that:

a) Groups influence views concerning variables that determine information security policy compliance intentions;
b) Groups place different weights on things related to security policy compliance when they form their intentions; and
c) Groups influence exceeds the TPB and seems to be related to a factor that is not accounted for not in the model of the TPB.

As noted in the introduction, information security culture concerns shared values and mental models, as well as activities that are shared and traded within a group of individuals (Karlsson et al., 2015). The three types of influence listed above describe the effects of shared values and mental models among group members, but not how perceptions and priorities are formed or traded between individuals. Thus, the details and steps in the process that form information security culture or where perceptions and priorities are formed through social interaction are not addressed in this paper.

Details on how information security culture is formed are inherently difficult to identify in a cross-sectional design like this one. However, further research using multilevel designs could attempt to single out the effects considered cultural (e.g., social interactions and underlying beliefs) from other background factors sometimes considered distinct from culture. For instance, the theory of attraction-selection-attrition suggests that there are links between where people work, what they work with, and their personalities (Schneider et al., 1995). Thus, the relationship between work-related groups and decision models might exist because of homogeneity in personality in these groups, and ideas already exist about the processes that cause homogeneity among employees' personalities.

5.2 The locale of information security compliance culture

There are many types of work-related groups in which information security culture can exist. This study is limited to four: industries, organizations, worksites, and professions.

As the results showed, all of these locations except worksites have cultures in the sense that they are somewhat homogeneous regarding attitudes, perceptions, and behavioral intentions. It is natural, and expected, that the influence of groups differs, and the insignificance of worksites might simply be the result of most of the conditions concerning information security being worksite-independent. For example, industries tend to have different security standards, organizations have different security policies,

and different professions work with different IT systems within organizations. However, when these other work-related groups are controlled for, it difficult to identify something directly related to information security policies, which tend to vary with worksites.

Regarding the weights of the predictor variables, the result was the opposite. The groups made up by worksites play a significant role, and the other types of work-related groups do not. Thus, if culture is seen as something more than a shared understanding of context, information security culture is primarily formed and upheld among employees at the same worksite. The relative insignificance of other types of work-related groups in the weighting of TPB variables is somewhat surprising, considering that information security governance is typically centralized in organizations (e.g., with an organizational policy), industries contain people of different mindsets (e.g., university employees vs. bank employees), and the professions work on different things with different IT systems (e.g., accountants vs. customer support).

The groups used in the present study were partly a result of convenience – Statistics Sweden does not keep track of all of the social interactions that people have and all identities they are related to – and future research could find groups (e.g., project teams) with more homogenous assumptions and beliefs concerning information security. It should also be acknowledged that the significance of work-related groups might be different in other sample frames. Sweden, the sample frame in this study, is by some measures extreme. On the Inglehart-Welzel Cultural Map, Sweden is the country with the second most secular-rational values and the country with the strongest self-expression values surveyed by the World Values Institute (Inglehart, 2015). It is also the most feminine country included in Hofstede's measurements, suggesting an extreme tendency among managers to seek consensus and that conflicts are often resolved by compromise (Hofstede, 1998). Thus, replication of this study in other societies might find that other work-related groups matter.

5.3 The significance of culture for information security policy compliance

As noted above, one method for assessing the significance of information security culture is to measure homogeneity in beliefs, opinions and values that can be expressed in a survey like this one. By this definition, culture within the groups explains some 3-6 percent of the variance in responses. To explain intentions, this finding is much less than that with a model based on the TPB that does not consider membership in work-related groups. In fact, the norms that people perceive and are able to articulate in the questionnaire are much better predictors of intentions than the classification of the work-related groups to which they belong. In this data, a model with the perceived norms as the only variable explains 37.4 percent of the variance in intentions while a model based on group membership explains 6.1 percent. Thus, the part of social influence from colleagues that is easily measured in surveys has much greater influence on decisions than membership in work-related groups does.

If culture is seen as shared opinions concerning the weights of variables, a comparison of a fixed effect model and a random slopes model is of interest. The fixed coefficients TPB model (#2 in Table 3) explained 4.3 percentage points less variance than one with random coefficients based on worksite and profession (#5 in Table 3). This difference in explained variance could be compared to the difference between a static model with perceived norms included or not. When perceived norms were added to a model with attitudes toward compliance and perceived behavioral control, the explained variance increased from 29.2 percent to 41.5 percent. Thus, while the improvement from group-specific variable weights was sizeable, it was less than the direct influence of perceived norms.

Overall, the studied work-related groups have modest influences on individuals' decision making. It is noteworthy that the perceived norms, which are largely heterogeneous

within the groups, play a much larger role than the work-related groups to which the respondents are part.

6 Conclusions

Culture related to information security policy compliance does exist in work-related groups. There are homogenous attitudes, perceived norms, perceived behavioral control, and intentions related to information security policies in different industries, organizations, and professions. No homogeneity was found within worksites when organization was controlled for. However, there were significant variations between worksites regarding how the other variables were related to intentions. Overall, the results suggest that work-related groups have some influence on employees' information security behavior. However, the effect sizes were modest to small compared to established models using easily measurable perceptions on the individual level. Thus, individuals' perceptions and their own ideas play larger roles in security decisions than shared environmental conditions and group-think.

7 References

Ajzen, I., 1991. The theory of planned behavior. Organ. Behav. Hum. Decis. Process. 50, 179–211.

Barlow, J.B., Warkentin, M., Ormond, D., Dennis, A.R., 2013. Don't Make Excuses! Discouraging Neutralization to Reduce IT Policy Violation. Comput. Secur.

Becker, G.S., 1968. Crime and Punishment: An Economic Approach, Journal of Political Economy.

Bélanger, F., Cefaratti, M., Carte, T., Markham, S.E., 2014. Multilevel research in information systems: Concepts, strategies, problems, and pitfalls. J. Assoc. Inf. Syst. 15, 614–650.

Campbell, D.T., Fiske, D.W., 1959. Convergent and discriminant validation by the multitrait-multimethod matrix. Psychol. Bull. 56, 81–105.

Chang, S.E., Lin, C.-S., 2007. Exploring organizational culture for information security management, Industrial Management & Data Systems.

Chipperfield, C., Furnell, S., 2010. From security policy to practice: Sending the right messages. Comput. Fraud Secur. 2010, 13–19.

Cram, W.A., Proudfoot, J.G., Arcy, J.D., 2017. Seeing the forest and the trees : A meta-analysis of information security policy compliance literature 4051–4060.

D'Arcy, J., Herath, T., 2011. A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. Eur. J. Inf. Syst. 20, 643–658.

Dinev, T., Goo, J., Hu, Q., Nam, K., 2009. User behaviour towards protective information technologies: the role of national cultural differences. Inf. Syst. J. 19, 391–412.

Finch, J., Furnell, S., Dowland, P., 2003. Assessing IT security culture: system administrator and end-user perspectives. In: Proceedings of ISOneWorld 2003 Conference and Convention. Las Vegas.

Fishbein, M., Ajzen, I., 2010. Predicting and Changing Behavior: The Reasoned Action Approach. Psychology Press, New York, NY, USA.

Furnell, S., Thomson, K.-L., 2009. From culture to disobedience: Recognising the varying user acceptance of IT security. Comput. Fraud Secur. 2009, 5–10.

Garson, G.D., 2013. Fundamentals of Hierarchical Linear and Multilevel Modeling. Hierarchical Linear Model. Guid. Appl. 3–26.

Gibbs, J.P., 1975. Crime, Punishment, and Deterrence. York, New York.

Goo, J.., Yim, M.-S.., Kim, D.J.., 2013. A path way to successful management of individual intention to security compliance: A role of organizational security climate. In: Proceedings of the Annual Hawaii International Conference on System Sciences. pp. 2959–2968.

Guldenmund, F.W., 2000. The nature of safety culture : a review of theory and research 34.

Gullberg Brännström, S., 2011. Yrkesregistret med yrkesstatistik En beskrivning av innehåll och kvalitet (AM76BR1105). Örebro.

Hassan, L.M., Shiu, E., Parry, S., 2016. Addressing the cross-country applicability of the theory of planned behaviour (TPB): A structured review of multi-country TPB studies. J. Consum. Behav. 15, 72–86.

Herath, T., Rao, H.R., 2009. Protection motivation and deterrence: A framework for security policy compliance in organisations. Eur. J. Inf. Syst. 18, 106–125.

Hofstede, G., 2011. Dimensionalizing cultures: The Hofstede model in context. Online readings Psychol. Cult. 2, 1–26.

Hofstede, G.E., 1998. Masculinity and femininity: The taboo dimension of national cultures, Cross-cultural psychology series, Vol. 3.

Hovav, A., D'Arcy, J., 2012. Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea. Inf. Manag. 49, 99–110.

Hsu, C., Lee, J.N., Straub, D.W., 2012. Institutional influences on information systems security innovations. Inf. Syst. Res. 23, 918–939.

Hu, Q., Dinev, T., Hart, P., Cooke, D., 2012. Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture*. Decis. Sci. 43, 615–660.

Ifinedo, P., 2012. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Comput. Secur. 31, 83–95.

Inglehart, R., 2015. Cultural evolution [WWW Document]. World Values Surv. URL http://www.iffs.se/en/world-values-survey (accessed 6.7.16).

Jenkins, J.L., Durcikova, A., 2013. What, I Shouldn't Have Done That?: The Influence of Training and Just-in-Time Reminders on Secure Behavior. In: International Conference on Information Systems. Milan, Italy, pp. 1–18.

Karlsson, F., Åström, J., Karlsson, M., 2015. Information security culture: State-of-the-art review between 2000 and 2013. Inf. Comput. Secur. 23, 246–285.

Lee, S.M., Lee, S.-G., Yoo, S., 2004. An integrative model of computer abuse based on social control and general deterrence theories. Inf. Manag. 41, 707–718.

Leidner, D.E., Kayworth, T., 2006. Review : A review of Culture in Information Systems Research : Toward a Theory of Information Technology Culture Conflict. MISQ Q. 30, 357–399.

Lowry, P.B., Posey, C., Roberts, T.L., Bennett, R.J., 2014. Is Your Banker Leaking Your Personal Information? The Roles of Ethics and Individual-Level Cultural Characteristics in Predicting Organizational Computer Abuse. J. Bus. Ethics 121,

385–401.

Maddux, J.E., Rogers, R.W., 1983. Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. J. Exp. Soc. Psychol. 19, 469–479.

McCoy, B., Stephens, G., Stevens, K., 2009. An Investigation of the Impact of Corporate Culture on Employee Information Systems Security Behaviour. In: 20th Australasian Conference on Information Systems. Melbourne, Australia.

Mearns, K.J., Flin, R., 1999. Assessing the State of Organizational Safety Culture or Climate ? Curr. Psychol. 18, 5–17.

Milicevic, D., Goeken, M., 2013. Systematic Review and Meta-Analysis of IS Security Policy Compliance Research. First Steps towards Evidence-Based Structuring of the IS Security Domain. In: International Conference on Wirtschaftsinformatik. Leipzig, Germany, pp. 1067–1081.

Peterson, R.A., 2014. Meta-analysis of Alpha Cronbach's Coefficient. J. Consum. Res. 21, 381–391.

Ramachandran, S., Rao, C., Goles, T., Dhillon, G., 2013. Variations in information security cultures across professions: A qualitative study. Commun. Assoc. Inf. Syst. 33, 163–204.

Schein, E., 1985. Organizational Culture and Leadership. Jossey-Bass, San Francisco, CA.

Schein, E., 2012. Preface. In: Ashkanasy, C., Wilderom, M.F. (Eds.), Organizational Culture and Climate. Sage Publications, Inc, 2455 Teller Road, Thousand Oaks California 91320 United States, pp. xi–xiii.

Schneider, B., Goldstein, H.W., Smith, D.B., 1995. The ASA framework: An update. Pers. Psychol. 48, 747–773.

Siponen, M.T., Adam Mahmood, M.., Pahnila, S., 2014. Employees' adherence to information security policies: An exploratory field study. Inf. Manag. 51, 217–224.

Siponen, M.T., Iivari, J., 2006. Six Design Theories for IS Security. J. Assoc. Inf. Syst. 7, 445–472.

Siponen, M.T., Pahnila, S., Mahmood, A., 2010. Compliance with Information Security Policies: An Empirical Investigation. Computer (Long. Beach. Calif). 43, 64–71.

Siponen, M.T., Vance, A., 2010. Neutralization: New insights into the problem of employee information systems security policy violations. MIS Q. Manag. Inf. Syst. 34, 487–502.

Sommestad, T., 2015. Social Groupings and Information Security Obedience Within Organizations, International Information Security and Privacy Conference. Springer Berlin / Heidelberg, Hamburg.

Sommestad, T., Hallberg, J., 2013. A review of the theory of planned behaviour in the context of information security policy compliance. In: Janczewski, E., Wolf, H., Shenoi, S. (Eds.), International Information Security and Privacy Conference. Springer Berlin / Heidelberg, Auckland.

Sommestad, T., Hallberg, J., Lundholm, K., Bengtsson, J., 2014. Variables influencing information security policy compliance: a systematic review of quantitative studies, Information management and computer security.

Sommestad, T., Karlzén, H., Hallberg, J., 2015. A Meta-Analysis of Studies on Protection Motivation Theory and Information Security Behaviour. Int. J. Inf. Secur. Priv. 9, 26–46.

Sommestad, T., Karlzén, H., Hallberg, J., 2017. The Theory of Planned Behavior and Information Security Policy Compliance (in press). J. Comput. Inf. Syst.

Statistics Sweden, 2016. No Title [WWW Document]. Longitud. Integr. database Heal. Insur. labour Mark. Stud. (LISA by Swedish acronym). URL http://www.scb.se/lisa-en (accessed 3.29.16).

U.S. Bureau of Labor Statistics, 2014. Table 5. Median years of tenure with current employer for employed wage and salary workers by industry, selected years, 2004-14 [WWW Document]. Empl. Tenure. URL http://www.bls.gov/news.release/tenure.t05.htm (accessed 5.9.16).

Yammarino, F.J., Dansereau, F., 2011. Multilevel Issues in Organizational Culture and Climate Research. In: Ashkanasy, N.M., Wilderom, C.P.M., Mark F. (Eds.), The Handbook of Organizational Culture and Climate. SAGE Publications, Inc., 2455 Teller Road, Thousand Oaks California 91320 United States, pp. 50–76.