HAL
archives-ouvertes.fr

Social Groupings and Information Security Obedience Within Organizations

Teodor Sommestad

▶ **To cite this version:**

Teodor Sommestad. Social Groupings and Information Security Obedience Within Organizations. Hannes Federrath; Dieter Gollmann. 30th IFIP International Information Security Conference (SEC), May 2015, Hamburg, Germany. IFIP Advances in Information and Communication Technology, AICT-455, pp.325-338, 2015, ICT Systems Security and Privacy Protection. <10.1007/978-3-319-18467-8_22>. <hal-01345118>

HAL Id: hal-01345118
https://hal.inria.fr/hal-01345118

Submitted on 13 Jul 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution| 4.0 International License

Social groupings and information security obedience within organizations

Teodor Sommestad

Swedish Defence Research Agency (FOI), Olaus Magnus väg 42, Linköping, Sweden
Teodor.Sommestad@foi.se

Abstract. Individuals' compliance with information security policies is important for the overall security of organizations. It has been suggested that obedience cultures exist in organizations and that social processes and structures play a role for the compliance intentions and compliance behavior of individuals. This paper investigates if individuals' compliance intention is more homogenous within social groups in the workplace than they are within the workplace overall workplace and the effect these groups have are in line with the theory of planned behavior. The results show that a considerable portion of variance in information security policy compliance intentions is explained by the respondents' organizational department (15%), professional knowledge area (17%), and the same lunch room (18%). While sizeable and significant effects can be found on intentions the effects on attitudes, norm and perceived behavior control are less clear. The only statistically significant ($p<0.05$) effect is from department on attitudes and perceived norm, each with 6% explained variance. This suggests that the theory of planned behavior fails to account for factors tied to these types of social groups.

Keywords: information security culture, theory of planned behavior, information security behavior, compliance, obedience.

1 Introduction

Information security behavior is important for the overall security of organizations. It is also a lively research area and a considerable number of studies have been performed to identify factors that influence individuals' information security behavior. In a recently published review we identified 29 quantitative empirical studies published

adfa, p. 1, 2011.
© Springer-Verlag Berlin Heidelberg 2011

before March 2012 testing antecedents of security policy compliance attitudes, intentions and behavior [1]. Meanwhile, social aspects related to information security have gained increased attention in recent years, often discussed as information security culture. Theory suggests that if managers can predict or control the information security culture(s) of their organization they can manage the information security of their organization more efficiently [2]. For instance, [3] suggests that educational efforts should be adapted to cultural differences.

Information security culture is a concept that is used and interpreted in many different ways. However, there is a wide agreement that it is a group phenomenon where something is shared in the group and that social context and communication play a role. For instance, Hofstede [4] states that "cultures of work organizations are acquired through socialization at the work place." It follows that the frequency and the way people interact ought to determine the culture they share. However, as will be shown below, there is little known about how social processes form individuals' information security compliance.

In this paper the relationship between social groups' and individuals' views of information security policy compliance is investigated. A questionnaire-based survey within a governmental research institute in Sweden is used to assess individuals' views on information security policy compliance and the social groups they belong. Individuals' views are measured as prescribed by the theory of planned behavior [5]. This theory states that the effect of social factors (like culture) on intentions to perform a behavior is fully mediated by attitude, perceived norms and perceived behavior control associated with the behavior [5]. The effect of social group membership on information security culture is measured by comparing the responses in the organization as a whole to the responses within three types of groups within the organization namely groups based on: organizational department, professional knowledge area, and lunch room.

The outline of this paper is as follows. Section 2 describes the theoretical background and presents the hypotheses that are addressed. Section 3 details the method. In section 4 the results are presented and in section 5 implications are discussed. In section 6 conclusions are drawn.

2 Theory and research questions

This section will introduce some of the more central ideas needed to understand the present focus and scope of the present study. The theory of planned behavior (TPB) is described in section 2.1 and a broad description of information security culture is given in 2.2. The hypotheses derived from this are described in section 2.3.

2.1 The theory of planned behavior

The TPB [6] and its predecessor, the theory of reasoned action [7], offer an established framework for predicting behavioral intentions and actual behavior. According to the theory, illustrated in Figure 1, behavior is influenced by people's intentions and

actual behavior control, where actual behavior control moderates the effect of intentions. Most applications use perceived behavior control as a proxy because of the difficulties associated with measuring actual behavior control, as advocated by [6]. Additionally, the moderating role of perceived behavior control has been difficult to establish empirically, and many models include it side-by-side with intentions in a simpler additive linear model [5].

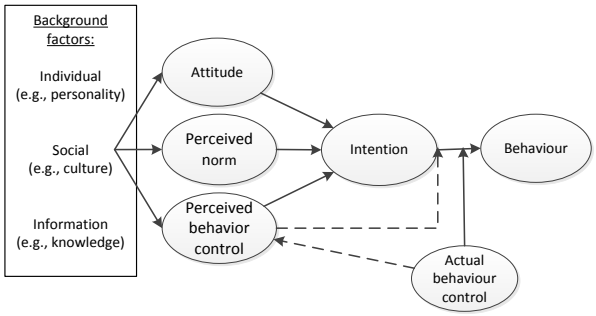

Fig. 1. The theory of planned behavior and culture, adapted from [5].

The TPB further states that intentions are influenced by attitude, perceived norms, and perceived behavior control. Their influences are assumed to be linear, i.e., the effects can be modeled using additive models. Although the theory claims that these three constructs are sufficient to explain the intentions concerning a behavior in question, there is no universal ordering of their importance. On the contrary, the relative importance of the constructs differs among populations and behaviors. For instance, for behaviors over which people feel they have almost full control, the variable perceived behavior control is of little value because it is equal for all respondents [6] .

A recent meta-analysis of observational questionnaire based studies of information security policy compliance behavior found the following sample-weighted correlation coefficients between variables: attitude-intention 0.48, perceived norm-intention 0.52, perceived behavior control-intention 0.45, intention-behavior 0.83 and actual behavior control-behavior 0.35 [8]. Approximately 0.4 of the variance in security policy compliance intentions is explained by the variables in the theory, leaving approximately 0.6 of the variance in intentions to be explained by measurement error and missing variables.

As Figure 1 shows, the originators of the theory of planned behavior explicitly list culture as a primary antecedent to the constructs that the theory says influence behavior [5]. The study presented in this paper focuses on this link between culture and information security compliance. More precisely, this study aims to investigate if social groups at the work place influence the variables of the theory of planned behavior in this way.

2.2 Information security culture

Research on information security culture rests heavily on the more general concept of organizational culture and the theories developed related to culture in other fields.

However, this is of little help when it comes to agreeing on a definition for the concept – already in 1998 a review found 54 different definitions of the concept of organizational culture in the literature [9].

Research on information security culture often focuses on policy compliance. For example, in [10] it is argued that information security obedience (i.e., compliance with policies) binds together information security, corporate governance and corporate culture and in [11] "culture" is described as the ideal state of "compliance. The most frequently cited their theoretical frameworks in r research on information security culture [12] are those of Edgar Schein and Geert Hofstede. Schein's framework is a three-tiered model that explains organizational culture on the levels of shared basic assumptions, espoused values and artifacts/behaviors [13]. Schein recently argued for a move away from discussions about abstract definitions and more concrete operationalizations instead, e.g., through measurement instruments [14]. Hofstede, known to have developed the first empirical model of dimensions of national cultures, provides a succinct definition of culture as "the collective programming of the mind that distinguishes the members of one group or category of people from another" [15].

In Hofstede's definition, and in Schein's model, culture can be tied to various groupings of humans, e.g., nations, cities, organizations, work groups, occupations, professions, and so on. Four levels of analysis for perception in organizational culture research are distinguished in [16]: 1) individuals, 2) workgroups or teams that interact on a face to face or virtual basis, 3) larger groups like whole organizations and 4) societies or countries. The current study is focused on level two and aims at examining the notion that social groupings in the workplace form individuals' information security policy compliance. There is little knowledge on the relative importance of different social groupings on this level, or what the relative importance depends on. Previous research on information security culture has primarily addressed the concept on an organizational level (e.g., [17] [2] [18]), surveyed how individuals perceive the culture (e.g., [19][20][21]) or group norms (e.g., [22]), and occasionally on a national level (e.g., [23]). Furthermore, there is also little known about the relative importance of different social groups for attitudes and values related to information security, such attitudes and values to safety. For example, no quantitative measurements on the relation between different groups and safety views can be found in the following reviews of safety climate and safety culture measurements [24][25][26].

To summarize, information security culture is (like culture in general) difficult to define and measure, it is relatively often coupled to policy compliance, and there is little research on information security culture between the levels of whole organizations and single individuals. The present study does not attempt to define the concept of culture, but use social groups within an organization as a proxy for the culture(s) individuals belong to and use these as proxies for the culture an individual belongs to. This paper follows the definition of Turner [27] and consider a social group to be two or more individuals who share a common social identification of themselves or two or more individuals who perceive themselves to be members of the same social category.

2.3 Hypotheses

Three main hypotheses together with nine sub-hypotheses are addressed in this study. These hypotheses concern how *organizational departments*, *professional knowledge* areas, and *lunch room* explain variation in constructs covered by the theory of planned behavior. They are discussed and presented below.

In most organizations, managers try to set goals, measure the achievement of goals and incentivize their staff through different types of social interactions (e.g., meetings, courses and documents). When it comes to information security, it can be expected that middle management plays the important role of implementing information systems strategies [28] and their behavior is believed to be vital to cultural change because of the feedback they give to employees [29]. In our study's organization, the management structure follows, as in many other organizations, the organizational structure and projects are heavily associated with this structure although they are not bound by it. Thus, the organizational department a person belongs to ought to shape its views on information security policies. The following hypotheses are therefore posed.

H1: Intentions to comply with information security policies are more homogenous within organizational department than within the organization as a whole.

H1.1: Attitudes to compliance with information security policies are more homogenous within organizational department than within the organization as a whole.

H1.2: Perceived norms with respect to compliance with information security policies are more homogenous within organizational department than within the organization as a whole.

H1.3: Perceived behavior control over compliance with information security policies is more homogenous within organizational department than within the organization as a whole.

In the studied organization eleven knowledge areas are defined by management. The knowledge area an individual is part of can also be expected to influence the culture an individual is a part of for several reasons. First, a professional knowledge area can be associated with certain codes of ethics, symbols, role models and professional goals. An example is the Hippocratic Oath sworn by those who practice medicine. Second, the professional knowledge area an individual works within often coincides with a particular type of schooling and knowledge. For instance, an individual who works with the secretive domain of electronic warfare can be expected to treat restrictions on electromagnetic leakage from information technology with more care than a person unaware of the risks associated with this. Third, it could be expected that individuals end up in social interactions with peers in the same knowledge area more often than they do with people from a randomly selected (other) knowledge area. In the studied organization most projects are within a particular knowledge area. Thus, the professional knowledge area ought to coincide with the workgroups and projects an individual belongs to. These factors lead to the following hypotheses.

H2: Intentions to comply with information security policies are more homogenous within professional knowledge areas than within the organization as a whole.

H2.1: Attitudes to compliance with information security policies is more homogenous within professional knowledge area than within the organization as a whole.

H2.2: Perceived norms with respect to compliance with information security policies are more homogenous within professional knowledge area than within the organization as a whole.

H2.3: Perceived behavior control over compliance with information security policies are more homogenous within professional knowledge area than within the organization as a whole.

Informal social interaction, like unstructured discussions and chattering, can be expected to play a role in the formation and conservation of information security culture. For instance, rumors, stories, gossip and opinions may be vetted during informal discussions and meetings might concern information security. To reliably group people according to how they socialize informally is of course difficult. However, in the present organization, located in Sweden, where "fika" (coffee breaks) is a social institution, and lunch rooms are places where informal meeting occur multiple times each day. Because of this, the lunch areas a person belong to captures much of an employee's informal social life and the following hypotheses are posed.

H3: Intentions to comply with information security policies are more homogenous within lunch areas than within the organization as a whole.

H3.1: Attitudes to compliance with information security policies are more homogenous within lunch areas than within the organization as a whole.

H3.2: Perceived norms with respect to compliance with information security policies are more homogenous within lunch areas than within the organization as a whole.

H3.3: Perceived behavior control over compliance with information security policies are more homogenous within lunch areas than within the organization as a whole.

None of the abovementioned hypotheses concerns actual behavior. The reason is not theoretical (culture is supposed to form behavior too); the reason is the costs and privacy issues associated with measuring actual policy compliance by monitoring employees behavior, especially without introducing observer bias.

3 Method and materials

This section presents the measurement instrument used in this study (section 3.1), the data collection procedure (section 3.2) and assessment of instrument validity in (section 3.3).

3.1 Measurement instrument

The questionnaire used contained an introductory section describing the purpose of the survey, a section explaining the question format, questions about the respondent's role and the social groups the respondent belonged to, questions operationalizing constructs in the theory of planned behavior, and other questions not directly related to the hypotheses addressed in this research.

Through a large number of applications, tests and reviews of the theory of planned behavior, a considerable amount of knowledge concerning how to best operationalize the theory in general has been accumulated. The parts of this measurement instrument associated with TPB was based on the example and template for direct scales given in [5] and followed the guidelines it provides. Thus, both instrumental (e.g., bad-good) and experiential (e.g., necessary-unnecessary) attitudes were measured; items of perceived norms measured both injunctive norms (i.e., what people that are important think) and descriptive norms (i.e., what people that are important do); perceived behavior control covered both autonomy (e.g., if it is under my control) and capability factors (e.g., if it is easy to do). Intentions were measured as outright intention predictions of future behavior. As recommended by [5] a questionnaire with open-ended questions was distributed in the target population to survey general beliefs related to the studied constructs before items were formulated. The answers were used as input in the formulation of the questionnaire items, e.g., to form bipolar scales for the attitude items. Three to four items were used for each TPB construct. Appendix contains a translation of the questions to English.

Questions regarding organizational department and knowledge area were formulated as multiple choice questions; lunch room was asked for in the form of a free text field with examples of the type of formulations to be used. All other questions in the questionnaire were associated with the behavior of complying with the information security policy and rules within the specific organization surveyed. These items were answered using a seven-point semantic differential scale. Their mean value is used to form the construct of interest, as proposed by [5].

The layout and understandability of the instrument was reviewed iteratively by six employees within the surveyed organization before a final version was established. In this review process it was also verified that respondents understood the questions related to organizational department, knowledge area and lunch area.

3.2 Data collection procedure

This study surveyed perceptions of individuals within the Swedish Defence Research Agency in Sweden (also the organization the author belongs to). This organization is distributed over four geographical sites and has approximately 1000 employees, with a median age of 45 years and a relatively even age distribution. Approximately 35 percent hold a PhD. Approximately 800 work as researchers and 200 as work as managers or with internal services (e.g., information systems or facilities).

The internal mail service distributed one printed copy of the survey to each employee during September 2013. A reminder was distributed electronically one week later. Surveys received within the first three months after the distribution were included in the analysis. A total of 311 questionnaires were returned within this time period. To ensure anonymity, respondents were encouraged to provide their department, knowledge area, and lunch area only if they wanted and felt comfortable doing so. Since many chose to only answer one or two of the three questions, a number of returned surveys could not be used for the test of research questions posed in this paper. In addition, it was deemed necessary to exclude respondents who belonged to groups

of less than two persons to obtain a meaningful statistical measurement of the variance in the group. As a result of this filtering, only 176-178 questionnaires contained the responses necessary for the analysis of the 12 hypotheses.

Visual inspection of QQ-plots and histograms suggests that all constructs are approximately normally distributed except attitude, which suffers from ceiling effects (with many respondents answering maximum). The results of tests with ANOVA (which is robust to deviations from the normality assumption (Schmider et al., 2010)) show that no mean differences of statistical significance (at the 5%-level) could be found between respondents returning the survey in different months for the four constructs. Nor was any statistical difference in mean values found between those who provided all the information that was required for the analysis and those that did not. Thus, the survey does not appear to suffer from problems due to non-response bias. Furthermore, the number of respondents from different departments, sites and roles match the overall distribution in the organization reasonably well, suggesting that the respondents are representative of the organization as a whole.

3.3 Instrument validity

Only five respondents used the feedback section to report difficulties in answering the questions in the questionnaire. Three of these reports concerned difficulties in answering because of the abstraction level of overall policy compliance rather than specific behavior (e.g., practices related to passwords or USB sticks). Two complained about the language and understandability of the questions.

The constructs and relationships of the theory of planned behavior are well established and this survey does not posit new constructs and builds on previous work on how questions should be formulated. Therefore the construct validity of the present survey is to some extent already given. The reliability, i.e., accuracy, of psychological measurements can be measured using Cronbach's alpha [30]. The reliability of all constructs except perceived behavior control exceeded 0.70, a commonly used threshold [31]. The reliability values for perceived behavior control (α=0.69) is on the border of acceptable, meaning that the answers to the three items used to measure these constructs are somewhat inconsistent. This might be because they are operationalized in two dimensions: perceived behavior control is supposed to capture both autonomy and capacity.

4 Results

The hypotheses stated in section 2.3 are evaluated by assessing if variance in peoples' views about information security policies is lower within groups than within the organization as a whole. In other words, it is expected that a part of the variance in respondents' responses is explained by the group they belong to.

Table 1 describes the results of one-way ANOVA tests. The effect size Eta squared reflects the portion of variance explained by the social groups that respondents belong to, i.e., the quotient of sum of squares between groups and the sum of squares of the

population as a whole. The p-value reflects the probability that the effect is due to chance.

Table 1. Variance explained by social groupings.

		Attitude	Perceived Norm	Perceived behavior control	Intention
Departments (K=5, N=177)	Eta-squared	0.06	0.06	0.03	0.15
	P-value	0.01	0.00	0.09	0.00
Knowledge areas (K=11, 178)	Eta-squared	0.05	0.05	0.05	0.17
	P-value	0.17	0.16	0.20	0.00
Lunch areas (K=21, N=176)	Eta-squared	0.10	0.13	0.11	0.18
	P-value	0.69	0.36	0.57	0.04

K: The number of groups
N: The number of respondents

As Table 1 shows, variance in all psychological constructs is lower within departments than within the organization as a whole. The effects are also statistically significant to the 0.05-level on all constructs except perceived behavior control. Thus, H1 and H1.1, and H1.2 are supported in this sample, but not H1.3.

The relationship to knowledge areas is not as straightforward. Considerable statistical significant reductions in variance are found for intention (H2), meaning that H2 is supported. However, a more modest measured and statistically insignificant effect is found for attitude, perceived norm, and perceived behavior control. Thus, H2.1, H2.2, and H2.3 are not supported.

As for knowledge areas, the effect measured by lunch areas is considerable and statistically significant for intentions to comply. However, even though the effect sizes are fairly large for attitude, perceived norm, and perceived behavior control, none of these effects are statistically significant. In other words, H3 can be accepted, but H3.1 H3.2, and H3.3 cannot be accepted.

Overall, the results confirm the hypotheses concerning an influence of social groups on intentions to comply with information security policies. Effects in terms of reduced variance (i.e., Eta-squared) on intentions are between 15 and 18 percent. These results suggest that social processes and structures play a large role in forming the information security obedience intentions. In other words, respondents' intentions to comply with the information security policy is to some extent explained by which department they work at, in which knowledge area they work, as well as who they drink coffee with and have their lunch with.

People within organizational departments are also more homogenous when it comes to attitudes and perceived norms. With a p-value of 0.09 the there is also a tendency that perceived behavior control is influenced by department. However, in contrast to what was predicted, professional knowledge areas and lunch rooms do not appear to explain variance in attitudes, perceived norms, and perceived behavior control. Thus, while people within the same professional knowledge areas and lunch room have homogenous intentions, there is no clear forming effect on attitudes, perceptions of norms and perceptions of how much control they have.

5 Discussion

The results of this study are far from clear-cut. To assist the reader in the interpretation of the results some of the major issues with the study are discussed below. Issues of dependence between the groups and confound variables are discussed in section 5.1, implications related to the theory of planned behavior in section 5.2, and measurement issues in section 5.3.

5.1 Dependence between social groupings and confounding variables

There are apparent relationships between the three types of social groups in the studied organization. First, both knowledge areas and coffee rooms are, to some extent, determined by departments. Knowledge areas are highly concentrated to specific departments because of organizational reasons. In seven of the knowledge areas the respondents comes from only one or two departments; within each of the departments one to seven knowledge areas are represented. Because of a tendency to collocate departments geographically the lunch areas are more likely to be shared by two persons form the department than by two persons from different departments. Overall the respondents use 21 lunch rooms, but within departments between one and nine lunch rooms are used. In addition, 14 of the 21 lunch rooms are used by people from one department only. Second, people within the same knowledge area are often collocated because of the need to interact with each other, and therefore often share the same lunch room. Ten lunch rooms is used by one knowledge area only and most knowledge areas are keep within three lunch rooms.

Unfortunately, the sample size makes it difficult to control for these dependencies by further partitioning of the sample into sub groups (e.g., a particular knowledge area within a specific department). Readers are therefore cautioned to treat the effects as independent. It is likely that parts of the variance that one social grouping explains is also explained by the other social groupings.

Furthermore, the effects on the response variables may be due to confounding variables that have little to do with culture but are related to the social groupings. The explained variance may be due to more direct links to influential variables than the social interaction that follows from these three groupings. It is not necessarily because they share the same culture (e.g., underlying assumptions or values). For example, the effect of knowledge area on compliance intentions might simply be because information security requirements are trickier to live up to for some types employees than others (e.g., because of certain clients), because some researchers are better skilled in tasks required to be compliant (e.g., are schooled in information security) or because information security is a more important issue within some areas.

In addition, variables associated with the Swedish culture and with this particular organization's culture or policies may skew the results obtained. For instance, the managers in this organization may be unusually influential, particularly homogenous knowledge areas may not be present, and discussions during coffee breaks may be unusually relevant or irrelevant to information security.

5.2 Theory of planned behavior as a mediator of cultural phenomena

The theory of planned behavior states that attitudes, perceived norm and perceived behavior control moderate the effect of culture on individuals' intentions. Based on this, one would expect that variables that predict behavioral intentions also predicts attitudes, perceived norm and perceived behavior control. For departments this is the case. Responses to all four variables within groups are more homogenous and the forming effect of these groups may be mediated as the theory of planned behavior claims. However, knowledge areas and lunch areas mean a significant reduction in variance in intentions to comply, but not attitudes, norms or perceived behavior control.

A direct effect on intentions, without mediation by attitude, perceived norm or perceived behavior control, suggests that something is missing in the theory of planned behavior which is common to members in the social groups. As noted above, this missing piece is not necessarily culture alone. It may be an effect of other factors already hypothesized as antecedents to the variables of the theory of planned behavior which are coupled to the social groups, like: knowledge, media exposure, interventions, age, gender, risk perception, moods or personality. Nevertheless, factors captured by knowledge areas and lunch areas seems to influence intentions without being mediated the way the theory of planned behavior say they should be. This warrants further investigations of the sufficiency of this theory with respect to social processes and structures.

5.3 Measurement issues

The sample frame used to test the hypotheses addressed in research is well defined: a Swedish defense research organization with highly educated employees, a fairly even age distribution and approximately 1000 employees distributed over four geographical locations. This workplace definitely represents an organization in which information security is of relevance and security policies are important. However, it is only one organization, chosen because it was convenient. Clearly, to generalize from one single organization is risky. Furthermore, the response rate (as low as 18% for some tests) is problematic. Even though no clear signs of response bias can be observed there are problems associated with drawing general conclusions from these results. For example, seven managers in one organization can hardly be said to represent managers/departments in general. And group sizes as small as two or three persons pose another potential source of measurement error if the actual groups (e.g., using a lunch area) are substantially bigger.

The small sample also prohibits the use of more sophisticated statistical measures to address the hypotheses. A multilevel analysis was performed using LISREL to identify the effect of a second level on predictions of intention. This analysis suggests that around five percent of the variance in intentions is explained by the groups (department 8%; knowledge area 7%; lunch area 3%) when they are added to a model that already includes the other antecedents (attitude, perceived norm and perceived behavior control). However, with the sample size of this study the effects are insignif-

icant and associated with considerable confidence intervals. With a larger sample, multi-level analysis could be used to better test if these types of social groups play a significant role in forming intentions without being mediated by attitude, perceived norms, and perceived behavior control. This would enable assessments of how much variance the social groupings add on top of the variables in the TPB.

6 Conclusion

In the studied organization, 15-18 percent of the variance in intentions to comply with information security policies can be explained by the department they belong to, knowledge area they work within and lunch room they use. The results are in line with the idea that group phenomena influence security behavior and those social processes and structures play a role for the information security obedience culture of organizations. In addition, the explanatory power of these social groupings based on professional knowledge areas and lunch rooms does not appear to be mediated by the constructs of the theory of planned behavior. This suggests that this theory misses important variables for explaining information security policy compliance.

7 References

1. Sommestad, T., Hallberg, J., Lundholm, K., Bengtsson, J.: Variables influencing information security policy compliance: a systematic review of quantitative studies. Inf. Manag. Comput. Secur. 22, 42–75 (2014).
2. Veiga, A. Da, Eloff, J.: A framework and assessment instrument for information security culture. Comput. Secur. 29, 196–207 (2009).
3. Lacey, D.: Understanding and transforming organizational security culture. Inf. Manag. Comput. Secur. 18, 4–13 (2010).
4. Hofstede, G.: National cultures, organizational cultures, and the role of management. In: González, F. (ed.) Values and Ethics for the 21st Century. pp. 385–403. BBVA, Madrid, Spain (2011).
5. Fishbein, M., Ajzen, I.: Predicting and Changing Behavior: The Reasoned Action Approach. Psychology Press, New York, NY, USA (2010).
6. Ajzen, I.: The theory of planned behavior. Organ. Behav. Hum. Decis. Process. 50, 179–211 (1991).
7. Fishbein, M.: A theory of reasoned action: Some applications and implications. Nebraska Symp. Motiv. 27, 65–116 (1979).
8. Sommestad, T., Hallberg, J.: A review of the theory of planned behaviour in the context of information security policy compliance. In: Janczewski, E., Wolf, H., and Shenoi, S. (eds.) International Information Security and Privacy Conference. Springer Berlin / Heidelberg, Auckland (2013).
9. Verbeke, W., Volgering, M., Hessels, M.: Exploring the Conceptual Expansion within the Field of Organizational Behaviour: Organizational Climate and Organizational Culture. J. Manag. Stud. 35, 303–329 (1998).
10. Thomson, K.-L., von Solms, R.: Information security obedience: a definition. Comput. Secur. 24, 69–75 (2005).
11. Furnell, S., Thomson, K.-L.: From culture to disobedience: Recognising the varying user acceptance of IT security. Comput. Fraud Secur. 2009, 5–10 (2009).

12. Karlsson, F., Åström, J., Karlsson, M.: Information security culture: State-of-the-art review between 2000 and 2013. Inf. Comput. Secur.
13. Schein, E.: Coming to a new awareness of organizational culture. Sloan Manage. Rev. 25, (1984).
14. Schein, E.: Preface. In: Ashkanasy, C. and Wilderom, M.F. (eds.) Organizational culture and climate. pp. xi–xiii. Sage Publications, Inc, 2455 Teller Road, Thousand Oaks California 91320 United States (2012).
15. Hofstede, G.: Dimensionalizing cultures: The Hofstede model in context. Online readings Psychol. Cult. 2, 1–26 (2011).
16. Yammarino, F.J., Dansereau, F.: Multilevel Issues in Organizational Culture and Climate Research. In: Ashkanasy, N.M., Wilderom, C.P.M., and Mark F. (eds.) The Handbook of Organizational Culture and Climate. pp. 50–76. SAGE Publications, Inc., 2455 Teller Road, Thousand Oaks California 91320 United States (2011).
17. Malcolmson, J.: What is security culture? Does it differ in content from general organisational culture? 43rd Annual 2009 International Carnahan Conference on Security Technology. pp. 361–366. IEEE (2009).
18. Schlienger, T., Teufel, S.: Information security culture-from analysis to change. IFIP TC11 International Conference on Information Security. , Cairo, Egypt (2003).
19. Hu, Q., Dinev, T., Hart, P., Cooke, D.: Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture*. Decis. Sci. 43, 615–660 (2012).
20. Dugo, T.M.: The insider threat to organizational information security: a sturctural model and empirical test, http://etd.auburn.edu/etd/handle/10415/1345, (2007).
21. McCoy, B., Stephens, G., Stevens, K.: An Investigation of the Impact of Corporate Culture on Employee Information Systems Security Behaviour. (2009).
22. Herath, T., Rao, H.R.: Protection motivation and deterrence: A framework for security policy compliance in organisations. Eur. J. Inf. Syst. 18, 106–125 (2009).
23. Furnell, S.: End-user security culture: A lesson that will never be learnt? Comput. Fraud Secur. 2008, 6–9 (2008).
24. Guldenmund, F.W.: The use of questionnaires in safety culture research – an evaluation. 45, 723–743 (2007).
25. Flin, R.: Measuring safety culture in healthcare : A case for accurate diagnosis. 45, 653–667 (2007).
26. O'Connor, P., O'Dea, A., Kennedy, Q., Buttrey, S.E.: Measuring safety climate in aviation: A review and recommendations for the future. Saf. Sci. 49, 128–138 (2011).
27. Turner, J.C.: Towards a cognitive redefinition of the social group. In: Tajfel, H. (ed.) Social identity and intergroup relations. pp. 15–40. Cambridge University Press, Cambridge, Great britain (1982).
28. Leidner, D.E., Milovich, M.: Middle Management and Information Systems Strategy: The Role of Awareness and Involvement. 2014 47th Hawaii International Conference on System Sciences. pp. 4396–4405. IEEE (2014).
29. Niekerk, J. Van, Solms, R. Von: An holistic framework for the fostering of an information security sub-culture in organizations. Information Security South Africa (ISSA) (2005).
30. Cronbach, L.J., Shavelson, R.J.: My Current Thoughts on Coefficient Alpha and Successor Procedures. Educ. Psychol. Meas. 64, 391–418 (2004).
31. Peterson, R.A.: Meta-analysis of Alpha Cronbach's Coefficient. J. Consum. Res. 21, 381–391 (2014).

Appendix: Questionnaire items

Attitude

Adhering to the information security policy at [the organization] *is:*

(bad<->good)

(meaningless <->meaningful)

(unimportant<->important)

(unnecessary<->necessary)

Perceived norm

Most people who are important to me think I should adhere to the information security policy that exists at [the organization]. (false<->true)

Most people whose opinion I respect would tolerate that I adhere to the information security policy that exist at [the organization]. (improbable<->probable)

Most people I respect would adhere to the information security policy at [the organization] *if they were in my situation*. (unlikely<->likely)

Most people at [the organization] *who are like me follow our information security policy.* (false<->true)

Perceived behavior control

I am certain that I can adhere to the information security policy that exists at [the organization]. (false<->true)

If I really want to, I can adhere to the information security policy that exists at [the organization]. (disagree<->agree)

Whether I adhere to the information security policy that exists at [the organization] is entirely within my control. (false<->true)

Intention

My intention is to henceforth adhere to the information security policy that exists at [the organization]. (false<->true)

In the future, I will adhere to all of the information security policies that exist at [the organization]. (unlikely<->likely)

Regardless of what happens and which situations arise, I will adhere to the information security policy that exists at [the organization]. (unlikely<->likely)

I cannot imagine violating the information security policy that exists at [the organization] *even once in the future*. (false<->true)