Is Social Learning Always Helpful? Using Quantile Regression to Examine the Impact of Social Learning on Information Security Policy Compliance Behavior.

Sebastian Hengstler
University of Goettingen, Germany
s.hengstler@stud.uni-goettingen.de

Stephan Kuehnel
Martin Luther University Halle-Wittenberg, Germany
stephan.kuehnel@wiwi.uni-halle.de

Simon Trang
University of Goettingen, Germany
simon.trang@uni-goettingen.de

Abstract

Social learning theory has attracted increasing attention in recent years in terms of its use to study information security policy non-compliance behavior. But previous results of studies in the field of information security have been rather heterogeneous. various influencing factors have been considered within the framework of social learning theory. Previous studies quantitatively assess the effectiveness of social learning by relying on mean-based regression methods. In contrast, we intend to apply quantile regression to provide a new perspective on the subject. Therefore, we estimate the overall impact of social learning interventions and uncover how their impact differs among employees with different propensities (quantiles) for information security policy compliance behavior—an important finding for determining safety interventions for specific employee groups. Based on data collected in Germany, our results show significantly different effects in the analyzed quantile aspects of imitations and differential reinforcement.

Keywords: Social Learning Theory, Information Security Policy Compliance Behavior, Information Security

1. Introduction

In recent years, information security has been an object of study considered relevant in the field of information systems (Cram et al., 2019; Whitman & Mattord, 2012). When the topic of information security first became significant, it was considered mainly as the technical protection of information systems, with the belief that those systems could be secured if only sufficient resources were invested (Bulgurcu et al., 2010; Solms, 2000). However, one of these resources itself bears a large part of the risks, namely employees who, for example, do not adhere to the information security policy (ISP) defined by the company (Höne & Eloff, 2002; Siponen et al., 2014). This is where research on compliance behavior in ISP addresses and considers a wide range of used theories from different fields (Sommestad et al., 2014).

Among these, the social learning theory (SLT) has become popular as a new theoretical angle to examine the role of social learning in organizations for achieving ISP compliance behavior (ISPCB) (Hengstler et al., 2021; Hengstler et al., 2022; Johnston et al., 2010; Warkentin et al., 2011; Yoo et al., 2020). The SLT describes how an individual's behavior is influenced by their social environment through imitation, differential associations, and reinforcements (Akers, 2002).

Despite other popular theories to explain ISPCB, the SLT does not focus on individual (rational) decisions but refers to the social impact a group has on behavior. However, the initial learning of a certain behavior often is influenced by the social group a person is part of and continues to influence their behavior beyond the learning phase. The role of social learning in ISPCB research is supported by recent findings that highlight the importance of group learning aspects in the context of information security (Hengstler et al., 2021; Hengstler et al., 2022; Niechoy et al., 2021). However, the effectiveness of social learning on ISPCB has not yet been studied widely enough to make general assumptions about its effective use in the information security domain (Hengstler et al., 2022; Tu et al., 2015).

Relating to this general issue in research, Robey and Boudreau (1996) emphasize that such assumptions, inconsistencies, and open issues in the literature can be addressed by applying three main strategies: 1) including additional contingency variables, 2) reviewing the research questions, and 3) evaluating the utilized research methods. Existing studies about the SLT have been examined from different perspectives. It is discussed whether differences can be triggered by various influencing

URI: https://hdl.handle.net/10125/103139
978-0-9981331-5-7

factors, such as cultural dissimilarities, contextual specificities, or other underlying behavioral intentions (Hengstler et al., 2021). However, apart from the contextual, theoretical, and methodological issues discussed in the literature to enhance the understanding of inconsistencies in findings, studies that quantitatively assess the effectiveness of social learning have predominantly relied on methods that analyze the underlying data using mean-based regression approaches (Trang & Brendel, 2019). Mean-based regression approaches suggest that the marginal effect of the independent variable is equally large at all levels of the dependent variable (i.e., propensities of security behavior) (Trang et al., 2020; Yu et al. 2003). We challenge this assumption and suggest that the impact of social learning constructs on ISPCB is not uniform across the individuals' behavioral propensities. Learning from behavioral studies in fields such as D'Arcy and Herath (2011) and Trang and Brendel (2019), we believe it is also reasonable to assume that social learning mechanisms work differently at different levels of security behavior propensities. We believe that a different quantitative analysis approach, i.e., quantile regression, can help to shed light on such empirical inconsistencies. Quantile regression allows researchers quantify the effect between social learning mechanisms and ISPCB in different quantiles. The advantage of this approach is that it can produce more accurate results, as it is applicable to data from any distribution, and, unlike the commonly used linear regression method, quantile regression minimizes the sum of the absolute values of the prediction error (Yu et al., 2003). It also allows researchers identify potential clusters of individuals that have different behavioral tendencies. Thus, it allows us to enhance our understanding under which conditions social learning may be more effective in the context of ISPCB (Trang et al., 2020).

For this reason, we develop a theoretical model based on the SLT. Building on a quantitative study with 256 participants, we first determine the influence of social learning mechanisms on ISPCB using a popular context for an ISP threat, namely missing logoff cases. Then, using the heterogeneous responses of the participants in our study, we use quantile regression to uncover the effect of social learning mechanisms on ISPCB in three categories of employees: employees who tend to behave in an ISP non-compliant manner, employees with average compliance behavior, and employees who tend to behave in a rather strict ISP compliant manner (Ahmad et al. 2016).

From a research perspective, our results have implications for the usage of SLT in information security research. Our primary contribution is empirical in nature (Agarfalk et al. 2017), i.e., with our quantile regression approach, we empirically identify boundary conditions for the applicability of social learning measures. More specifically, we reveal that the effect of imitations and differential reinforcement, as part of social learning, differ across our defined quantiles. Moreover, our results show that ISPCB is a complex problem in which SLT-based information security measures should be distinguished not only by security threats or other security-related contexts but also based on different behavioral principles of employees. The practical implication of our results is that social learning-related information security measures (such as group-based training, e.g., escape rooms or group-based learning games) could work differently in different groups of employees. For example, imitation should only be part of measures for employees who tend to be non-compliant, as this concept does not show any significant effect on ISPCB in the employee groups with average and rather strict compliant behavior. The same occurs for measures based on differential reinforcement concepts.

The rest of the paper is structured as follows. Based on our research approach, we first review the SLT and its usage in information security research. We then derive our statistical model for the quantile regression approach and describe the data gathering and data analysis context. The paper continues with the presentation and discussion of the results, followed by implications for theory and practice. Finally, we offer some conclusions.

2. Reviewing social learning theory

The SLT was first introduced by Bandura in 1977 and explained human behavior by focusing on the social relationship with others (Bandura, 1977). The theory was developed to explain the action of criminals and thereby allows the development of new approaches to stop deviant behavior (Sutherland, 1972). Therefore, it describes the cognitive process of humans to acquire, maintain, and change behavior as a result of their social interactions and environment (Akers & Sellers, 2011). This continuous learning process operates to motivate or inhibit conforming behavior and is composed of the following four major psychological mechanisms (Akers, 2002).

Differential association (DA) refers to behavior learned from others by identifying and interacting with them (Sutherland, 1972). Therefore, it includes a normative and a behavioral dimension, which is shaped by the group of people with whom the association occurs (Akers & Sellers, 2011). Hence, learned definitions (DE) or values, attitudes, and norms, which one attaches to a given behavior, influence one's conduct and thereby may abet non-conforming behavior (Pratt et al., 2010). The initial learning process, however, is often linked with the imitation (IM) of others (Bandura, 1977) and the modeling of their behavior after first associating with them and later observing a certain behavior (Lembcke et al., 2019). Furthermore, social learning includes a differential reinforcement mechanism (DR), which refers to anticipated or actual rewards and punishments that are consequences of a certain behavior (Burgess & Akers, 1966). These reinforcement mechanisms manifest themselves in a social form, for instance, when a specific behavior gives one a higher status in a peer group, and/or in a material form, for example, when an action leads to a fine.

SLT has been used multiple times in computer crime (Skinner & Fream, 1997) and various other domains, as a meta-analysis by Pratt et al. (2010) has shown. It has been used to explain human behavior in information systems and information security research (Lippert & Forman, 2005; Hill et al., 2009). Warkentin et al. (2011) examined the antecedents of compliance self-efficacy to highlight the influence of informal social learning environments. Yoo et al. (2020) used the concept of collective workgroup information security effectiveness to emphasize the importance of co-worker influence. Other studies, including Ifinedo (2014), Wiafe et al. (2020), and Ahmad et al. (2019), use the social norms aspect (Definitions) from SLT and Johnston et al. (2010) the IM aspect. Recently, Hengstler et al. (2021) have shown that social learning has a significant influence on ISPCB.

All reviewed papers have in common that they rely on a mean-based analyzing approach (mostly structural equation models) and, thus, do not consider different compliance levels. In contrast, Shropshire et al. (2015) describe that there is a spectrum of different compliance levels, which are linked to personality. Ahmad et al. (2016) proposed a typology of employees' information security behavior that differentiates between groups. This study builds upon this argument of having different compliance levels or groups of behavioral tendencies related to ISPCB and analyses different quantiles of ISPCB and their relation to SLT to account for different levels of compliance behavior.

3. Research design

3.1 Research model, data collection, pre-test, and descriptive statistics

The study was conducted online in Germany because most studies on ISP compliance behavior and social learning have been conducted in Germany (Hengstler et al., 2021; Hengstler et al., 2022; Lembcke et al., 2019) . Thus, we set a stage for better comparability with our results because the difference in cultural factors of influence within one country appears to be less significant (Moody et al., 2018).

The questionnaire is constructed as an experimental vignette study, which means that the participants are presented with a hypothetical situation (scenario) and afterward answer questions about their feelings and how they would behave in the given situation (Atzmüller & Steiner, 2010). This study uses a popular scenario about information security logoff situations, adapted from Moody et al. (2018), and describes the misconduct of an employee of a fictitious company who does not comply with the security policy for a certain reason.

The scenario describes a popular issue with a log-out policy most companies implement. Employees who leave their workplace must log out of their personal accounts to prevent unauthorized access by third parties or colleagues. In the given scenario, the main character is a recently hired middle manager in a medium-sized company. The division uses an inventory application program for purchases, and the responsible employee in the scenario assumes that it is more time-saving if all purchases are made through their account than if each employee has to log in and log out again. The scenarios are designed to be simple and relevant so that one can understand them and may have experienced the situation before. Also, it is made clear to the participants that the action performed violates the ISP. This is important to ensure the content validity of the measurement instrument (Siponen & Vance, 2014).

Since this study focuses on ISPCB, it is essential to ensure that participants use a computer at work and have at least some knowledge of their organization's ISP. Therefore, control questions about computer use and ISP awareness were included. After confirming that the participants fulfill the criteria of our target group the scenario is shown for at least ten seconds to ensure that it is read appropriately. Subsequently, the questions related to the described SLT and ISPCB constructs are shown. The items were adapted from Hengstler et al. (2021) and adapted to our context (see appendix). Moreover, the name of the described person in the scenario is adjusted to match the gender of the participant. Male participants are presented with a scenario where the acting person is named Felix, and for all other participants, the name of the acting person is Anna. This ensures optimal association with the person, as research has shown that humans can better identify themselves with the same gender (Nangle et al., 2004).

A seven-point Likert scale from strongly disagree to strongly agree was used to assess the answers. Additionally, an attention check question was used, where participants were instructed to give a certain answer to improve the data quality of the online study (Curran & Hauser, 2019; Peer et al., 2014).

Due to the sensitive subject of the study, all participants remained anonymous and only answered the demographic questions discussed before. Before the actual experiment started, a pre-test with ten persons was conducted to ensure the correctness of the questionnaire and the data collection process. No item with a lower factor loading than .65 has been detected (Trang et al., 2020). All constructs reported a high Cronbach's Alpha (>.8). In addition, a common method bias test, according to Harman's One-Factor-Test, was performed to detect potential common method variance in the study (Hair et al., 2019). The unrotated solution shows how many factors are needed to capture the variance in the variables and the basic assumption of this test is that common method variance is present when only a single factor explains a large part of the covariance between the variables (Podsakoff et al., 2003). The total variance extracted by one factor does not exceed .50 (.26), which indicates no evidence for common method variance in the study. Therefore, we conclude that the measurement instruments are valid and reliable. The used items, including their factor loadings, are listed in table 1. No items were removed, because they were no less than 0,7 (rounded up for DR_1) (Hair et al., 2019).

Table 1: Construct validities.

Construct	Item	Factor Loading	CA	CR	AVE
Differential Reinforcement (DR)	DR_1	.671	.845	.888	.728
	DR_2	.969			
	DR_3	.781			
Imitations (IM)	IM_1	.955	.976	.971	.917
	IM_2	.967			
	IM_3	.976			
Differential Association (DA)	DA_1	.959	.964	.952	.869
	DA_2	.947			
	DA_3	.939			
Definitions (DE)	DE_1	.817	.853	.871	.771
	DE_2	.717			
	DE_3	.907			
Information Security Policy Compliance Behavior (ISPCB)	CB_1	.923	.91	.918	.788
	CB_2	.829			
	CB_3	.887			

In total, 256 participants completed the survey across the two different scenarios. After applying our quality criteria, the attention check question, and a fully completed survey, 206 valid answers remained. According to Hair et al. (2010) our sample size fulfills the criteria for a solid sample size (. The age of the participants is concentrated in the range of 20 to 30 years, with an average age of 30 years. An equal distribution of 48.9% female participants is also given. The participants mainly have an academic background: 50.1% had a bachelor's degree, 28.3% had a master's degree or diploma, and an additional 1.7% had a doctoral degree. 14.5% indicated their highest level of education was high school graduation. Most participants worked in an organization with less than 500 employees (36.8%), 72.6% of the participants worked in an organization with up to 5000 employees, and 13.6% worked for an organization with more than 10000 employees. The descriptive statistics are summarized in table 2 (The values in brackets are the nominal occurrences within the sample).

Table 2: Descriptive Statistics.

Gender	Age	Education	Company Size
Male (106)	<20 (2)	Less than high school (1)	Less than 500 (81)
Female (101)	20-29 (128)	Secondary School (0)	500 – 999 (17)
	30-39 (47)	High School (4)	1,000-4,999 (57)
	40-49 (16)	College or Further Education (24)	5,000 - 10,000 (27)
	50-59 (10)	Bachelors degree (13)	More than 10000 (25)
	>60 (4)	Masters degree (108)	
		Doctoral degree (57)	

3.2 Data validation

We used a quantile regression approach to test our models because in combination with an ordinary least square (OLS) regression to analyze the regression line for the mean and for determined quantiles (Li, 2015; Yu et al., 2003). This allows us to examine whether social learning mechanisms affect ISPCB in different quantiles of our data. We defined a potential grouping of employees for our quantiles (.25 - tending to be non-compliant; .5 - average compliant, .75 – tending to be compliant) based on general assumptions in the typology from Ahmad et al. (2016). We used the software IBM SPSS 25 to perform our analysis. As a first step, we evaluated the validity and reliability of the instruments of our sample. After that, we analyzed our data in light of our research approach. Common quality criteria for reflective measurement models in information security research were applied to our study and are listed in table 3 (Lowry et al., 2016) (the bold numbers are the square root of the AVE). To validate our data quality, we used typical quality criteria for quantile regressions (Li, 2016; Trang et al., 2020). We used individual item reliability, composite reliability, average variance extracted and Cronbach's alpha as indicators of convergent validity for our model (see table 1) (Hair et al., 2010). Additionally, the cross-loadings show that all items have higher loadings on their assigned construct than on the other constructs in each model (Chin, 2001). In summary, our results indicate that our measurement model is acceptable and reliable.

Table 3: Data validity.

Construct	Mean (Std. Dev)	DR	DA	IM	DE	ISPCB
DR	4.319 (1.521)	**.853**				
DA	4.129 (1.64)	.077	**.932**			
IM	3.388 (1.908)	.238	.685	**.957**		
DE	5.181 (1.372)	.356	-.236	-.328	**.878**	
ISPCB	5.743 (.9302)	.267	-.247	-.360	.604	**.887**

4. Results

4.1 Model specification

To determine possible specifications for the use of the SLT in information security measures, we analyzed our data in two sequential steps. In the first step, we performed an OLS regression to obtain insights into changes in the mean of the mechanisms analyzed. We specified a regression equation (1) that includes the variables of the SLT and control variables for demographic variables on age and gender:

ISPCB$_i$ = ß$_0$
+ ß$_1$ Differential reinforcement$_i$
+ ß$_2$ Imitation$_i$
+ ß$_3$ Differential association$_i$
+ ß$_4$ Definition$_i$
+ ß$_5$ Computer use$_i$
+ ß$_6$ Company size$_i$
+ ß$_7$ Gender$_i$
+ ß$_8$ Age$_i$
+ ß$_9$ Education$_i$ + e$_i$

The OLS regression results show a multimodal distribution of our data based on our 7-point Likert scales. Assuming the findings of previous research that SLT mechanisms are context-dependent and that effectiveness may differ contextually and based on an individual's behavioral intentions, we can also statistically expect different peaks in the collected data and suggest the existence of different groups within them. These differences correspond well with our assumption of different behaviors toward ISP across an organization. They reinforce our motivation to run quantile regressions to investigate whether the mechanisms of SLT have differential effects on ISPCB across the distribution

Quantile regression is a type of regression that is widely used in quantitative modeling. It is an extension of the standard linear regression that estimates the conditional mean of the outcome variable (Yu et al., 2003). It can be used, among other things, when the assumptions of linear regression are not met or when quantiles other than the mean (as in linear regression) are to be analyzed, as represented in our example by different groups of employee behaviors. This allows quantile regression to be used to better understand relationships between variables outside the mean of the data (Trang et al., 2020). Accordingly, it is primarily used to understand outcomes that are not normally distributed and have non-linear relationships with predictor variables. In addition, quantile regression allows us to drop the assumption that variables act the same in the upper or lower parts of the distribution as they do at the mean and to identify the factors that are important determinants of the variables. We, therefore, rely on the following specification of our quantile regression equation (2), where the quantiles are indexed by θ:

Quantθ[ISPCB$_i$] = $\gamma_{0;\theta}$
+ $\gamma_{1;\theta}$ Differential reinforcement$_i$
+ $\gamma_{2;\theta}$ Imitation$_i$
+ $\gamma_{3;\theta}$ Differential association$_i$
+ $\gamma_{4;\theta}$ Definition$_i$
+ $\gamma_{5;\theta}$ Computer use$_i$
+ $\gamma_{6;\theta}$ Company size$_i$
+ $\gamma_{7;\theta}$ Gender$_i$
+ $\gamma_{8;\theta}$ Age$_i$
+ $\gamma_{9;\theta}$ Education$_i$ + e$_i$+ e $_{i,\theta}$.

4.2 Model estimation

To uncover the differential effects of sanctions on ISPCB, we tested whether our equation (2) had differential effects for the .25, .50, and .75 quantiles. The results of our quantile regression are shown in table 4 (see columns 3-5).

Based on our equation given in (1) and its specification, we first estimated an OLS regression to examine the effect of SLT mechanisms on the conditional mean of ISPCB (see table 4). The OLS regressions shows that IM has a negative influence (β2 = -.105, p < .01), while DE (β4 = .278, p < .001) has a positive and significant influence on ISPCB. For the control variables only computer use (β7 = .184, p < .05) has a small positive influence on ISPCB. The rest of the control variables are insignificant and show no strong effect. The adjusted R² for the regression is .525.

DR and IM are only significant in the .25 quantile with low effect sizes of γ1,.25 = .057* and γ2,.25 = -.061 . The difference between DR and IM is significant for the .25 quantile and not significant for the .50 and .75 quantiles (Δ(γ1;.25 – γ2;.25) = .118, p < .05; Δ(γ1;.50 – γ2;.50) = .091, ns; Δ(γ1;.75 – γ2;.75) = .052, ns). Interestingly, the positive effect of DE is significant for all three quantiles with decreasing effect towards the third quantile. Additionally, DE was tested to be significantly different across all three quantiles (F(2.616) = 6.20, p < .01). The bold numbers in table 4 highlight the significant effects.

Table 4: Results of the Quantile Regression (*p < .05, **p < .01, ***p < .001).

Variables	OLS (Std. Error)	Quantile Regression		
		.25	.50	.75
(Intercept)	2.336*** (.568)	.955* (.419)	1.976* ** (.582)	2.434*** (.696)
DR	.039 (.037)	.057* (.027)	.021 (.038)	.010 (.045)
IM	-.105** (.038)	-.061* (.028)	-.070 (.039)	-.042 (.046)
DA	-.013 (.039)	-.026 (.029)	-.013 (.040)	-.044 (.047)
DE	.278*** (.042)	.406*** (.031)	.244** * (.043)	.159* (.051)
Computer use	.184* (.087)	.161* (.064)	.209* (.089)	.309* (.107)
Company size	.019 (.034)	.000 (.025)	.027 (.035)	-.038 (.042)
Female	.007 (.093)	-.025 (.069)	-.055 (.096)	-.184 (.114)
Age	-.008 (.005)	-.003 (.004)	-.077 (.005)	-.004 (.006)
Education	-.014 (.046)	.002 (.034)	.022 (.047)	.093 (.056)
Adj. R² / Pseudo-R²	.525	.419	.323	.302

5. Discussion

This study aimed to explore the extent to which the SLT mechanisms have a different effect on distinct quantiles within an analyzed data set. In our analysis, we look at both the differences in results between our OLS and our quantile regression and the comparison with previous research findings.

Taking a deeper look into the quantiles, we can identify significant differences between the three levels of ISPCB. However, unexpectedly, the lowest quantile does not show non-complying behavior, but more so, is not always willing to comply. Therefore, we suggest different names for the quantiles: (.25) tending to be non-compliant, (.50) average compliant, and (.75) tending to be compliant behavior. For the low compliance behavior group, the SLT can be applied. IM (γ2;.25 = -.061*) has a small negative impact on this group, while DE (γ4;.25 = .406***) is the strongest mechanism concerning ISPCB. Additionally, DR (γ1;.25 = .057*) has a small positive influence on this group. For the moderate and high compliance behavior groups, DE is the only mechanism from social learning that shows a positive effect.

5.1 Research implications

Our results indicate the importance of social learning in the field of information security research and ISPCB. First, the strong positive influence of definitions for the ISPCB that has been identified by the research of Hengstler et al. (2021) and Hengstler et al. (2022) can be further supported. The authors reported an effect size of .298, which is close to our results in both scenarios. Unfortunately, the research of Lembcke et al. (2019) does not evaluate the influence of definitions in their work. Thus, another comparative value is missing, which could have further supported this effect.

Our study has implications for information security research in several ways. First, we theorize that social learning affects different behavioral groups of employees and positively influences compliance behavior with ISPs. We show how the effectiveness of SLT mechanisms differs along different ISPCB tendencies. The goal of such a distinction is to target ISPCB within the organization. We propose that an appropriate set of specifications is likely to increase ISPCB. By drawing attention to the specifics of how social learning aspects differ in effectiveness across behavioral groups, our study lays the groundwork for future research to more purposefully design mechanisms to ensure information security in the future. Our results suggest that it is worth having a glimpse beyond the mean when evaluating the effectiveness of security interventions. We find that social learning mechanisms have a more complex function for the individual depending on their inclination, especially for the social learning constructs of imitation and differential reinforcement.

Second, our chosen grouping of employees based on behavioral inclinations toward compliance in their organization is a well-useful division for examining the effectiveness of different theoretical mechanisms necessary for designing targeted ISPs. Our findings demonstrate that IM and DR have different effects on ISPCB. This implies that focusing solely on differences in effectiveness due to contextual diversity (e.g., different security threats or cultural differences) might not be enough as a contextual condition to precisely narrow down the boundary conditions for the usage of SLT in information security research. Thus, we provide the argumentation for the proposition that ISPCB is a complex problem, where a solution does not lie in purely differentiating security threats or cultural differences, but attention must be paid to different employee behavioral principles. The quantile regression approach we used shows a possible way to further research this problem. Previous interventions that were only mean-based measured could also be considered different in our approach and give different insights into the usage of the SLT constructs to influence ISPCB positively. The next step for research in this area would be to define the underlying conditions for our different analyzed groups of ISPCB tendencies in order to be able to address inconsistencies more precisely.

5.2 Practical implications

Practical implications can be derived from the results of our work. The negative influence of imitation on the low compliance behavior group suggests that the actions of social leaders in a team have a great impact. Encouraging them to adopt positive compliance behavior can help the low-level compliance group (.25 quantile) imitate this behavior and this, in turn, leads to better compliance behavior.

Our findings have important implications for information security professionals and managers responsible for developing and implementing information security measures. First, it is important to note that there cannot be only one generally applicable solution for using SLT constructs as an information security measure. One general measure for different groups of people or security contexts is rather unlikely to be effective due to the diverse effects of social learning in terms of information security compliance (Hengstler et al. 2021). To find a promising mix of social learning elements, security experts first need to identify the different target groups in their organization (e.g., through different awareness campaigns or tools, such as phishing). In general, our results can be used by information security experts to tailor security measures more specifically to the groups of employees we have analyzed in our quantiles. First, our results state that individuals, who tend to be less compliant with their organization's ISP (.25 quantile), are more responsive to the DR an IM elements. If an organization has to deal with many employees who tend to be non-compliant, it is advisable to take advantage of information security measures, given the impact of those social learning elements. Second, for employees who tend to average compliance behavior (.50 quantile) or compliant behavior (.75), the use of DE of is recommended. Thirdly, for all groups of employees' ISP compliance behavior tendencies, IM and DE are usable. Security professionals should consider the benefits of those elements when designing security measures for all groups of employees in the sense that they should emphasize the likelihood of social learning when conducting security training. Furthermore, we suggest to use the quantile regression approach for other established theories in information security compliance behavior research. Applying this methodology for deterrence theory, for example, could create new insights about the effect of sanctions on compliance behavior, especially because research in this area shows heterogeneous results (Trang & Brendel, 2019).

5.3 Limitations

First of all, this study collects data using a self-reporting questionnaire. Even though this approach is well established in information security research (Moody et al., 2018), we may not be able to measure the actual compliance behavior. Instead, we measure the theoretical willingness or intention to comply, which may not be the same. Moreover, the participant may interpret the questions differently in light of their past experiences and may think that their behaviors are secure when in reality, it is not. The recruited participants work for numerous organizations, each with its own policies and organizational structure. Future research should conduct similar research in a few selected companies only to get a more specific picture (Siponen & Vance, 2014). This can help develop more practically relevant recommendations depending on the organization's structure and social learning environments (Crossler et al., 2009).

This study tries to mitigate the problem of different participant backgrounds by using a realistic and relevant scenario-based questionnaire, which includes making the participant aware of the ISP violation as recommended by Siponen and Vance (2014). However, social learning is a complex process, which we may not be able to capture fully in this study. Even though the reported model fit is relatively high compared to other studies in the same research area, other external factors, such as personal attributes and experiences, may be able to distort the collected data (Vroom & Solms, 2004).

Willison and Warkentin (2013) classified human information security threats as passive non-volitional non-compliance (e.g., accidental data leakage), volitional (but not malicious) non-compliance, or intentional malicious computer abuse. Our used scenario in this study can be characterized as volitional noncompliance; nonetheless, the two other cases are also very much relevant in today's organizations. Therefore, further research needs to be conducted to investigate these different cases (D'Arcy et al., 2009). Especially studying intentional malicious behavior considering SLT, where social factors may be even more important (Dang, 2014; Liang et al., 2016), could lead to a more general understanding of human information security.

6. Conclusion

This study is the first one in this research field to use a quantile regression approach to explain ISPCB, and we want to encourage researchers to consider quantile regression and the SLT when analyzing compliance behavior in future studies. We first determined the general influence of social learning mechanisms on ISP compliance behavior and then used the heterogeneous responses of the participants to perform a quantile regression. We uncovered the effect of social learning mechanisms on ISPCB in three different quantiles (.25, .50, and .75 quantiles) and proposed categories of employees: employees, who tend to behave in an ISP non-compliant manner, employees with an average behavioral intention, and employees, who tend to behave in a more strict ISP compliant manner. We expand the current knowledge of IS security in practical and theoretical ways and contribute to a better understanding of ISPCB by differencing between three compliance behavior levels. Firstly, we introduce the notion of different factors that apply to different compliance levels. Secondly, we found that DE is a significant factor across all levels of compliance and is the most influential mechanism of the SLT on ISPCB. Thirdly, we show the special importance of social learning in low compliance groups. As this single study is the first step in the empirical investigation of SLT in different data-based behavioral groups, we hope that future studies will follow our path and consider the similarities and differences in different behavioral groups when analyzing sanctions on ISPCB.

7. References

Ahmad, Z., M., Norhashim, O. T. Song, & L. T. Hui (2016). A typology of employees' information security behavior. In: *2016 4th International Conference on Information and Communication Technology (ICoICT): IEEE*, 1–4.

Ahmad, Z., T., Liew, T. H., & Norhashim, M. (2019). Security monitoring and information security assurance behavior among employees. *Information & Computer Security* 27(2), 165–188.

Akers, R. L. (2002). A Social Learning Theory of Crime. In *S. Cote (ed.) Criminological theories. Bridging the past to the future*, 135–143. Thousand Oaks: Sage Publications.

Akers, R. L. (2017). Social Learning and Social Structure: Routledge.

Akers, R. L., & Sellers, C. S. (2011). Social Learning Theory. *The Oxford Handbook of Juvenile Crime and Juvenile Justice*: Oxford University Press.

Ali, R. F., Dominic, P. D. D., Ali, S. E. A., Rehman, M., & Sohail, Al. (2021). Information Security Behavior and Information Security Policy Compliance: A Systematic Literature Review for Identifying the Transformation Process from Noncompliance to Compliance. *Applied Sciences* 11(8), 3383.

Atzmüller, C., & Steiner, P. M. (2010). Experimental Vignette Studies in Survey Research. *Methodology* 6(3), 128–138.

Bandura, A. (1977). Social Learning Theory. Englewood Cliffs, New Jersey: Prentice-Hall.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly* 34(3), 523.

Burgess, R. L. & Akers, R. L. (1966). A Differential Association-Reinforcement Theory of Criminal Behavior. *Social Problems* 14(2), 128–147.

Chen, H. & Li, W. (2014). Understanding Organization Employee's Information Security Omission Behavior: An Integrated Model of Social Norm and Deterrence. In: *Proceedings of PACIS*.

Cram, W. A., D'Arcy, J., & Proudfoot, J. G. (2019). Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance. *MIS Quarterly* 43(2), 525–554.

Crossler, R. E. and Belanger, F. (2009). The Effects of Security Education Training and Awareness Programs and Individual Characteristics on End User Security Tool Usage. *Journal of Information System Security* 3(5).

Curran, P. G., & Hauser, K. A. (2019). I'm Paid Biweekly, Just not by Leprechauns: Evaluating Valid-but-Incorrect Response Rates to Attention Check Items. *Journal of Research in Personality* 82, 103849.

Dang, D. P. (2014). Predicting Insider's Malicious Security Behaviors: A General Strain Theory-Based Conceptual Model. In: *CONF-IRM 2014 Proceedings*.

D'Arcy, J., & Herath, T. (2011). A Review and Analysis of Deterrence Theory in the IS Security Literature:

Making Sense of the Disparate Findings. *European Journal of Information Systems* 20(6), 643–658.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research* 20(1), 79–98.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). Multivariate Data Analysis (Seven ed.). *Upper Saddle River*, NJ Prentice Hall: Pearson.

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to Report the Results of PLS-SEM. *European Business Review* 31(1), 2–24.

Hengstler, S., Pryazhnykova, N., & Kuehnel, S. (2022). How Employees Learn Information Security Policy Compliance Behavior: Toward a Social Learning Perspective. In: *Thirtieth European Conference on Information Systems (ECIS 2022)*, Timișoara, Romania.

Hengstler, S., Pryazhnykova, N., & Trang, S. (2021). How do Employees Learn Security Behavior? Examining the Influence of Individual Cultural Values and Social Learning on ISP Compliance Behavior. In: *Proceedings of the 54th Hawaii International Conference on System Sciences*. Ed. by T. Bui: Hawaii International Conference on System Sciences.

Hill, J. R., Song, L., & West, R. E. (2009). Social Learning Theory and Web-Based Learning Environments: A Review of Research and Discussion of Implications. *American Journal of Distance Education* 23(2), 88–103.

Höne, K., & Eloff, J. (2002). Information Security Policy — What do International Information Security Standards Say?. *Computers & Security* 21(5), 402–409.

Ifinedo, P. (2014). Information Systems Security Policy Compliance: An Empirical Study of the Effects of Socialisation, Influence, and Cognition. *Information & Management* 51(1), 69–79.

Johnston, A., Wech, B., Jack, E., & Beavers, M. (2010). Reigning in the Remote Employee: Applying Social Learning Theory to Explain Information Security Policy Compliance Attitudes. In: *AMCIS 2010 Proceedings*, 493.

Lembcke, T. B., Masuch, K., Trang, S., Hengstler, S., Plics, P., & Pamuk, M. (2019). Fostering Information Security Compliance: Comparing the Predictive Power of Social Learning Theory and Deterrence Theory. In *Proceedings of Americas Conference on Information Systems (AMCIS)*, Mexico.

Li, M. (2015). Moving Beyond the Linear Regression Model: Advantages of the Quantile Regression Model. *Journal of Management* 41(1), 71–98.

Liang, N., Biros, D. P., & Luse, A. (2016). An Empirical Validation of Malicious Insider Characteristics. *Journal of Management Information Systems* 33(2), 361–392.

Lippert, S. K., & Forman, H. (2005). Utilization of Information Technology: Examining Cognitive and Experiential Factors of Post-Adoption Behavior. *IEEE Transactions on Engineering Management* 52(3), 363–381.

Lowry, P. B., D'Arcy, J., Hammer, B., & Moody, G. (2016). “Cargo Cult” Science in Traditional Organization and Information Systems Survey Research: A Case for Using Nontraditional Methods of Data Collection, Including Mechanical Turk and Online Panels. *Journal of Strategic Information Systems* 25(3), 232-240.

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a Unified Model of Information Security Policy Compliance. *MIS Quarterly* 42(1), 285–311.

Nangle, D. W., Erdley, C. A., Zeff, K. R., Stanchfield, L. L., & Gold, J. A. (2004). Opposites do not Attract: Social Status and Behavioral-style Concordances and Discordances Among Children and the Peers Who Like or Dislike Them. *Journal of abnormal child psychology* 32(4), 425–434.

Niechoy, A., Masuch, K., & Trang, S. (2021). How Do Employees Learn Security Behavior? An Integrated Perspective on Social Learning and Rational Decision Making. In: C. Metallo, M. Ferrara, A. Lazazzara and S. Za (eds.) *Digital Transformation and Human Behavior*, 149–164. Cham: Springer International Publishing.

Peer, E., Vosgerau, J., & Acquisti, A. (2014). Reputation as a Sufficient Condition for Data Quality on Amazon Mechanical Turk. *Behavior research methods* 46(4), 1023–1031.

Podsakoff, P. M., MacKenzie, S.B., Lee, Y. J., & Podsakoff, N. P. (2003). Common Method Biases in Behavioral Research: a Critical Review of the Literature and Recommended Remedies. *Journal of Applied Psychology* 88(5), 879–903.

Pratt, T. C., Cullen, F. T., Sellers, C. S., Thomas Winfree, L., Madensen, T. D., Daigle, L. E., Fearn, N. E., & Gau, J. N. (2010). The Empirical Status of Social Learning Theory: A Meta-Analysis. *Justice Quarterly* 27(6), 765–802.

Rees, J., Bandyopadhyay, S., & Spafford, E. H. (2003). PFIRES. *Communications of the ACM* 46(7), 101–106.

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, Attitudes, and Intentions: Predicting Initial Adoption of Information Security Behavior. *Computers & Security* 49, 177–191.

Siponen, M., Adam M., & Pahnila, S. (2014). Employees’ Adherence to Information Security Policies: An Exploratory Field Study. *Information & Management* 51(2), 217–224.

Siponen, M., & Vance, A. (2014). Guidelines for Improving the Contextual Relevance of Field Surveys: the Case of Information Security Policy Violations. *European Journal of Information Systems* 23(3), 289–305.

Skinner, W. F., & Fream, A. M. (1997). A Social Learning Theory Analysis of Computer Crime Among College Students. *Journal of research in crime and delinquency* 34(4), 495–518.

Solms, B. von (2000). Information Security — The Third Wave?. *Computers & Security* 19(7), 615–620.

Solms, B. von, & Solms, R. von (2004). The 10 Deadly Sins of Information Security Management. *Computers & Security* 23(5), 371–376.

Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables Influencing Information Security

Policy Compliance. *Information Management & Computer Security* 22(1), 42–75.

Sutherland, E. H. (1972). The Theory of Differential Association. In: D. Dressler (ed.) *Readings in Criminology and Penology*, 365–371: Columbia University Press.

Trang, S., & Brendel, B. (2019). A Meta-Analysis of Deterrence Theory in Information Security Policy Compliance Research. *Information Systems Frontiers* 21(6), 1265–1284.

Trang, S., Trenz, M., Weiger, W. H., Tarafdar, H., & Cheung, C. M. (2020). One App to Trace Them All? Examining App Specifications for Mass Acceptance of Contact-Tracing Apps. *European Journal of Information Systems* 29(4), ,415–428.

Tu, Z., Turel, O., Yuan, Y., & Archer, N. (2015). Learning to Cope With Information Security Risks Regarding Mobile Device Loss or Theft: An Empirical Examination. *Information & Management*, 52(4), 506-517.

Vroom, C., & von Solms, R. (2004). Towards Information Security Behavioral Compliance. *Computers & Security* 23(3), 191–198.

Warkentin, M., Johnston, A. C., & Shropshire, J. (2011). The Influence of the Informal Social Learning Environment on Information Privacy Policy Compliance Efficacy and Intention. *European Journal of Information Systems* 20(3), 267–284.

Whitman, M. E., & Mattord, H. J. (2012). Principles of Information Security. 4. ed., International ed. Stamford, Conn.: Course Technology Cengage Learning.

Wiafe, I., Koranteng, F. N., Wiafe, A., Obeng, E. N., & Yaokumah, W. (2020). The Role of Norms in Information Security Policy Compliance. *Information & Computer Security* 28(5), 743–761.

Willison, R., & Warkentin, M. (2013). Beyond Deterrence: An Expanded View of Employee Computer Abuse. *MIS Quarterly* 37(1), 1–20.

Yoo, C. W., Goo, P., & Rao, H. R. (2020). Is Cybersecurity a Team Sport? A Multilevel Examination of Workgroup Information Security Effectiveness. *MIS Quarterly* 44(2), 907–931.

Yu, K., Lu, Z., & Stander, J. (2003). Quantile Regression: Applications and Current Research Areas. *Journal of the Royal Statistical Society. Series D (The Statistician)* 52(3), 331–350.

8. Appendix

Table A1: Used items per construct.

Construct	Question
Scenario	Anna/Felix is a middle manager in a medium-sized company where she/he was recently hired. Her/his department uses an inventory procurement application program to ensure that only authorized employees can make purchases. The company has a firm policy that employees must log off or lock their computers when they are not using them. Anna/Felix assumes that she/he and her/his colleagues could save time on ordering by keeping her/his account logged in.
DR1	It's likely I'll get caught if I stay logged in as Anna did.
DR2	I will be punished quickly if I stay logged in like Anna.
DR3	The expected penalty will be high if I stay logged in like Anna.
DA1	Many of my colleagues in my team stay logged in like Anna.
DA2	Many colleagues who are important to me stay logged in like Anna.
DA3	Many colleagues, with whom I have a lot to do, stay logged in like Anna.
IM1	Since many colleagues on my team, like Anna, stay logged in, I act the same way.
IM2	Since many colleagues who are important to me remain logged in, like Anna, I behave the same way.
IM3	Since many colleagues I deal with a lot stay logged in like Anna, I act the same way.
DE1	Because it contradicts my employer's rules, I would never stay logged in like Anna.
DE2	In general, I do not stay logged in like Anna.
DE3	Since it goes against my personal values, I would not stay logged in like Anna.
ISPCB1	I will comply with the requirements of my organization's information security policy in the future.
ISPCB2	I will protect information and technology resources in the future in accordance with the requirements of my organization's information security policy.
ISPCB3	I will fulfill my responsibilities prescribed in the information security policy when using information and technology in my organization in the future.
C1	What gender do you identify as? *male; female; diverse; not specified*
C2	How often do you use a computer at your workplace? *Never; once a month; several times a month; several times a week; daily [must be at least once a month]*
C3	To what extent are you familiar with the contents of your organization's information security policy? *Select on a scale from 1 (completely unknown) to 7 (completely known). [must be > 1]*
C4	Please indicate your age: input box
C5	Please indicate your highest level of education: *Less than high school; Secondary School; High School; Some College or Further Education; Completed training; Bachelors degree; Masters degree; Doctoral degree*
C6	Please indicate the size of the company in which you work or last worked (number of employees): *Less than 500; 500 – 999; 1000-4999; 5000 - 10000; More than 10000*