Productivity vs. Security: Mitigating Conflicting Goals in Organizations[*]

Peter Mayer[1], Nina Gerber[2], Ronja McDermott[2], Melanie Volkamer[1,3] & Joachim Vogt[2]

Faculty of Computer Sciences, Technische Universität Darmstadt, Germany[1]
Faculty of Human Sciences, Technische Universität Darmstadt, Germany[2]
Faculty of Computer Sciences, Karlstad University, Sweden[3]

e-mail: peter.mayer@secuso.org

Abstract

Purpose – This paper aims to contribute to the understanding of goal setting in organizations, especially regarding the mitigation of conflicting productivity and security goals.

Design/methodology/approach – This paper describes the results of a survey with 200 German employees regarding the effects of goal setting on employees' security compliance. Based on the survey results, a concept for setting information security goals in organizations building on actionable behavioral recommendations from information security awareness materials is developed. This concept was evaluated in three small to medium-sized organizations (SMEs) with overall 90 employees.

Findings – The survey results revealed that the presence of rewards for productivity goal achievement is strongly associated with a decrease in security compliance. The evaluation of the goal setting concept indicates that setting their own information security goals is welcomed by employees.

Research limitations/implications – Both studies rely on self-reported data and are therefore likely to contain some kind of bias.

Practical implications – Goal setting in organizations has to accommodate for situations, where productivity goals constrain security policy compliance. Introducing the proposed goal setting concept based on relevant actionable behavioral recommendations can help mitigate issues in such situations.

Originality/value – This work furthers the understanding of the factors affecting employee security compliance. Furthermore, the proposed concept can help maximizing the positive effects of goal setting in organizations by mitigating the negative effects through the introduction of meaningful and actionable information security goals.

Keywords Organizational context, Information security compliance, Goal setting
Paper type Research paper

[*] Author Accepted Manuscript version of this article. To cite this article, refer to the Version of Record available from: http://www.emeraldinsight.com/doi/abs/10.1108/ICS-03-2017-0014

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 $\beta=0.15$ to $\beta=0.64$). 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 results of this survey imply that productivity goals indeed hinder secure behavior in organizations. Therefore, we developed a concept to include information security goals into the goal setting process in organizations. To investigate this concept, we evaluated it in three small to medium-sized organizations (SMEs). The results indicate our concept is actionable in practice, when certain preconditions are met. In particular, the results of our study point out aspects which should receive special attention when implementing our concept in practice

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 survey hypotheses and the third section describes the survey. Section four then introduces our concept for security goal setting in organizations. Section five describes the study performed to evaluate the concept. Section six summarizes and concludes.

2. Theoretical background and hypotheses for the survey

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; Kohn, 1999).

As stated above, information security goals often compete with productivity 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. Study 1: Survey

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.

3.1. Research Methodology

3.1.1. Participants

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).

3.1.2. 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

Table 1 about here

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).

3.2. 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.

3.2.1. 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.

Table 2 about here

3.2.2. 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).

Table 3 about here

3.2.3. 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).

Table 4 about here

3.3. Discussion of the Survey Results

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).

3.3.1. 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.

3.3.2. Limitations

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.

4. Concept for Security Goal Setting in Organizations

From the findings of our survey it became apparent, that setting information security goals is required to mitigate the detrimental effects on security compliance of setting productivity goals. Therefore, we developed a concept for setting information security goals in the organizational context. To maximize the effectiveness of our concept, we base it on the prerequisites needed to reliably reproduce the positive effects of goal setting as defined by Locke and Latham (2002): (1) the required knowledge for task completion is conveyed, (2) a sufficient range of goal difficulty levels is offered, (3) sufficiently specific goals are set, (4) goal commitment is created, (5) the right type of goals (performance goals vs. learning goals) are set, (6) existing self-set goals are respected, (7) proximal goals are set, when the environment is characterized by uncertainty, (8) goal attainment is assessed using a matching measure, and (9) feedback about goal attainment is offered. In the following we will first describe the concept in general and then discuss fulfillment of the individual prerequisites.

4.1. General Working Principle

It is considered best practice for organizations to offer information security awareness materials to their employees (Wilson & Hash 2003). Especially web-based training is widely used, which is why we base our concept on this type of security awareness material. In order to give employees a direct opportunity to improve their information security-related behavior, well-designed security awareness materials must include behavioral recommendations. The basic idea of our concept is setting goals based on these behavioral recommendations. Thereby, each behavioral recommendation is used to formulate one or more goals of varying difficulty. Goals are pre-formulated by security experts to ensure they fully reflect the behavioral recommendations. All goals are formulated as performance goals to match the predominant formulation of productivity goals.

The actual goal-setting occurs after completion of the information security awareness material of one specific topic. The employee can then choose one or multiple of the goals formulated from the behavioral recommendations pertaining to that specific topic. The designer of the goals can freely choose how many goals can be set and the employee can freely choose the goal(s) s/he wants to set. To not unnecessarily influence the choice of goals (e.g. through the employee's perceived self-efficacy), there is no indication of the goal's difficulty while the employee chooses the goals s/he wants to set for her/himself.

Each goal is associated with a certain timeframe (usually weeks or months), in which the goal has to be achieved. After that timeframe, the employee is asked to return to the web-based training platform to indicate, whether the goal has been attained. In case the goal could not be attained, the employee has two choices: (a) s/he can prolong the timeframe to attain the goal, when s/he believes s/he can still attain the goal in the increased timeframe, or (b) s/he can set an alternative goal, e.g. because changes in the working environment made attaining the goal impossible.

This concept does not include extrinsic rewards, since these can easily carry unintended negative side-effects (cf. sections 2.6 & 3.3). In order to mitigate the negative effects associated with extrinsic motivation and rewards, the concept is built on the effects of intrinsic motivation (Ryan and Deci, 2000) instead. Additionally, to maximize the effectiveness of our concept, we explicitly consider all prerequisites identified by Locke and Latham (2002).

4.2. Addressing the Prerequisites

As described in section 2.6, Locke and Latham (2002) list nine prerequisites for the reliable reproduction of the positive effects of goal setting. In the following, we will discuss how our concept addresses each of these prerequisites.

4.2.1. Conveying the Required Knowledge

The goals are based directly on the behavioral recommendations included in the security awareness materials. Thus, the knowledge, required to successfully complete the tasks involved in attaining the goal, is conveyed in these materials. To ensure that this information is indeed present in the materials, only materials, whose effectiveness has been positively evaluated, should be used as basis for our concept.

4.2.2. Range of Goal Difficulty Levels

This prerequisite is fulfilled since, by design, goals of different difficulty levels should be derived from the behavioral recommendations. Thereby, the difficulty is not set by the required knowledge, since after consumption of the security awareness materials all required knowledge should have been conveyed effectively (cf. section 4.2.1). Instead the difficulty of the goals arises from the integration of the required tasks into the workflow of the employee (and how much additional work is involved in these tasks). Finding goals of varying difficulty is eventually up to the designer of the goals and therefore the range of difficulty among the goals should be verified with a variety of people before deploying the goals to employees. In order to decrease bias as much as possible (i.e. through the (mis)perception of the employee’s own self-efficacy), the goals are not explicitly labeled with their difficulty level during the actual goal selection.

4.2.3. Specific Goals

The goals are directly derived from the behavioral recommendations in the awareness materials. Therefore, the specificity of the goals is directly linked to the specificity of the behavioral recommendations. Consequently, only security awareness materials with specific behavioral recommendations should be used as basis for the proposed concept. In particular, we advise practitioners aiming to implement our concept in an organization to verify the specificity of the goals with laypeople beforehand.

4.2.4. Goal Commitment

Two aspects contribute to the goal commitment of an employee (Locke & Latham, 2002): (1) importance of attaining the goal, and (2) the perceived self-efficacy of the employee.

Regarding the importance of attaining the goal, it is beneficial to allow participation of the employee in the goal selection process. Since in our concept the goals cannot be freely set, but are chosen from a certain pre-defined set, it is important that the information security awareness materials include explanations regarding the reasoning behind each of the behavioral recommendations (Locke *et al.*, 1988). If the reasoning behind a certain goal is explained, setting the goal creates intrinsic interest and motivation regrading attainment of the goal (Haradkiewicz & Elliot, 1998).

Additionally, the employee’s perceived self-efficacy must be sufficiently high for her/him to believe the goals are attainable. Therefore, only security awareness materials effectively conveying the required knowledge should be used as basis for any implementation of our concept (cf. section 4.2.1).

4.2.5. Type of Goals

All goals are formulated as performance goals. The formulation as learning goals is no viable option, since the goal setting is implemented after the learning process using the information security awareness materials. This also aligns the goal type of the security goals with the traditional productivity goals of the employee (cf. section 2.6).

4.2.6. Respecting Self-set Goals

Respecting existing goals self-set by the employee, when offering information security goals for selection, can pose a challenge. Laws and regulations regarding data protection and informational self-determination can hinder capturing self-set goals. In larger organizations implementing such a system might require involvement of the employee representation, rendering the process potentially very time consuming. Therefore, we do not recommend a mandatory inclusion of goals self-set by the employee. An opt-in procedure can be used instead.

4.2.7. Proximal Goals in Case of Uncertainty

In cases where the behavioral recommendations are sufficiently complex to be divided into subtasks, the overall goal can be split up into suitable proximal goals. For each of these proximal goals, an individual timeframe (cf. section 4.1) should be defined and the employee asked about the goal attainment after each individual timeframe has expired.

To accommodate for uncertainty in the working environment, the employee can choose alternative goals, if completion of a goal became impossible due to changes in the working environment.

4.2.8. Matching Performance Measure and Goal

In principle, deriving the goals from behavioral recommendations allows measuring success in goal attainment by measuring whether the desired behavior is shown by the employee. However, measuring goal attainment in practice is difficult, since the goal related tasks are potentially performed in areas where observation of the employees is not easily possible. Additionally, the same limitations as for the collection of personal data for the inclusion of self-set goals apply (cf. section 4.2.6). Therefore, our concept relies on self-report of the employees.

4.2.9. Offering Feedback about Goal Attainment

Since the concept relies on self-report by the employees, feedback mechanisms cannot be implemented in a meaningful way. All information the system has on the attainment of the goals stems directly from the employee. However, the platform hosting the web-based training can send out reminders regarding the goals to employees.

5. Study 2: Concept Evaluation

We conducted a study to gauge the impressions of potential users and the practicability of our concept for setting information security goals in organizations. To this end, we derived goals from existing information security awareness materials and captured the impressions regarding our concept in a user study. In this section, we will first describe the creation of the goals used in the study, then the overall study design, and finally present the results.

5.1. Creation of the Goals used in the study

Our proposed concept requires the goals to be derived from behavioral recommendations of information security awareness materials. We chose an extended version of the NoPhish anti-phishing awareness and education materials (Stockhardt *et al.*, 2016) as basis for our goal derivation. They were a perfect fit, since they include clear behavioral recommendations and their effectiveness was proven in many settings (Canova *et al.*, 2014; Kunz *et al.*, 2016; Stockhardt *et al.*, 2016).

The extended NoPhish awareness and education materials included topics relating to the handling of fraudulent messages of different kinds. In particular, the participants received information about the following aspects: (1) how to check messages regarding their plausibility, (2) how to check whether links are potentially fraudulent, (3) how to check whether attachments potentially include malicious software, (4) what to do, if one is unsure regarding a message/link/attachment one received, and (5) what to do if one has come across a malicious message/link/attachment which was difficult to detect. All five aspects included in the materials specify behavioral recommendations. Overall, we created five goals, each relating to the behavioral recommendation of one of the aspects:

G-1. In the future, I will check all messages I receive regarding their plausibility.

G-2. In the future, I will check all links before clicking them.

G-3. In the future, I will check all files in messages I receive, before opening them.

G-4. In the future, I will report any potentially malicious messages to the IT department/the person responsible for the IT in my organization.

G-5. In the future, I will show malicious messages which are difficult to detect to my colleagues and explain why it is a malicious mail.

5.2. Study Design and Procedure

The study was conducted at three SMEs in Germany: one organization from the IT sector, one from the financial sector, and one from the travel sector. To comply with our university's requirements regarding research involving human participants, there was one contact person in each organization, who distributed and collected the materials for us. These contact persons were not involved in the analysis of the data.

Overall, 90 participants were recruited for our study, 30 from each of the three organizations. In particular, we asked our contacts in the organizations to distribute the materials to employees who do not mainly work in the field of information security. Each participant received the education materials electronically as a PDF file. Instructions to choose one of the five goals were added at the end of the materials.

After having read through the materials, the participants filled out a questionnaire. This questionnaire was comprised of two questions regarding the participants' demographics (age and gender) and two questions pertaining to the goal setting: (1) which of the goals G1-G5 the participants had chosen (it was possible to indicate no goal had been chosen), and (2) an open question to collect feedback from the participants.

5.3. Results

5.3.1. Participant Demographics

The responses from 87 of the 90 participants could be included in our analysis, since three participants returned empty questionnaires. All three participants returning empty questionnaires were from one organization. Of the responses, twenty-seven (31%) were from female participants. All participants were between 18 and 55 years old (M=33 years; SD=9.4 years).

5.3.2. Goal Selection

All goals were selected by at least one participant. However, the frequencies vary greatly (see Table 5). G2 ("*In the future, I will check all links before clicking them.*") was by far the most popular choice. It was chosen by 38 participants (43.7%). The second most frequently selected goal, G4 ("*In the future, I will report any potentially malicious messages to the IT department/the person responsible for the IT in my organization.*"), was selected by only half as many participants (19; 21.8%). G5 ("*In the future, I will show malicious messages which are difficult to detect to my colleagues and explain why it is a malicious mail.*") was selected by 14 participants (16.1%) and G3 ("*In the future, I will check all files in messages I receive, before opening them.*") by 9 participants (10.3%). The least popular goal was G1 ("*In the* *future, I will check all messages I receive regarding their plausibility.*"), which was selected by only 6 participants (6.9%). Only one participant indicated that she had not chosen any of the goals.

Table 5 about here

To investigate the influence of the participants' gender and the organizations they work for, we conducted further analyses using Fisher's Exact Test. Neither the gender of the participants (FET, p=0.526) nor the organization the participants work for (FET, p=0.051) have a significant influence on the selected goals at the α=0.05 level.

5.3.3. Collected Feedback

Using the second question in our questionnaire, we collected the participants' impressions and suggestions regarding our scheme. Overall, 36 participants gave feedback in this second question. Eight participants explicitly stated that they thought selecting goals as part of the information security training was a good idea, e.g. P59: "*I believe this is a good idea. I will try to attain my goal!*" In contrast, six participants questioned the usefulness of the goals, e.g. P66: "*I already try to [follow the behavioral recommendations] anyway.*"

The most frequently voiced feedback (12 participants) was that participants would have liked to select multiple goals, e.g. P24: "*It should be possible to set multiple goals instead of just one.*" Six participants would have liked to set completely individual goals instead of selecting one from the five goals given, e.g. P80: "*It would be great, if it was possible to set my own goals!*". One additional participant wished for a greater selection of goals, P23: "*Please give more options, so one has more freedom in choosing the goal.*"

5.4. Discussion of the Concept Evaluation

The vast majority of participants (86 of 87) chose a goal after reading the information security education materials. Only one participant chose none of the goals. Unfortunately, this participant did not provide feedback using the second question of our questionnaire. However, other participants stated that they would have preferred the possibility to formulate their own goals. We argue that this might be a way to not only mitigate this issue, but also give participants, who stated to already conform to all behavioral recommendations, an option to select a goal as well.

From the predefined goals, some were much more frequently chosen than others. G2 ("*In the future, I will check all links before clicking them.*") proved to be a popular goal. The reason might be that checking links is the original core element of the NoPhish education materials and consequently the most information is provided with regard to this goal. The other two goals relating to checking content of received messages, G1 (plausibility) and G3 (attached files), were much less popular. For G1 it seemed that participants felt that they would not need to set this goal explicitly, since they were doing it anyways, e.g. P64: "*Most employees will check emails regarding their plausibility anyways. Who would ever click on a link saying 'You have won 1000000 Euros'?*" While none of the participants' comments contained any information regarding the low frequency for G3, we argue that the opposite effect might be the cause. For laypeople, it might be difficult to identify file types which can potentially contain malicious software, since they handle many of these files on a daily basis (e.g. MS Office documents with malicious code embedded in macros). This underlines the importance of conveying the necessary knowledge in the information security education materials. Proximal goals might potentially have improved the frequency of selection for G3.

Neither the gender of the participants nor the organization the participants work for had a significant influence on the selected goals. However, the influence of the organization the participants work for missed the $\alpha=0.05$ level very closely. Therefore, larger samples might lead to significant results. The difference seems to stem mainly from the participants from O1 (IT sector) choosing G1 more frequently and G4 less frequently than the participants from the other two organizations. Further studies are needed to investigate this effect in detail.

5.4.1. Practical Implications

Considering the results of our study, two aspects should be paid particular attention to, when implementing our concept in practice. Firstly, goals become more attractive, when the education materials they are based on include relevant actionable behavioral recommendations. Secondly, the concept should include both, (1) the possibility to choose completely own goals in addition to the ones derived from the behavioral recommendations and (2) the possibility to choose multiple goals.

5.4.2. Limitations

Unfortunately, we could not conduct a follow-up study to check whether participants actually attained their goals. We acknowledge this as limitation of our study. Since the goal of this study was to gauge the general idea behind our concept this was acceptable, but future studies should include this in their methodology. Furthermore, like our first study, this study relies on self-reported data.

6. Conclusion

In this work, we presented our findings regarding the effects of goal setting in organizations. The findings of our survey regarding the implications of conflicting goals are twofold. Firstly, it provides additional evidence for the relationships between the constructs of the theory of planned behavior. Secondly, it revealed that the presence of rewards for performance goal achievement is strongly associated with a decrease in security compliance and thereby provides evidence supporting the assumption of conflicting goals in the workplace.

To mitigate this conflict between productivity and information security goals, we presented a concept for goal setting in organizations and evaluated it in a user study with participants from three SMEs. Our results indicate that this concept can be implemented in practice using available information security awareness materials such as the NoPhish anti-phishing training. Any practical implementation should thereby pay special attention to the aspects identified in our study to maximize its effectiveness. Firstly, the information security awareness materials used as basis must contain relevant actionable behavioral recommendations. Secondly, participants should not only have the possibility to select multiple goals, but also to define their own goals.

Further studies are needed as experimental investigation of actual security compliance and the causal effects of goal setting on security behavior. In particular, study designs should include measuring the goal attainment. Future studies should also consider the actual content of the information security policies employees are referring to, employee's knowledge of these security policies and the security related knowledge the employees possess. As the recent trend in securing an organization's information assets goes to risk assessment instead of compliance, future research should also consider the current organizational practices concerning information security and how to best set goals in this changing environment.

7. Acknowledgements

The research reported in this paper has been supported in part by the German Federal Ministry of Education and Research (BMBF) within CRISP (www.crisp-da.de/). Furthermore, this work has been developed within the project `KMU AWARE' which is funded by the German Federal Ministry for Economic Affairs and Energy under grant no. BMWi-VIA5-090168623-01-1/2015. The authors assume responsibility for the content.

8. References

Ajzen, I. (1991), “The theory of planned behavior“, *Organizational Behavior and Human Decision Processes*, Vol. 50, No. 2, pp. 179-211.

Bandura, A. (1982), “Self-efficacy mechanism in human agency“, *American Psychologist*, Vol. 37, pp. 122-147.

Canova, C., Volkamer, M., Bergmann, C. and Borza, R. (2014), “NoPhish: An Anti-Phishing Education App”, in Mauw, S. and Jensen, C.D. (Ed.) *Security and Trust Management. STM 2014. Lecture Notes in Computer Science*, Vol. 8743, Springer, Cham

Gilliland, S. W. and Landis, R. S. (1992), “Quality and quantity goals in a complex decision task: Strategies and outcomes“, *Journal of Applied Psychology*, Vol. 77, No. 5, pp. 672– 681.

Haradkiewicz, J.M. and Elliot, A.J. (1998), “The Joint Effects of Target and Purpose Goals on Intrinsic Motivation: A Mediational Analysis”, *Personality and Social Psychology Bulletin*, Vol. 24, No. 7, pp. 675–689.

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, pp. 615-659.

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, pp. 83-95.

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

Kohn, A. (1999), *Punished by rewards: The trouble with gold stars, incentive plans, A's, praise, and other bribes*, Houghton Mifflin, Boston.

Kunz, A., Volkamer, M., Stockhardt, S. and Palberg, S. (2016), “NoPhish: Evaluation of a web application that teaches people being aware of phishing attacks”, in Mayr, H.C. and Pinzger, M. (Ed.) *INFORMATIK 2016, Lecture Notes in Informatics (LNI),* 509-518.

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, pp. 133-146.

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

Locke, E. A., Alavi, M., and Wagner, J. (1997), “Participation in decision- making: An information exchange perspective”,. in Ferris, G. (Ed.), *Research in personnel and human resources management*, Vol. 15, pp. 293–331.

Latham, G. P., Erez, M. and Locke, E. (1988), “Resolving scientific disputes by the joint design of crucial experiments by the antagonists: Application to the Erez–Latham dispute regarding participation in goal setting”, *Journal of Applied Psychology*, Vol. 73, pp. 753–772.

Locke, E.A. and Latham, G.P. (2002), “Building a practically useful theory of goal setting and task motivation: A 35-year odyssey”, *American Psychologist*, Vol. 57, No. 9, pp. 705–717.

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, pp. 152-156.

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)*, pp. 156-156b.

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, pp. 22-34.

Ryan, R. M.and Deci, E. L. (2000), "Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being", *American Psychologis, Vol.* ***55, No.*** *1, pp. 68–78.*

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, pp. 93-106.

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. (Ed.) *Security and Privacy Protection in Information Processing Systems*, Springer, Berlin, Heidelberg.

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, pp. 42-75.

Stockhardt, T., Reinheimer, B., Volkamer, M., Mayer, P., Kunz, A. and Lehmann, D. (2016), "Teaching Phishing-Security: Which Way is Best?", *31st International Conference on ICT Systems Security and Privacy Protection - IFIP SEC 2016*, pp. 135-149

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, pp. 1228-1240.

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, pp. 79-89.

Wilson, M. and Hash, J. (2003). "Building an Information Technology Security Awareness and Training Program", *National Institute of Standards and Technology*, available at: http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf (accessed 15 March 2015).

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, pp. 993-1020.

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 6: Sources of measurement items

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 7: Regression model for intention to comply with security policies

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 8: Regression model for perceived top management participation

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	.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 9: Regression model for actual compliance with security policies

Goal	O1 (IT)	O2 (travel)	O3 (financial)	Male	Female	Overal
G1	6	0	0	4	2	6
G2	10	12	16	29	9	38
G3	4	3	2	5	4	9
G4	3	8	8	13	6	19
G5	4	6	4	9	5	14
NG	0	1	0	0	1	1

Table 10: The frequencies for each goal. G1 - G5 signify the selection of a goal described in section 5.1, NG signifies that no goal was selected. O1 – O3 signify the three organizations.