Computers & Security 133 (2023) 103370

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Should i really do that? Using quantile regression to examine the impact of sanctions on information security policy compliance behavior

Sebastian Hengstler[a,#,*], Stephan Kuehnel[b], Kristin Masuch[a], Ilja Nastjuk[a], Simon Trang[c]

[a] Georg-August-Universität Göttingen – Research Group on Information Security and Compliance, Platz der Göttinger Sieben 5, Göttingen 37073, Germany
[b] Martin Luther University Halle-Wittenberg, Chair for Information Systems, esp. Business Information Management, Universitaetsring 3, Halle (Saale) 06108, Germany
[c] University of Paderborn – Chair of Information Systems and Sustainability, Warburger Str. 100, Paderborn 33098, Germany

ARTICLE INFO

Article history:
Received 1 January 2023
Revised 30 May 2023
Accepted 25 June 2023
Available online 29 June 2023

Keywords:
Information security policy compliance
International information security management
Deterrence theory
Quantile regression
Compliance behavior

ABSTRACT

Deterrence theory is one of the most commonly used theories to study information security policy noncompliance behavior. However, the results of studies in the information security field are ambiguous. To further address this heterogeneity, various influencing factors have been considered in the context of deterrence theory. However, a current challenge with these findings is that recent studies that quantitatively assess the effectiveness of deterrence have relied predominantly on methods that analyze the underlying data, starting from a regression-based approach. By applying quantile regression, we estimate the overall effect of deterrents, and uncover how their effect differs among employees with different inclinations toward ISP compliance behavior – a critical insight for determining security measures for specific employee groups. Based on longitudinal data gathered in the U.S., our findings show significantly different effects in the analyzed quantiles for both aspects of sanctions, namely certainty and severity.

1. Introduction

The increasing interconnectivity and digitalization in the present-day business world has led to an enormous rise in the risk of cyber security attacks on organizations (Verizon, 2022). This results in damage amounting to billions of dollars every year (Gartner, 2018). One of the greatest risks is the misbehavior of employees who, for example, do not adhere to the information security policy (ISP) defined by the company. This is where research on compliance behavior in ISP addresses and considers a wide range of theories from different fields (Sommestad et al., 2014). Among these, deterrence theory is one of the most commonly used theoretical lenses to explain ISP-compliance behavior (D'Arcy and Herath, 2011). It helps to explain whether and how sanction mechanisms work to deter employees from non-compliant ISP behavior (Gordon et al., 2011). Deterrence is also considered the de facto standard in organizations to enforce compliance (Trang and Brendel, 2019). However, the effectiveness of sanctions on ISP-compliance behavior remains controversial, as research findings in this area are inconsistent (Lowry et al., 2015). Consequently, research has questioned the merits of deterrence theory in explaining ISP-compliance behavior (D'Arcy and Herath, 2011; Lowry et al., 2015).

Robey and Boudreau (1999) emphasized that inconsistencies in the literature can be resolved by applying three main strategies: 1) including additional contingency variables, 2) reviewing the research questions, and 3) evaluating the utilized research methods. Studies have examined more specific contexts to identify differences in the effectiveness of sanctions (for a review, see Trang and Brendel, 2019). It is discussed whether differences can be triggered by various influencing factors, such as cultural differences, contextual specificities, different security threats, or other underlying behavioral intentions, such as malicious or unintentional behavior (Aurigemma and Mattson, 2019; Vance et al., 2020). In line with Robey and Boudreau (1999), researchers have also critically examined substantive theoretical assumptions (substantive research questions) to explain inconsistent findings in deterrence-based studies, such as the generalizability of deterrence constructs or their applicability to explain positive or negative outcome variables

[*] Corresponding author.
E-mail addresses: Sebastian.hengstler@volkswagen.de (S. Hengstler), stephan.kuehnel@wiwi.uni-halle.de (S. Kuehnel), kristin.masuch@wiwi.uni-goettingen.de (K. Masuch), Simon.trang@uni-paderborn.de (I. Nastjuk), ilja.nastjuk@wiwi.uni-goettingen.de (S. Trang).
[#] On behalf of the co-authors, Sebastian Hengstler

https://doi.org/10.1016/j.cose.2023.103370
0167-4048/

(D'Arcy and Herath, 2011). In contrast, it appears that the positive influence of sanction certainty on ISP-compliance behavior works better for positive behaviors than for negative ones (Trang and Brendel, 2019). The literature has also raised methodological issues to explain inconsistencies in findings, such as the utilization of objective and perceptual sanction measures, the interaction between formal and informal sanction measures, and the sampling methodology design (D'Arcy and Herath, 2011; D'Arcy and Lowry, 2019; Siponen and Baskerville, 2018).

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 deterrence have predominantly relied on methods that analyze the underlying data using mean-based regression approaches (Trang and Brendel, 2019). Mean-based regression approaches suggest that the marginal effect of the independent variable (i.e., sanctions) is equally large at all levels of the dependent variable (i.e., propensities of security behavior). We challenge this assumption and suggest that the impact of deterrence constructs on ISP-compliance behavior is not uniform across individuals' behavioral propensities. Learning from behavioral studies in the field, such as D'Arcy and Herath (2011), Kuo et al. (2020), and Trang and Brendel (2019), we believe it is reasonable to assume that deterrence mechanisms work differently at different levels of security behavior propensities. The inconsistent findings in the literature support our assumptions. For example, a plethora of studies reveal a statistically positive relationship between common deterrence-related constructs, such as formal sanction certainty and ISP compliance (Aurigemma and Mattson, 2017; D'Arcy and Hovav, 2009). Other studies have shown no or opposite effects (Guo et al., 2011; Li et al., 2014; Pahnila et al., 2007; Siponen and Vance, 2010). We believe that a different quantitative analysis approach, that is, quantile regression, can help shed light on such empirical inconsistencies. A quantile regression allows quantification of the effect between deterrence mechanisms and ISP-compliance behavior 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, median regression, or least absolute deviation minimizes the sum of the absolute values of the prediction error. It also allows the identification of potential clusters of individuals that have different ISP compliance behavior tendencies. Thus, it allows us to enhance our understanding of the conditions under which deterrence mechanisms may be more effective (Trang et al., 2020).

We developed a theoretical model based on deterrence theory's most commonly used mechanisms in the field of ISP-compliance behavior research. Building on a quantitative study with 263 participants, we first determined the general influence of deterrence mechanisms on ISP compliance behavior. Then, using the heterogeneous responses of the participants in our study, we use quantile regression to uncover the effect of deterrence mechanisms on ISP-compliance behavior in three categories of employees: employees who tend to behave in an ISP non-compliant manner, employees with average compliance, and employees who tend to behave in a stricter ISP-compliant manner (Ahmad et al., 2019).

From a research perspective, our results have implications for the usage of deterrence theory in information security research. Our primary contribution is empirical in nature (Trang et al., 2020); i.e., with our quantile regression approach, we empirically identify boundary conditions for the applicability of deterrence measures. More specifically, we reveal that the effectiveness of formal and informal sanctions based on different groups of employees using the mechanisms of deterrence theory differs. Moreover, our results show that ISP compliance behavior is a complex problem in which security measures based on deterrence theory cannot only be distinguished by different security threats or other security context-related differences, but rather pay attention to different employee behavioral principles. Furthermore, we respond to the call for more applied longitudinal research with our analyzed dataset, using a novel method to study the effects of sanctions on ISP compliance behavior (Siponen and Baskerville, 2018). The practical implication of our results is that for the severity of a sanction, threats of very likely formal and informal sanctions work differently in different groups of employees. For example, severe sanctions are found to perform particularly well for less compliant employees with their organizations' ISP. Conversely, for employees who are neither particularly compliant nor non-compliant, formal sanctions work well. Additionally, informal sanctions were found to work well, regardless of ISP-compliance behavior.

The rest of the paper is structured as follows. Based on our research approach, we first review deterrence theory 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 a presentation and discussion of the results, followed by implications for theory and practice, and finally offers some conclusions.

2. Reviewing deterrence theory

Deterrence theory originally belongs to the criminology field and appears to be one of the most commonly used theories to explain ISP-compliance behavior (Vance et al., 2020). In broadest terms, the theory states that individuals choose to commit a crime when the benefits outweigh the underlying punishments. Deterrence theory states that the compromise between benefits and expected punishments can fail. In doing so, the theory addresses different influencing factors, such as sanction certainty, sanction severity, and sanction celerity (Sommestad et al., 2014; Vance et al., 2020). Sanction certainty is defined as the degree to which sanctions are perceived as expected by an individual. Sanction severity describes the expected amount of penalty when a policy violation is committed. Sanction celerity describes the perceived rapidity with which a punishment is enforced if a person is caught for non-compliant behavior (Pratt et al., 2010). Information security research also often distinguishes between formal and informal sanctions (D'Arcy and Herath, 2011). Examples of formal sanctions include warnings, fines, job loss, and criminal charges. Aspects such as loss of reputation and trust, shame, or lost opportunities for promotion in the organization are mentioned as informal sanctions (Kuo et al., 2020).

The usability of sanctions to positively influence ISP-compliance behavior cannot be clearly answered with the existing literature. In particular, D'Arcy and Herath (2011) point out that, depending on contextual differences, such as different security threats, moral beliefs, the job position of an employee, and cultural diversity, these differences can influence the applicability of sanctions on ISP-compliance behavior. They indicate that strong moral beliefs can effectively restrain compliant behavior. Therefore, the threat of punishment is weaker in this context (Pratt et al., 2010). Less morally inhibited employees are more influenced by the threat of sanctions. Job position or job tenure affects how engaged employees are with their organization, policies, and consequences of ISP violations because employees identify themselves with their jobs and the organization in a certain way (D'Arcy and Hovav, 2009; Herath and Rao, 2009).

Trang and Brendel (2019) highlight the previous findings and show the different applications of the constructs of deterrence theory in ISP compliance behavior research. They show the limited importance of sanction certainty in its subordinate role in explaining ISP-compliance behavior (Guo et al., 2011; Johnston et al., 2015). The importance of contextual differences is supported by

Table 1
Construct Definitions for Theory of Planned Behavior.

Construct	Definition
Formal Sanction Severity	Formal sanction severity is the formally expected penalty when a policy violation is committed, such as a fine or a warning.
Formal Sanction Certainty	Formal sanction certainty describes the perceived probability of being formally punished, if one is caught for ISP non-compliant behavior.
Informal Sanction Severity	Informal sanction severity is the expected amount of an informal penalty when an ISP policy violation is committed, such as the loss of reputation among colleagues and superiors or shame.
Informal Sanction Certainty	Informal sanction certainty describes the perceived probability of being informally punished by the social environment if one is caught (e.g., at the workplace).

their findings as well, as they show that a malicious context better fits deterrence theory in terms of the severity of sanctions. Sanction certainty has a higher correlation with behavior in ISP compliance studies related to positive rather than negative behavior. Similar to Trang and Brendel (2019), Vance et al. (2020) also show that culture can have an impact on the effectiveness of deterrence mechanisms on ISP-compliance behavior.

When looking at the current state of research, some challenges can be identified from the existing evidence. Recent studies that quantitatively assess the effectiveness of deterrence predominantly rely on methods that analyze the underlying data starting from the mean in regression-based approaches (Trang and Brendel, 2019). The results of these studies provide important insights into whether elements of deterrence theory generally have an effect on ISP-compliance behavior, regardless of whether the respondent is generally more compliant or more non-compliant. Nevertheless, such approaches do not provide insights into which behavioral groups of employees sanctions work in the most effective way (Ahmad et al., 2019; Trang et al., 2020). A more precise differentiation in such groupings is revealed by inconsistent modes of action of deterrence constructs, which we can notice in existing research (Aurigemma and Mattson, 2017; D'Arcy and Hovav, 2009; Guo et al., 2011).

From a practical perspective, however, this is crucial since information security professionals need to deploy security controls in their organization to ensure the highest possible level of information security. It is important to know which groups of employees can be better addressed with which type of measures, which are sanctions in our case. To examine such a distinction in different groups of employees, we use quantile regression. We rely on the deterrence constructs that have been identified in past research as predominantly effective in different contexts and follow the suggestion of D'Arcy and Herath (2011) to use both formal and informal deterrence mechanisms. The constructs used in our research model are summarized in Table 1. Based on the findings of existing research, sanction celerity was not considered since it plays only a minor role in explaining ISP-compliance behavior alongside the other mentioned deterrence constructs (Trang and Brendel, 2019).

3. Research design

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

We chose the U.S. as the empirical setting because most studies on ISP-compliance behavior and deterrence have been conducted in the U.S. 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 (Hovav and D'Arcy, 2012; Moody et al., 2018). We collected data in the U.S. at two different periods of time to avoid common weaknesses in measuring behavior through a cross-sectional study and to measure actual ISP-compliance behavior instead of only the intention to comply (D'Arcy and Lowry, 2019).

Our variables followed a context-independent approach and measured general ISP-compliance behavior to make generalized statements about the effectiveness of deterrence mechanisms and to compare their explanatory power across the quantiles analyzed without considering contextual specifics, such as different security threats (Aurigemma and Mattson, 2019). We used the items from D'Arcy and Lowry (2019) to measure behavior and generalized them for our study. The items on formal and informal sanction severity and certainty of deterrence theory (3 items each) were taken from Moody et al. (2018) and adapted for our study. We also used a 7-point Likert scale for our questionnaires (from strongly disagree to strongly agree) from the survey at both the first period of time (T0) and the subsequent one (T1). The demographic characteristics of the respondents were adapted from Hovav and D'Arcy (2012). A pilot study was conducted by sending questionnaires to five academic experts for review. A test run was conducted with 50 participants, and at least 30 results were complete and valid. We used the crowdsourcing platform "Amazon Mechanical Turk" (MTURK) to collect the data, taking into account the quality criteria defined by Lowry et al. (2016). First, only participants with a cultural background and origin in the U.S. were able to participate in our study. Second, their acceptance rate of previous participation in other jobs on the platform must have been higher than 98% (Lowry et al., 2016). Third, there was a preselection at the beginning of the study to select the participants who fulfilled the criteria of participation, namely: currently employed, worked at least partially with a computer in their job, and their organization has an ISP. To additionally avoid potential biases (e.g., lack of attention, or socially desirable responding), we used several attention checks, such as queries about study entry requirements, neutral wording, a warning that inattentive respondents would not be paid, quality controls using a common method bias test, and a large sample (Jia et al., 2017). Respondents of T0 who did not complete T1 or did not meet the quality criteria were excluded from the sample. We tested for a potential attrition bias. More specifically, we tested whether non-respondents (in T1) were significantly different from respondents (in T1) in regard to our central sample characteristics of age, gender, and results regarding formal and informal sanction severity and certainty. A t-test revealed no significant differences for Age ($t = 1.258$; $p > 0.10$), Gender ($t = 0.118$; $p > 0.10$), and our deterrence constructs Formal Sanction Severity ($t = 1.438$; $p > 0.10$), Formal Sanction Certainty ($t = 0.625$; $p > 0.10$), Informal Sanction Severity ($t = 1.250$; $p > 0.10$), and Informal Sanction Certainty ($t = 0.657$; $p > 0.10$). We conclude that panel attrition is not a significant concern in our analysis.

The average age in our sample is between 30 and 35 years, and the proportion of men is higher than 60%. The majority of the participants in our studies work in a sector that is at least IT related (28%), with a further majority working in manufacturing, finance, or healthcare. At least 82% have a bachelor's degree or higher. Most participants work in technical, administrative, or thematic-professional areas. About 43% of participants have a management position. The majority of the participants work in a company with

Table 2
Sample Demographics.

Demographics	Characteristics ($N = 263$)
Age	< 20 years = 8% (21) | 20–25 years = 10% (26) | 26–30 years = 21% (55) 31–35 years = 23% (60) | 36–40 years = 17% (45) | 41–45 years = 9% (24) 46–50 years = 6% (16) | 51–60 years = 4% (11) | >= 60 years = 2% (5)
Gender	Male = 60% (158) | Female = 40% (105)

Industry	Manufacturing = 22% (58) | Finance = 15% (39) | IT = 28% (74)
	Healthcare = 11% (29) | Education = 9% (24) | Retail = 7% (18) | Other = 8% (21)

Education	High School = 2% (5) | Two-Year College = 16% (43) | Bachelor’s Degree = 37% (97) Master’s Degree = 35% (92) | Doctoral Degree = 10% (26)
Job Position	Senior Manager = 13% (34) | Middle Manager = 39% (103) | Technical Staff = 20% (53) Professional Staff = 19% (50) | Administrative = 9% (23)
Company Size (nr. of employees)	<100 = 3% (8) | 100–499 = 5% (13) | 500–999 = 9% (24) | 1000–2499 = 16% (42) 3500–9999 = 21% (55) | 10,000–100,000 = 32% (84) | More than 100,000 = 14% (37)

Table 3
Used Items and Factor Loadings.

Construct	Item	Factor Loading
Formal Certainty	What is the chance, that you would be formally sanctioned (punished) if management learned that you had violated company information security policies?	0.784
Formal Certainty	I would receive corporate sanctions, if I violated company ISP procedures.	0.814
Formal Certainty	What is the chance, that you would be warned if management learned you had violated company information security procedures?	0.799
Formal Severity	How much of a problem would it create in your life, if you violated the company information security policy?	0.912
Formal Severity	How much of a problem would it be, if you received severe sanctions if you violated the company information security policy?	0.864
Formal Severity	How much of a problem would it create in your life, if you were formally sanctioned if you violated the company information security policy?	0.879
Informal Severity	It would create a problem in my life, if my career was adversely affected for not complying with ISP procedures regularly.	0.775
Informal Severity	It would create a problem in my life, if I lost the respect and good opinion of my colleagues for not following ISP procedures regularly.	0.701
Informal Severity	It would create a problem in my life, if I lost the respect of my manager for not complying with ISP procedures regularly.	0.941
Informal Certainty	How likely is it that you would lose the respect and good opinion of your business associates for violating company information security procedures?	0.871
Informal Certainty	How likely is it that you would jeopardize your promotion prospects if management learned that you had violated company information security procedures?	0.765
Informal Certainty	How likely is it that you would lose the respect and good opinion of your manager for violating company information security policies?	0.832
ISP-Compliance Behavior	I complied with the requirements of the ISP procedures of my organization in the past.	0.923
ISP-Compliance Behavior	I protected information and technology resources according to the requirements of the ISP procedures of my organization.	0.941
ISP-Compliance Behavior	I carried out my responsibilities prescribed in the ISP procedures of my organization when I use information and technology.	0.877

more than 1000 employees. The demographics are summarized in Table 2.

We used the marker variable technique to carry out the common method bias test and chose the respondent’s outside activities as the theoretically unrelated marker variable (D’Arcy and Lowry, 2019; Lindell and Whitney, 2001). The highest variance that the marker shares with another construct is less than 0.05. Participants were paid $1.65 for successful and conscientious participation in the study. In total, 623 people participated in the study. According to the applied quality criteria, the resulting sample consisted of 263 valid responses (42% validity rate, 09:20 min average completion time). To measure ISP-compliance behavior instead of the intention to comply, after 30 days, 263 MTURK participants with valid results from T0 were asked to participate in a second similar study. For the second study, participants were paid $2 for successful and conscientious participation, including a validity check of also participating in the first study. In total, 180 people participated in the second study, and 142 valid results were collected (54% validity rate, 08:40 min average completion time). Both response rates fit the stringent guideline that the sample should be ten times larger than the number of maximal paths in our model (Hair et al., 2017). The items used, including their factor loadings, are listed in Table 3.

3.2. Data validation

We used a quantile regression approach to test our models because we did not perform an ordinary least squares (OLS) regression to analyze the regression line for the mean but for a determined quantile (Li, 2015). This allowed us to examine whether deterrence mechanisms have an effect on ISP compliance behavior in different quantiles of our longitudinal data. We defined a potential grouping of employees into our quantiles (0.25 – tending to be non-compliant; 0.5 – average compliant, 0.75 – compliant) and analyzed them for differences. We used IBM SPSS 25 software to perform our analysis. As the first step, we evaluated the validity and reliability of our sample’s instruments. After that, we analyzed our data in light of our research approach. To verify the validity and reliability of our data, common quality criteria for reflective measurement models in information security research were applied to our study and are listed in Table 4 (Lowry et al., 2016). To validate our data quality, we used typical quality criteria for quantile regressions (Li, 2015; Trang et al., 2020). We used individual item reliability and Cronbach’s alpha as indicators of convergent validity for our model. The factor loadings of the items used were all above 0.7, which indicates sufficient item reliability (Hair et al., 2012; Trang et al., 2020). The Cronbach’s alpha values were higher than

Table 4
Correlations and Quality Criteria of the Model.

Variable	Mean (Std. Dev.)	CA	FSS	FSC	ISS	ISC	ISPCB
Formal Sanction Severity (FSS)	5.305 (1.722)	0.789	1.00				
Formal Sanction Certainty (FCC)	5.284 (2.061)	0.740	0.318	1.00			
Informal Sanction Severity (ISS)	5.289 (1.971)	0.873	0.456	0.209	1.00		
Informal Sanction Certainty (ISC)	5.222 (2.104)	0.798	0.211	0.396	0.311	1.00	
Information Security Policy Compliance Behavior (ISPCB)	5.899 (1.287)	0.866	0.264	0.150	0.283	0.195	1.00

Note. All scales measured on a 1–7 Likert scale; CA: Cronbach's Alpha.

0.7 for every variable used in our model (Gefen and Straub, 2005). Additionally, the cross-loadings showed that all items had 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.

4. Results

We used an SEM approach to test the theoretical models. We used the partial least squares method.

4.1. Model specification

To determine possible specifications for the use of sanctions 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 the changes in the means of the mechanisms analyzed. We specified a regression equation (1) that included the variables of deterrence theory and control variables for demographic variables on age and gender:

$$
\begin{aligned}
&\text{ISP\_compliance\_behavior}_{\text{i}} = \text{ß}_0 \\
&\quad + \text{ß}_1 \text{x Formal\_sanction\_severity}_{\text{i}} \\
&\quad + \text{ß}_2 \text{x Formal\_sanction\_certainty}_{\text{i}} \\
&\quad + \text{ß}_3 \text{x Informal\_sanction\_certainty}_{\text{i}} \\
&\quad + \text{ß}_4 \text{x Informal\_sanction\_severity}_{\text{i}} \\
&\quad + \text{ß}_5 \text{x Age}_{\text{i}} \\
&\quad + \text{ß}_6 \text{x Gender}_{\text{i}} + \text{e}_{\text{i}}.
\end{aligned}
$$

The OLS regression results show a multimodal distribution of our data based on our 7-point Likert scale. Assuming the findings of previous research that deterrence theory 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 deterrence theory have differential effects on ISP-compliance behaviors across the distribution (Boichuk et al., 2019).

Quantile regression is a type of regression that is widely used in quantitative modeling, is primarily used for this purpose, and is an extension of standard linear regression, which estimates the conditional mean of the outcome variable. It can be used when, among other things, the assumptions of linear regression are not met, or quantiles other than the mean (as in linear regression) are to be analyzed. Quantile regression can be used to better understand the relationships between variables outside the mean of the data. Accordingly, it is used primarily to understand outcomes that are not normally distributed and have nonlinear relationships with predictor variables. In addition, the methodology makes it possible to drop the assumption that variables operate at the upper ranges of the distribution, just as they do at the mean, and to identify the factors that are important determinants of the variables. Therefore, we rely on the following specification of our quantile regression equation (2), where the quantiles are indexed by θ:

$$
\begin{aligned}
&\text{Quant}_\theta[\text{ISP\_compliance\_behavior}_{\text{i}}] = \gamma_{0,\theta} \\
&\quad + \gamma_{1,\theta} \text{x Formal\_sanction\_severity}_{\text{i}} \\
&\quad + \gamma_{2,\theta} \text{x Formal\_sanction\_certainty}_{\text{i}} \\
&\quad + \gamma_{3,\theta} \text{x Informal\_sanction\_certainty}_{\text{i}} + \text{e}_{\text{i},\theta} \\
&\quad + \gamma_{4,\theta} \text{x Informal\_sanction\_severity}_{\text{i}} \\
&\quad + \gamma_{5,\theta} \text{x Age}_{\text{i}} \\
&\quad + \gamma_{6,\theta} \text{x Gender}_{\text{i}}
\end{aligned}
$$

4.2. Model estimation

To uncover the differential effects of sanctions on ISP compliance behavior, we tested whether equation (2) had differential effects for the 0.25, 0.50, and 0.75 quantiles. The results of our quantile regression are shown in Table 5 (see columns 3–5).

Based on the equation given in (1) and its specification, we first estimated an OLS regression to examine the effect of deterrence mechanisms on the conditional mean of ISP compliance behavior (see Table 5, column 2 for the results). We found that, unlike informal sanction severity ($\beta_4 = 0.059$, $p < 0.10$), there was a significant effect on ISP-compliance behavior of the other constructs in our model. Both formal sanction certainty ($\beta_2 = 0.185$, $p < 0.01$) and informal sanction certainty ($\beta_3 = 0.304$, $p < 0.01$) have a positive and significant effect on ISP-compliance behavior. Additionally, we were able to identify a significant effect of formal sanction severity as well ($\beta_1 = 0.106$, $p < 0.05$). The effect of the control variable gender was statistically insignificant, where the effect for age was significant ($\beta_5 = 0.106$, $p < 0.05$).

We tested whether equation (2) had differential effects for the 0.25, 0.50, and 0.75 quantiles to uncover the differential effects

Table 5
OLS and Quantile Regression Estimation.

Variable	OLS	Quantile regression		
	Mean	0.25	0.50	0.75
Constant	2.463 (0.359)	0.906 (0.329)	2.566 (0.388)	4.463 (0.345)
Formal Sanction Severity	**0.106*** **(0.030)**	**0.251**** **(0.069)**	**0.133*** **(0.076)**	0.**196**** **(0.07)**
Formal Sanction Certainty	**0.185**** **(0.059)**	0.056 (0.064)	**0.140*** **(0.082)**	−0.090 (0.067)
Informal Sanction Severity	0.059 (0.057)	0.048 (0.065)	0.002 (0.077)	0.048 (0.069)
Informal Sanction Certainty	**0.304**** **(0.060)**	**0.479*** **(0.062)**	**0.358*** **(0.073)**	**0.240*** **(0.073)**
Age	**0.106*** **(0.030)**	**0.070*** **(0.033)**	**0.158**** **(0.034)**	**0.126**** **(0.037)**
Gender	0.060 (0.103)	0.039 (0.114)	**0.273*** **(0.112)**	0.127 (0.126)
Adj R^2	0.322	0.519	0.400	0.322

(*: significant at 0.05; **: significant at 0.01); bold marked numbers are statistically significant effects.

of formal and informal sanction mechanisms on different behaviors. Our quantile regression results are shown in Table 5 (see columns 3–5). The results from the OLS analysis were similar to those from the 0.50 quantile for all the mechanisms analyzed. The effect for formal sanction severity is higher in the 0.25 quantile than in the 0.50 and 0.75 quantiles ($y_{1,0.25} = 0.251$, $p < 0.01$). A similar effect size can be seen for informal sanction certainty, for which the effect size decreases from the 0.25 to the 0.75 quantile ($y_{4,0.25} = 0.479$, $p < 0.05$). Formal sanction certainty shows a significant effect size only in the 0.50 quantile ($y_{2,0.5} = 0.140$, $p < 0.05$). Furthermore, the adjusted R^2 for the 0.25 quantile is higher than for the OLS analysis and the other quantiles considered. Moreover, the predictive capability of deterrence theory for the 0.25 quantile in terms of variance explained (i.e., adjusted R^2) is higher than for the 0.50 and the 0.75 quantiles. Overall, this may indicate that the selected variables of deterrence theory are comparatively better suited to explaining information security policy compliance behavior in the 0.25 quantile than in the other quantiles.

5. Discussion

The aim of this study was to explore the extent to which deterrence theory mechanisms of formal and informal sanction severity and certainty have different effects on distinct quantiles within an analyzed longitudinal dataset. 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. In our study, significant effects can be identified for the OLS regression, especially for formal sanction severity (0.106*), formal sanction certainty (0.185**), and informal sanction certainty (0.304**). The effect sizes for formal sanction severity and formal sanction certainty can be classified in the effect size interval determined by Trang and Brendel (2019) for the corresponding construct from ISP-compliance behavior and are close to the average effect size determined in each case. The effect of informal sanction certainty in our study is significantly higher than the average determined by Trang and Brendel (2019; 0.144). As mentioned, the results of the OLS regression are not very different from those of the 0.50 quantile. This could indicate that the OLS regression, which is widely used in existing research, has similar results to the quantile which tends to include results from the middle range of the Likert scale we used. Thus, safety measures derived from such results could be effective for employees who tend to behave neither more positively nor more negatively than average. Unexpectedly, the effect for the severity of formal sanctions is higher in the 0.25 quantile than in the 0.50 and 0.75 quantiles, and is above the effect size found in existing research. A similar effect size was observed for informal sanction security, for which the effect size decreased from the 0.25 to the 0.75 quantile. This could indicate that safety measures based on formal sanction severity tend to work better for employees whose feedback is in the 0.25 quantile, as well as for informal sanction certainty. On the contrary, the 0.25 and 0.75 quantiles for formal sanction certainty only showed a significant effect in the OLS and 0.50 quantile regressions, which may indicate a lack of effectiveness for groups of people within the 0.25 and 0.75 quantiles.

5.1. Research implications

Our study has several implications for information security research. First, we theorize how sanctions affect different behavioral groups of employees and positively influence compliance behavior with ISPs. We show how the effectiveness of formal and informal sanctions differs according to different ISP-compliance behavior tendencies, based on the mechanisms of deterrence theory (Moody et al., 2018). The goal of such a distinction is to target ISP-compliance behavior within the organization. We propose that an appropriate set of specifications is likely to increase ISP-compliance behavior. By drawing attention to the specifics of how formal and informal sanctions differ in effectiveness across behavioral groups, our study lays the groundwork for future research to more purposefully design mechanisms to ensure information security. Our results suggest that it is worthwhile to have a glimpse beyond the mean when evaluating the effectiveness of security interventions. We find that deterrence mechanisms have a more complex deter function for individuals depending on their inclination, especially for the deterrence constructs of formal sanction certainty and informal sanction certainty. With respect to the factor of age in our model, we were able to identify that the age of our subjects has an influence on the effectiveness of the different analyzed deterrence mechanisms. Our study results show that a higher age can positively influence the effectiveness of formal and informal sanction certainty and sanction severity.

Second, our chosen grouping of employees based on behavioral inclinations toward compliance (i.e., tending to be non-compliant, average compliant, and compliant) 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 formal sanction severity, formal sanction certainty, and informal sanction certainty have different effects on ISP-compliance behavior. 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 the boundary conditions for the usage of deterrence theory in information security research. Thus, we provide the argument for the proposition that ISP-compliance behavior 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 use of deterrence constructs to positively influence ISP-compliance behavior. A next step for research in this area would be to define the underlying conditions for our different analyzed groups of ISP-compliance behavior tendencies in order to be able to address inconsistencies more precisely.

5.2. Practical implications

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 sanctions 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 sanctions in terms of information security compliance (Kuo et al., 2020). To find a promising mix of sanctions, security experts first need to identify the different target groups in their organizations (e.g., through different awareness campaigns or tools, such as phishing). Based on the results of our quantile regressions, we discuss general strategic options for using sanctions to ensure information security. In general, our results can be used by information security experts to tailor security measures to the groups of employees we have defined. First, our results state that individuals who tend to be less compliant with their organization's ISP are more responsive to the severity of sanctions. If an organization has to deal with many employees who tend to be non-compliant, it is advisable that information security measures, given the impact of more severe penalties, take advantage of this (Kishore et al., 2013). Second, for employees who tend to exhibit neither fully compliant nor non-compliant behavior, the use of threats of very likely formal sanctions is recommended, combined with the work of different sanction severities. Third, for all groups of employees' ISP compliance behavior tendencies, informal sanction certainty is effective in influencing ISP behavior rather positively. Security professionals should consider the benefits of informal sanctions when designing security measures for all groups of employees in the sense that they should emphasize the likelihood of informal sanctions occurring when conducting security training.

5.3. Limitations

Our research has some limitations that provide opportunities for further research. First, by choosing the U.S. as the research setting, the influence of cultural differences may affect our results. Our study design was exemplary because it allowed us to collect a dataset without large cultural differences. Recognizing that national culture influences ISP-compliance behavior, particularly in sanctions (Kuo et al., 2020; Trang and Brendel, 2019), more empirical research is needed to generalize our findings to other national cultures. Therefore, we would encourage further research to examine the role of cultural characteristics in our context. Second, we examined the effectiveness of sanctions on employees with different tendencies regarding ISP-compliance behavior. While our results show differences in the effectiveness of formal and informal sanction severity and sanction likelihood, we know that information security professionals cannot develop and implement specific security measures for each group of employees' ISP-compliance behavior tendencies. Therefore, future research should focus on defining an appropriate mix of security measures and, most importantly, addressing other contextual differences, such as different security offenses, as our study only measured and analyzed general ISP-compliance behaviors. Likewise, industry specifics and other moderating factors, such as age and work experience, should be considered.

6. Conclusion

Evidence of the effectiveness of sanctions in achieving ISP compliance behavior is diverse and exists in different cultural contexts and for different security breaches. Nevertheless, the effectiveness of sanctions is questioned due to heterogeneous results, and research calls for more nuanced approaches to consider this phenomenon. Our study used the quantile regression method to take a new perspective, using sanctions as a tool to ensure information security. We developed a theoretical model based on deterrence theory's most commonly used mechanisms in the field of ISP compliance behavior research and analyzed longitudinal data from 263 participants. We first determined the general influence of deterrence mechanisms on ISP compliance behavior and then used the heterogeneous responses of the participants to perform a quantile regression. We uncovered the effect of deterrence mechanisms on ISP compliance behavior in three different quantiles (0.25, 0.50, and 0.75 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 stricter ISP-compliant manner.

Our results show that the different sanctioning mechanisms analyzed perform differently in the quantiles considered. We identified that formal sanction severity and informal sanction certainty are more likely to work for employees with a rather non-compliant attitude than for employees with average compliance behavior, whereas formal sanction certainty is only applicable for employees with average behavior tendency. As this single study is the first step in the empirical investigation of deterrence theory 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 ISP-compliance behavior.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

CRediT authorship contribution statement

Sebastian Hengstler: Conceptualization, Methodology, Validation, Formal analysis, Writing – original draft. **Stephan Kuehnel:** Conceptualization, Writing – review & editing. **Kristin Masuch:** Conceptualization, Methodology, Validation. **Ilja Nastjuk:** Writing – review & editing. **Simon Trang:** Supervision, Writing – review & editing.

Data availability

Data will be made available on request.

Acknowledgment

The project on which this study is based was funded by the German Federal Ministry of Education and Research under grant number 16KIS1331.

References

Ahmad, Z., Ong, T.S., Liew, T.H., Norhashim, M., 2019. Security monitoring and information security assurance behaviour among employees. Inf. Comput. Secur. (27:2) 165–188.

Aurigemma, S., Mattson, T., 2017. Deterrence and punishment experience impacts on ISP compliance attitudes. Inf. Comput. Secur. (25:4) 421–436.

Aurigemma, S., Mattson, T., 2019. Generally speaking, context matters: making the case for a change from universal to particular ISP research. J. Assoc. Inf. Syst. 20 (12), 1700–1742.

Boichuk, J.P., Bommaraju, R., Ahearne, M., Kraus, F., Steenburgh, T.J., 2019. Managing laggards: the importance of a deep sales bench. J. Market. Res. (56:4) 652–665.

Chin, W., 2001. In: PLS-Graph User's Guide, 15. CT Bauer College of Business, University of Houston, USA, pp. 1–16.

D'Arcy, J., Herath, T., 2011. A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. Eur. J. Inf. Syst. 20 (6), 643–658.

D'Arcy, J., Hovav, A., 2009. Does one size fit all? Examining the differential effects of IS security countermeasures. J. Bus. Ethics (89:1) 59–71.

D'Arcy, J., Lowry, P.B., 2019. Cognitive-affective drivers of employees' daily compliance with information security policies: a multilevel, longitudinal study. Inf. Syst. J. (29:1) 43–69.

Gartner 2018. Gartner forecasts worldwide information security spending to exceed $124 billion in 2019. URL: https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwideinformation-security-spending-to-exceed-124-billion-in-2019 (Visited on October 30, 2021).

Gefen, D., Straub, D., 2005. A practical guide to factorial validity using PLS-graph: tutorial and annotated example. Commun. Assoc. Inf. Syst. (16) 91–109.

Gordon, L.A., Loeb, M.P., Zhou, L., 2011. The impact of information security breaches: has there been a downward shift in costs? J. Comput. Secur. (19:1) 33–56.

Guo, K.H., Yuan, Y., Archer, N.P., Connelly, C.E., 2011. Understanding nonmalicious security violations in the workplace: a composite behavior model. J. Manag. Inf. Syst. 28:2, 203–236.

Hair, J.F., Hult, G.T.M., Ringle, C.M., Sarstedt, M., 2017. A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM). SAGE, Los Angeles, London, New Delhi, Singapore, Washington DC, Melbourne.

Hair, J.F., Sarstedt, M., Pieper, T.M., Ringle, C.M., 2012. The use of partial least squares structural equation modeling in strategic management research: a review of past practices and recommendations for future applications. Long Range Plann. (45:5–6) 320–334.

Herath, T., Rao, H.R., 2009. Protection motivation and deterrence: a framework for security policy compliance in organizations. Eur. J. Inf. Syst. (18:2) 106–125.

Hovav, A., D'Arcy, J, 2012. Applying an extended model of deterrence across cultures: an investigation of information systems misuse in the U.S. and South Korea. Inf. Manag. (49:2) 99–110.

Jia, R., Steelman, Z.R., Reich, B.H., 2017. Using mechanical turk data in IS research: risks, rewards, and recommendations. Commun. Assoc. Inf. Syst. (41) 301–318.

Johnston, A.C., Warkentin, M., Siponen, M., 2015. An enhanced fear appeal rhetorical framework: leveraging threats to the human asset through sanctioning rhetoric. MIS Q. (39:1) 113–134.

Kishore, S., Rao, R.S., Narasimhan, O., John, G, 2013. Bonuses versus commissions: a field study. J. Market. Res. (50:3) 317–333.

Kuo, K.M., Talley, P.C., Huang, C.H., 2020. A meta-analysis of the deterrence theory in security-compliant and security-risk behaviors. Comput. Secur. (96) 2–10.

Li, M., 2015. Moving beyond the linear regression model: advantages of the quantile regression model. J. Manag. (41:1) 71–98.

Li, H., Sarathy, R., Zhang, J., Luo, X., 2014. Exploring the effects of organizational justice, personal ethics and sanction on internet use policy compliance. Inf. Syst. J. (24:6) 479–502.

Lindell, M.K., Whitney, D.J., 2001. Accounting for common method variance in cross–sectional research designs. J. Appl. Psychol. (86:1) 114–121.

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. J. Strat. Inf. Syst. (25:3) 232–240.

Lowry, P.B., Posey, C., Bennett, R.J., Roberts, T.L., 2015. Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: an empirical study of the influence of counterfactual reasoning and organisational trust. Inf. Syst. J. (25:3) 193–273.

Moody, G.D., Siponen, M., Pahnila, S., 2018. Toward a unified model of information security policy compliance. MIS Q. (42:1) 285–311.

Pahnila, S., Siponen, M., Mahmood, A., 2007. Employees' behavior towards IS security policy compliance. In: Proceedings of the 40th Annual Hawaii International Conference on System Sciences. Hawaii, USA.

Pratt, T.C., Cullen, F.T., Blevins, K.R., Daigle, L.E., Madensen, T.D., 2010. The empirical status of deterrence theory: a meta-analysis. In: Cullen, F.T., Wright, J.P., Blevins, K.R. (Eds.), Taking Stock: The Status of Criminological Theory. Transaction Publishers, Piscataway.

Robey, D., Boudreau, M.C., 1999. Accounting for the contradictory organizational consequences of information technology: theoretical directions and methodological implications. Inf. Syst. Res. (10:2) 167–185.

Siponen, M., Baskerville, R.L., 2018. Intervention effect rates as a path to research relevance: information systems security example. J. Assoc. Inf. Syst. (19:4) 247–265.

Siponen, M., Vance, A., 2010. Neutralization: new insights into the problem of employee information systems security policy violations. MIS Q. (34:3) 487–502.

Sommestad, T., Lundholm, J., Bengtsson, J., 2014. Variables influencing information security policy compliance: a systematic review of quantitative studies. Inf. Manag. Comput. Secur. (22:1) 42–75.

Trang, S., Brendel, B., 2019. A meta-analysis of deterrence theory in information security policy compliance research. Inf. Syst. Front. (6:21) 1265–1284.

Trang, S., Trenz, M., Weiger, W.H., Tarafdar, M., Cheung, C.M.K., 2020. One app to trace them all? Examining app specifications for mass acceptance of contact–tracing apps. Eur. J. Inf. Syst. (29:4) 415–428.

Vance, A., Siponen, M.T., Straub, D.W., 2020. Effects of sanctions, moral beliefs, and neutralization on information security policy violations across cultures. Inf. Manag. (57:4) 103–212.

Verizon Business 2022. 2022 data breach investigations report. URL: https://www.verizon.com/business/resources/de/T624/reports/2022-dbir-executive-summary.pdf (Visited on May 18, 2023).

Sebastian Hengstler is a Ph.D. student at Georg-August-University Göttingen, Germany, with a Master's degree in Business Informatics from the same institution in 2019. His-research interest is in the field of information security compliance behavior. His-research focuses on the analysis of cultural influences on factors explaining information security compliance behavior. In this context he is mainly concerned with differences in behavior based on national culture and the influence of culture on the individual level. His-work has been presented and published in conferences such as the *International Conference on Information Systems* and the *Hawaii International Conference on System Sciences*. In this context, he has also acted as a reviewer on several occasions. He has professional experience in the pharmaceutical and manufacturing industries, mainly in data management and strategic IT management.

Stephan Kuehnel is a project manager and postdoctoral researcher at the Institute of Information Systems and Operations Research at Martin Luther University Halle-Wittenberg. There, he earned his Ph.D. in Business Informatics focusing on approaches for the economic assessment and analysis of business process compliance. His-research interests are mainly in compliance and information security management as well as in current challenges of design science and data science projects. His-research has been published in journals such as *ACM Computing Surveys* and *Journal of Decision Systems*, as well as in peer-reviewed conference proceedings such as the *European Conference on Information Systems* and the *International Conference on Conceptual Modeling*.

Kristin Masuch is a Postdoctoral Researcher at the University of Goettingen, Germany. She earned a Ph.D. in Information Systems specializing in Information Security and Compliance from the University of Goettingen. Her research interests include the field of security crisis response strategies and research on the workplace's information security behavior. Her research focuses mainly on investigating the influencing factors and response strategies after a data breach occurs. In this context, she considers the effects on the customer reaction, but also on the market value of the affected company. She also investigates ways to influence employees' information security behavior to avoid crises such as data breaches. Her work has been published in outlets such as Electronic Markets, Computers & Security, and at international conferences such as ICIS, and others.

Ilja Nastjuk is a Postdoctoral Researcher at the University of Goettingen, Germany. He earned a Ph.D. in Information Systems from the University of Goettingen and a Ph.D. in Accounting and Corporate Governance from Macquarie University. His-research interests span the influence of technology on stress and human behavior, the adoption of self-driving cars, and information security management. His-work has been published in numerous peer-reviewed journals and conference proceedings, such as European Journal of Information Systems, Computers & Security, Technological Forecasting and Social Change, Electronic Markets, Transportation Research Part D: Transport and Environment, Transportation Research Part F: Traffic Psychology, and International Conference on Information Systems.

Simon Trang is Professor for Information Systems, esp. Sustainability at the University of Paderborn. He received his Ph.D. in management science, specializing in management information systems, from the University of Goettingen. His-work focuses on information security management, privacy, and sustainable IS. His-research has been published in outlets such as the *Journal of the Association for Information Systems, European Journal of Information Systems, Information Systems Frontiers*, and others.