Understanding Information Security Compliance - Why Goal Setting and Rewards Might be a Bad Idea

N. Gerber[1,3], R. McDermott[1], M. Volkamer[2,3,4] and J. Vogt[1,3]

[1]Faculty of Human Sciences, Technische Universität Darmstadt, Germany[1]
[2]Faculty of Computer Sciences, Technische Universität Darmstadt, Germany[2]
[3]CASED (Center of Advanced Security Research Darmstadt), Germany[3]
[4]Faculty of Computer Sciences, Karlstad University, Sweden[4]
e-mail: n.gerber@psychologie.tu-darmstadt.de

Abstract

Since organizational information security policies can only improve security if employees comply with them, understanding the factors that affect employee security compliance is crucial for strengthening information security. Based on a survey with 200 German employees, we find that reward for production goal achievement negatively impacts security compliance. Whereas a distinct error aversion culture also seems to impair security compliance, the results provide no evidence for an impact of error management culture, affective commitment towards the organization, security policy information quality or quality of the goal setting process. Furthermore, the intention to comply with security policies turns out to be a bad predictor for actual security compliance. We therefore suggest future studies to measure actual behavior instead of behavioral intention.

Keywords

Information security, Goal Setting, Error Culture, Theory of Planned Behavior

1. Introduction

Every organization is concerned with information security nowadays. In some organizations (e.g., high reliability organizations like aviation), the core business is to provide safety and security. In most organizations, however, security is only one goal among many. If an organization's main goals compete with security goals, employees have to walk a fine line to perform well in their jobs without breaching security too much.

Sommestad et al. (2014) conducted a review of more than a hundred publications, containing a total of 29 studies dealing with employee information security policy compliance. Although several of the examined variables like perceived behavioral control, perceived justice of punishment, threat appraisal or normative beliefs seem to explain employee security policy compliance to some extent, no 'clear winner' could be identified. Furthermore, predictive power of some constructs differed considerably between the individual studies (for example, effect sizes for the influence of attitude towards compliance on the intention to comply ranged from β=0.15 to β=0.64). However, none of the studies focused explicitly on the subject of conflicting goals.

To close this gap, we conducted a survey with a diverse sample of German employees to further investigate the implications of conflicting (security and productivity) goals. Furthermore, we included the employees' evaluation of security policies, organizational culture, top management participation in security promotion and affective commitment to the organization, as these factors seem to influence security compliance (e.g., Sommestad et al., 2014).

The remainder of this paper is organized as follows: The second section provides the theoretical background for the explanation of security compliance behavior as well as the research hypotheses, the third section focuses on the research methodology, while the fourth section contains the analysis and results of our study. Finally, research findings are discussed in section five.

2. Theoretical background and hypotheses

2.1. Theory of planned behavior

The theory of planned behavior (TPB; Ajzen, 1991) is frequently used to explain human behavior, as it links cognitive beliefs, behavioral intention and behavior. According to TPB, attitude towards a behavior, subjective norm as well as perceived behavioral control shape the intention of an individual to behave in a specific way (e.g., to follow information security policies), which in turn affects the actual behavior. As defined by Ajzen (1991), attitude refers to the appraisal of a behavior, i.e. the performance of the behavior is perceived as positive or negative. Subjective norm means the social pressure to perform a behavior, which arises from the attitudes and beliefs of significant others. Finally, perceived behavioral control is based on Bandura's (1982) concept of perceived self-efficacy and refers to the subjective perception of a behavior as either easy or difficult to perform. Several researchers have successfully applied TPB to study information security compliance (e.g., Hu et al., 2012; Ifinedo, 2012; Sommestad & Hallberg, 2013). Based on the TPB, we propose that:

H1a: A positive attitude towards security policy compliance is associated with stronger intention to comply with security policies.

H1b: A positive subjective norm towards security policy compliance is associated with stronger intention to comply with security policies.

H1c: Higher levels of perceived behavioral control are associated with stronger intention to comply with security policies.

H2: A stronger intention to comply with security policies is associated with greater probability of actual security policy compliance.

2.2. Perceived top management participation in security initiatives

Hu and colleagues (2012) showed that perceived top management participation in security initiatives is one crucial factor in employee security policy compliance intention. Their study revealed that perceived top management participation influences employee's subjective norm and perceived behavioral control as well as organizational culture, which all in turn impact behavioral intention. Furthermore, attitude is influenced by perceived management participation indirectly through its effect on organizational culture. This leads us to the following assumptions:

H3a: Higher levels of perceived top management participation in security initiatives are associated with a more positive subjective norm towards security policy compliance.

H3b: Higher levels of perceived top management participation in security initiatives are associated with more perceived behavioral control.

2.3. Organizational culture

Referring to employee security compliance, one of the most important facets of organizational culture is error management. Error management culture has been shown to influence company performance through the communication about errors, help in error situations and quick detection and handling of errors (van Dyck et al., 2005). In this sense, a high error management culture is expected to enhance company performance. Moreover, it seems likely that it also improves security behavior. Another possible relationship exists between security compliance and error aversion culture, an opposite dimension of organizational error culture. High values in error aversion culture (i.e. covering errors up) are expected to impair security compliance, because employees are discouraged to talk about errors, which reduces the opportunity to learn from external as well as internal errors. Based on these assumptions, we hypothesize:

H4a: High error management culture is associated with a greater probability of actual security policy compliance.

H4b: Low error aversion culture is associated with a greater probability of actual security policy compliance.

2.4. Affective commitment to the organization

Employees who show high affective commitment towards their organization tend to perform better on their jobs than those lacking affective commitment (Meyer et al., 1989). Given that security policy compliance is somehow part of their jobs, employees exhibiting high commitment are also expected to do better in terms of security compliance:

H5: High affective commitment is associated with a greater probability of actual security policy compliance.

2.5. Quality of security policy information

No matter how motivated employees are to comply with security policies, to actually follow them, they need to know and understand these policies in the first place. Accordingly, Pahnila et al. (2007) showed that the quality of security policy information significantly influences security policy compliance. Therefore, we propose that:

H6: Higher quality of security policy information is associated with a greater probability of actual security policy compliance.

2.6. Goal Setting

Goal Setting can be described as the most popular and widely used management tool in our time. This is not surprising, considering that - following the basic assumptions of goal setting theory - challenging and specific goals lead to employees' higher commitment and ultimately higher performance (Locke & Latham, 1990). But goal setting might not be the panacea it has been taken for. A growing body of research shows that goal setting, when not used in a considerate manner, is also linked to a series of undesirable consequences. Among those are unethical behavior, disruptive effects on organizational climate and deterioration of subsequent performance if one misses one's goal (Welsh & Ordoñez, 2014; Zhang & Jia, 2013).

As stated above, information security goals often compete with production goals. It has been shown that competing goals can prompt employees to follow those goals that are easier to achieve or of higher personal value (Gilliland & Landis, 1992). Employees who are trying to meet excessive demands, thus may disregard information security goals, if they find them hard to follow (e.g., due to a lack of information quality) or if reaching their performance goal is more important to them (e.g., when performance is linked to a reward). On this account, the quality of the process, in which goals are set and the extent of rewards agreed on, is of high importance. Therefore, we propose that:

H7a: Performance incentives (rewards) for individual goal achievement are associated with a smaller probability of actual security policy compliance.

H7b: A high quality goal-setting process (e.g., supervisor support, goal clarity, participation, organizational resources) is associated with a greater probability of actual security policy compliance.

3. Research Methodology

3.1. Procedure and Participants

We conducted an online survey with 200 German employees. All questionnaires were implemented in SoSci Survey (oFb - der onlineFragebogen, 2016) and presented in German. It took participants about 20 minutes to complete the whole survey with a total of 115 items. Participants were recruited from the German online access panel 'keyfacts' (keyfacts online access panel, 2016). Of the respondents, 60.4% were female and 39.6% were male, ranging in age from 18 to 75 years. Employees from various industries (e.g., retail, consulting, health care, manufacturing, information technology, education, industry, financial services) participated in the study, with organizations ranging from small (less than 10 employees) to very large (more than 100.000 employees).

3.2. Measures

The quantitative measures used in the present study are based upon previously validated instruments whenever available (see Table 1). If not stated otherwise, the items are based on a 5-point Likert scale (1=strongly disagree; 5=strongly agree). To ensure reliability of the measures, internal consistency and factor loadings are checked for every subscale. Nearly all items showed an acceptable internal consistency (Cronbach's alpha > 0.7) and satisfying factor loadings (>.65), except for some of the error management culture items with factor loadings between .35 and .77. All inverted items measuring information quality were significantly impairing reliability, strongly indicating a methodological bias. Therefore, they were dropped from further analysis. Afterwards, only two items measuring appropriateness of information amount showed a non-satisfying Cronbach's alpha value of .65. All items can be found at http://www.arbing.psychologie.tu-darmstadt.de/home/forschung_4/forschungsergebnisse_fai.de.jsp

Construct	Reference
Theory of planned behavior	Hu et. al (2012)
Organizational culture	van Dyck (2005)
Commitment towards the organization	Schmidt et al. (1998)
Information quality	Lee et al. (2002)
Goal setting	Putz & Lehner (2002)
Goal Setting -Dysfunctional effects (four items)	Self-constructed

Table 1: Sources of measurement items

Actual compliance with security policies was measured using a single item ('Have you ever avoided or tried to avoid following a security policy (for example: You need information from a certain file, but don't have the right to access it. Since a request for access would take too long, you ask a colleague to send the file to you)?'). The item was based on a 5-point Likert scale (1=never, 5=always).

To further investigate employees' security policy compliance, we asked participants to answer several multiple choice questions about security policy handling in their organization. Furthermore, we added four open-ended questions to gain a deeper understanding of security policy knowledge management and participants' perceptions of the communication about security policies in their organization.

4. Analysis and Results

Hypothesis testing was conducted using a set of regression analyses. All statistical analyses were performed using IBM SPSS Statistics 21. Significance of p-values is considered on an alpha level of 5%, i.e. a p-value less than .05 is considered as significant. For interpretation of the results, it should be kept in mind that high values for the dependent variable 'actual security policy compliance' indicate little compliance with security policies, whereas low values imply good compliance.

4.1. Intention to comply with security policies (H1a-c)

As collinearity between the three predictor variables can be assumed, we chose a hierarchical regression procedure. Based on the results by Sommestad et al. (2014), perceived behavioral control (PBC) was entered as first and most important predictor into the model, resulting in an adjusted R^2 of .28, $F=67.98$, $p<.001$; i.e. a total of 28% in the variance of intention to comply with security policies can be explained by perceived behavioral control. Attitude (ATT) was entered as second predictor ($a.R^2=.62$, $F=141.44$, $p<.001$), whereas subjective norm (SN) was entered last ($a.R^2=.65$, $F=108.63$, $p<.001$). These results show that if attitude is added as predictor, the regression model explains a total of 62% in the variance of intention to comply, compared to 28% if only perceived behavioral control is used as predictor. However, the inclusion of subjective norm as predictor only adds another 3% of explained variance. The results of the final model are presented in Table 2. Although perceived behavioral control was entered first based on theoretical assumptions, attitude seems to be the best predictor for behavioral intention.

Mod.	Predictor	Beta	t-Value	Sig.	Hypothesis result
1	PBC	.53	8.25	<.001	H1a supported
2	PBC	.26	4.93	<.001	H1a supported
	ATT	.65	12.41	<.001	H1b supported
3	PBC	.15	2.89	=.008	H1a supported
	ATT	.52	9.04	<.001	H1b supported
	SN	.27	4.10	<.001	H1c supported

Table 2: Regression model for intention to comply with security policies

4.2. Perceived top management participation (H3a-b)

To test the effects of perceived top management participation (TMP), two simple linear regression analyses were conducted, resulting in an adjusted R^2 of .20 ($F=40.05$, $p<.001$) for subjective norm and an $a.R^2$ of .26 ($F=60.84$, $p<.001$) for perceived behavioral control (see Table 3 for predictor values).

DV	Predictor	Beta	t-Value	Sig.	Hypothesis result
SN	TMP	.44	6.33	<.001	H3a supported
PBC	TMP	.51	7,80	<.001	H3b supported

Table 3: Regression model for perceived top management participation

4.3. Actual compliance with security policies (H2, H4a-b, H5a-c, H6, H7)

To investigate the relationship between the supposed predictors and actual compliance with security policies, another hierarchical regression analysis was conducted. To determine the order in which predictors were entered into the analysis, we relied once more on the results by Sommestad et al. (2014), indicating intention to comply as first predictor ($a.R^2$=.03, F=6.52, p<.05), followed by error management culture, error aversion culture as well as affective commitment to the organization ($a.R^2$=.10, F=6.00, p<.001), for which no individual order of predictors could be assumed based on theoretical or empirical evidence. Quality of security policy information (IQ) was entered next ($a.R^2$=.10, F=4.91, p<.001), since it has proven to be of poor predictive power. As the focus of this study is to explore which new insights can be achieved by adding goal setting to the examination of security policy compliance, the different goal setting variables were entered in a last step ($a.R^2$=.24, F=4.91, p<.001) Although intention is a significant predictor in the first model, the subsequent analyses show that its predictive power disappears if other predictors are added to the model. The same applies to error aversion culture, which is only of predictive power as long as the goal setting variables are not included. In the final model, only reward for goal achievement provides a significant prediction for actual security policy compliance, with greater reward for goal achievement implying less compliance with security policies (see Table 4).

Mod.	Predictor	Beta	t-Value	Sig.	Hypothesis result
1	INT	-.19	-2.55	0.012	H2 supported
2	INT	-.12	-1.38	.171	H2 not supported
	ErrManCulture	-.02	-0.28	.779	H4a not supported
	ErrAverCulture	.26	3.55	.001	H4b supported
	AffComm	-.10	-1.28	.204	H5 not supported
3	INT	-.13	-1.55	.124	H2 not supported
	ErrManCulture	-.06	-0.58	.566	H4a not supported
	ErrAverCulture	.26	3.52	.001	H4b supported
	AffComm	-.11	-1.35	.179	H5 not supported
	IQ	.07	0.80	.427	H6 not supported
4	INT	-.01	-0.14	.891	H2 not supported
	ErrManCulture	-.13	-1.34	.182	H4a not supported
	ErrAverCulture	.07	0.80	.427	H4b not supported
	AffComm	-.10	-1.23	.220	H5 not supported
	IQ	.06	0.71	.479	H6 not supported
	Goal Clarity	.02	0.26	.795	H7a supported
	Goal Conflicts	.13	1.32	.188	H7b not supported
	Overstrain	.02	0.22	.828	
	Dysfunctional Effects	.07	0.67	.502	
	Support	-.21	-1.78	.076	
	Participation	.14	1.10	.271	
	Feedback	.17	1.34	.183	
	Reward	.30	3.08	.002	
	Resources	-.20	-1.94	.054	

Table 4: Regression model for actual compliance with security policies

4.4. Further investigation of security policy compliance, knowledge and communication

Statistical analysis of the multiple choice questions and actual security policy compliance yielded a significant relationship between compliance and participation in an information security training at the beginning of employment (Cramer's V=.27, p<.01) as well as perceived compliance of colleagues (Cramer's V=.29, p<.01). As expected, employees reporting security policies to constrain them in their daily work exhibit a greater probability for not complying with these policies (r=.62, p<.001).
Regarding knowledge of security policies, 58% of the participants stated that the extent to which their employer informs them about security policies is just right, whereas 37% require more and 5% fewer information. A total of 60% stated to have participated in trainings for information security at the beginning of their employment. Half of the participants (52%) stated that their colleagues sometimes depart from security policies, even though 40% claimed that compliance with security policies is monitored in their organization at least from time to time. While 41% feel that security policies constrain them in accomplishing their daily work tasks at least occasionally, 35% stated to have always complied with these policies. 30% reported to work around security policies infrequently and yet another 30% occasionally. Only a few participants reported intentional acts against security

policies frequently (3%) or always (1.5%), respectively. 72% reported to be taken seriously in discussions about information security, 68% stated that they are granted enough time to talk about their problems or concerns relating to information security and 65% uttered the impression that in discussions about information security, the 'same language is spoken'. If participants could change anything in communication about information security, 14% would require a clearer, more explicit formulation of security policies, as well as information through personal conversations, followed by an increase in communication itself or a higher frequency of meetings (13%). Ten percent would like to communicate only via e-mail, newsletter or bulletin, while another 6% prefer active discussions and 'round tables'.

5. Discussion and Conclusions

The findings of this study are twofold. We found evidence for the relationships between intention, attitude, perceived behavioral control and subjective norm, as they are stated in the theory of planned behavior (Ajzen, 1991). However, with perceived behavioral control being the least important predictor for behavioral intention, the relative importance of the individual constructs in our study differs from those Sommestad et al. (2014) found in their meta-analysis. According to our results, intention to comply with security policies is primarily affected by attitude towards compliance, followed by the subjective norm. Another important factor for security compliance intention is perceived top management participation in security initiatives, which in turn affects subjective norm and perceived behavioral control. This is in line with the results by Hu et al. (2012).

With regard to actual security policy compliance, intention to comply is only of predictive value as long as no other predictors are considered. The same is true for error aversion culture, which loses predictive power once goal setting is added to the prediction model. According to our analyses, error management culture, affective commitment and security policy information quality provide no predictive improvement at all. This is in contrast to Pahnila et al. (2007), who found that security compliance is affected by information quality. If all investigated predictors are considered, only the presence of rewards for performance goal achievement and their scale is associated with a decrease in security compliance. This is in line with recent findings implying several negative consequences for goal setting (e.g., Welsh & Ordonez, 2014).

5.1. Practical implications

Information security depends on both, technical excellence and human commitment to use it. The best technology does not ensure safe operation, if people don't use it as it was designed. Information security must make sense to employees, must be easy to understand and intuitively used; otherwise, people will find shortcuts and workarounds. To receive an improvement in employee security compliance, managers need to reconsider their rewarding arrangements, especially if goal achievement is likely to be constrained by security policy compliance.

5.2. Limitations and future research

One limitation of our study is that actual security compliance was measured via self-report and is therefore likely to contain some kind of bias as participants may be reluctant to report unsafe behavior. Another limitation is the use of regression analyses based on self-reported data, which allows no interpretation of causality. Further studies are needed to provide an experimental investigation of actual security compliance and the causal effects of goal setting on security behavior. Moreover, size and structure of the organizations should be considered. Future studies should also consider the actual content of the information security policies employees are referring to, as well as employee's knowledge of these security policies. As the recent trend in securing an organization's information assets goes to risk and risk assessment instead of compliance, future research should also consider the current organizational practices concerning information security.

6. References

Ajzen, I. (1991), "The theory of planned behavior", *Organizational Behavior and Human Decision Processes*, Vol. 50, No. 2, pp179-211.

Bandura, A. (1982), "Self-efficacy mechanism in human agency", *American Psychologist*, Vol. 37, pp122-147.

Gilliland, S. W., & Landis, R. S. (1992), "Quality and quantity goals in a complex decision task: Strategies and outcomes", *Journal of Applied Psychology,* Vol. 77, No. 5, pp672– 681.

Hu, Q., Dinev, T., Hart, P. and Cooke, D. (2012), "Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture", *Decision Sciences Journal*, Vol. 43, No. 4, pp615-659.

Ifinedo, P. (2012), "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory", *Computers & Security*, Vol. 31, No. 1, pp83-95.

keyfacts online access panel (2016), http://www.keyfacts-gmbh.de. (Accessed 15 January 2016)

Lee, Y.W., Strong, D.M., Kahn, B.K. and Wang, R.Y. (2002), "AIMQ: a methodology for information quality assessment", *Information & Management*, Vol. 40, pp133-146.

Locke, E.A. and Latham, G.P. (1990), *A theory of goal setting and task performance*, Prentice-Hall, Englewood Cliffs, ISBN: 0139131388.

Meyer, J.P., Paunonen, S.V., Gellatly, J.R., Goffin, R.D. and Jackson, D.N. (1989), "Organizational commitment and job performance: It's nature of the commitment that counts", *Journal of Applied Psychology*, Vol. 74, pp152-156.

oFb - der onlineFragebogen (2016), https://www.soscisurvey.de. (Accessed 22 October 2015)

Pahnila, S., Siponen, M. and Mahmood, A. (2007), "Employees' Behavior towards IS Security Policy Compliance", *Proceedings of the 40th Hawaii International Conference on System Sciences (HICSS'07)*, pp156-156b.

Putz, P. and Lehner, J. M. (2002), „Effekte zielorientierter Führungssysteme – Entwicklung und Validierung des Zielvereinbarungsbogens (ZVB)“, Zeitschrift für Arbeits- und Organiationspsychologie, Vol. 46, No 1, pp22-34.

Schmidt, K.-H., Holland, S. and Sodenkamp, D. (1998), “Psychometrische Eigenschaften und Validität einer deutschen Fassung des "Commitment"-Fragebogens von Allen und Meyer (1990)“, *Zeitschrift für Differentielle und Diagnostische Psychologie*, Vol. 19, No. 2, pp93-106.

Sommestad, T. and Hallberg, J. (2013), “A Review of the Theory of Planned Behaviour in the Context of Information Security Policy Compliance“, in Janczewski, L.J., Wolfe, H.B. and Shenoi, S. (Eds.) *Security and Privacy Protection in Information Processing Systems*, Springer, Berlin, Heidelberg, ISBN: 978-3-642-39217-7.

Sommestad, T., Hallberg, J. Lundholm, K. and Bengtsson, J. (2014), "Variables influencing information security policy compliance: A systematic review of quantitative studies", *Information Management & Computer Security*, Vol. 22, No. 1, pp42-75.

van Dyck, C., Frese, M., Baer, M. and Sonnentag, S. (2005), “Organizational error management culture and its impact on performance: a two-study replication“, *Journal of Applied Psychology*, Vol. 90, No. 6, pp1228-1240.

Welsh, D.T. and Ordoñez, L.D. (2014), “The dark side of consecutive high performance goals: Linking goal setting, depletion, and unethical behavior“, *Organizational Behavior and Human Decision Processes*, Vol. 123, No. 2, pp79-89.

Zhang, Z. and Jia, M. (2013), “How can companies decrease the disruptive effects of stretch goals? The moderating role of interpersonal- and informational- justice climates“, *Human Relations*, Vol. 66, No. 7, pp993-1020.