Information & Management 58 (2021) 103318

Contents lists available at ScienceDirect

Information & Management

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

The role of deterrability for the effect of multi-level sanctions on information security policy compliance: Results of a multigroup analysis

Lennart Jaeger [a,*], Andreas Eckhardt [b,c], Julia Kroenung [a]

[a] EBS University of Business and Law, Department Management and Economics, Rheingaustraße 1, 65375, Oestrich-Winkel, Germany
[b] German Graduate School of Management and Law, Bildungscampus 2, 74076, Heilbronn, Germany
[c] University of Innsbruck, Faculty of Business and Management, Universitaetsstraße 15, 6020, Innsbruck, Austria

ARTICLE INFO

Keywords:
Information security policy compliance
Attitude
Deterrence
Sanctions
Deterrability
Information security policy awareness

ABSTRACT

This paper offers a new perspective on the effectiveness of sanctions in influencing information security policy compliance. We observe compliance from a group perspective to identify undeterrable employees who comply based on inner conviction and deterrable employees who comply because of external coercion. Drawing upon survey data, we show that multilevel sanctions (i.e., formal, social, and personal sanctions) have a varying impact on the compliance of inclined and disinclined employees. We also find that multilevel sanction perceptions are differently influenced by information security policy awareness. This group-based deterrability perspective opens up new avenues to study the value of sanctions.

1. Introduction

Although external factors (e.g., hackers and malware) constitute a considerable threat to an organization's information security, employees' actions are often considered a higher security risk [1]. A key instrument to reduce information security threats associated with such employees is to create, deploy, and enforce information security policies. These policies specify the employees' roles and responsibilities in properly using and protecting organizational information systems (IS) resources [2,3]. However, it is widely reported that many employees do not comply with these policies or intentionally bypass them [4]. While employees typically do not want to harm their organization, in most cases they are not sufficiently motivated to comply with policies [4]. Specifically, in today's digitally driven world in which speed, productivity, and adaptability are driving and defining employees' capabilities to be faster and more efficient, employee behavior is often characterized through accessing or using external systems that did not get prior approval from the Information Technology (IT) department [5]. One such example is public cloud systems, such as Dropbox, which are used by many employees to save and share company data without the consideration of organizational information security policies [5]. A recent survey by Oracle and KPMG showed that over 93 % of the responding organizations deal with employees using unsanctioned personal devices and storage or file share software for corporate data [6]. The largest IT practitioner leadership survey in the world also detected the unstoppable rise of technology expenditure controlled outside the IT department, as almost two-thirds of those organizations that completely disallow business-managed IT still reported its existence [7]. As many organizations surveyed referred to a lack of security controls and misconfigurations as common reasons for data breaches, more than every fourth organization regards the unauthorized use of cloud services as their biggest challenge for information security [6]. In addition to exposing the organization to considerable security threats, with 1 in 4 having already experienced data theft from the public cloud [8], using such systems may also have legal implications. Many public cloud services do not meet regulatory requirements of data sovereignty as mandated by external regulations, such as the European Union General Data Protection Regulation (GDPR) [9]. Against this backdrop, it is important to ensure that the cloud services used by employees are compliant with internal and external regulations and do not expose the organization or its employees to risk.

To understand employees' conduct, behavioral information security research has focused on examining the influence of formal sanctions (e.g., fines, wage cuts, or negative performance reviews) [10] expected to encourage/discourage employees' information security policy compliance/noncompliance [11], principally taking the theoretical perspective of deterrence theory and extensions thereof [12]. However, the results of these sanctions have been inconsistent and sometimes

* Corresponding author.
E-mail addresses: lennart.jaeger@ebs.edu (L. Jaeger), andreas.eckhardt@ggs.de (A. Eckhardt), julia.kroenung@ebs.edu (J. Kroenung).

https://doi.org/10.1016/j.im.2020.103318
Received 26 January 2018; Received in revised form 7 April 2020; Accepted 12 April 2020
Available online 17 May 2020

contradictory, especially when other factors such as informal sanctions (e.g., social disapproval and self-disapproval) are considered [12]. Building on the learnings of the criminology literature, we believe the discrepancies between findings in prior studies might be cleared up by paying closer attention to the potentially moderating role of employees' sanction expectations, i.e., the effect of formal and informal sanctions may not be homogeneous across employees [12] and that deterrence also in particular depends on potential offenders to be deterrable [13]. Deterrence refers to the perceptual process where individuals weigh the risks and rewards to determine whether to offend, while the capacity or willingness of the potential noncomplier to engage in this calculation refers to individuals' deterrability [14].

As long as 50 years ago, research in criminology criticized that few approaches remarked that the effectiveness of deterrent measures are related to the class of persons and thus their differential deterrability [15]; still little can be said about how individuals perceive and respond to formal sanctions [13]. One of the few scholars to explicitly address this issue was Pogarsky [14, p. 432] who stated that "*punishment threats are consequential only for a subgroup of the general population.*" Till this day, group-based approaches to investigating deterrability are still rare in the criminology field, and nonexistent in information security research. It is not well understood how awareness and perceptions are affected by sanction threat responsiveness, and thus deterrability [16]. Research shows that policies can manipulate sanction threat perceptions [17]. Whether the policy affects individuals' threat perceptions also depends on their attitudes toward the policy. These attitudes need to be distinguished from attitudes toward risk [18], which are more related to the consequences of a policy violation than the policy itself. Thus, it is of particular importance to observe exclusively how attitudes toward policies, which implicitly include an assessment of their perceived justness [19] and their creator [20,21] influence employees' deterrability.

An important step in the organizational process toward becoming compliant and avoiding the potential risk of breaching external regulations involves ensuring that employees are aware of the organization's policies, practices, and procedures. Accordingly, employees' awareness of and compliance with cloud usage policies is among the top concerns of information security managers [22]. But as several groups of employees in today's organizations tend to bypass policies and use unapproved technologies, it is very important to examine how formal and informal sanctions affect the groups of employees who are (dis)inclined to comply and how their attitude toward such policies affects their deterability in this regard.

Therefore, we apply a group-based approach as proposed and implemented by Pogarsky [14], and investigate employee deterrability by examining whether the effect of formal, social, and personal sanctions on information security policy compliance differs depending on the degree to which employees have a positive or negative attitude toward the organization's security policies. Thus, within this research, we address the following research question: *What is the role of employees' deterrability in the relationship between multilevel sanctions and information security policy compliance?*

We test our research model empirically using a survey on information security policy compliance related to the usage of public cloud services at work. We survey 311 employees in the public sector who are regulated by their organization's information security policies, as well as the GDPR, but work in an environment where peers tend to frequently circumvent these policies [23–25]. Partial least squares multigroup analysis (PLS-MGA) is employed to test the moderating effects on the relationships. Our study contributes to the literature on employees' information security policy compliance by introducing the concept of deterrability. In particular, we confirm the role and importance of deterrability in behavioral information security studies by providing evidence that the effect of formal, informal social, and personal self-sanctions largely depends on employees' attitude toward information security policies. Specifically, based on our group-based approach, we find that different groups of employees adhere to the policies in their public sector organization. *Inclined compliers* (i.e., employees with a positive attitude who subsequently comply) are undeterrable in the sense that they are insensitive to formal sanctions as they comply out of inner conviction, whereas *disinclined compliers* (i.e., employees with a negative attitude who comply nevertheless) are deterrable. We also find that information security policy awareness has a stronger association with personal self-sanctions for inclined employees and partially a stronger association with formal and social sanctions for disinclined employees. This group-based perspective focusing on individuals' deterrability opens new avenues to examine the value of formal, informal social, and personal self-sanctions in security management and provides insight into the inconsistent results of prior deterrence-related information security research [12].

2. Research background

2.1. Deterrence and deterrability

Deterrence deals with how sanction threats inhibit criminal or deviant behaviors such as disobedience of rules and policies. Deterrence is commonly accepted to be a perceptually based phenomenon because individuals must perceive sanction threats to be affected by them [26–28]. Thus, in deterrence research, the perceptual states of sanctions are typically measured [12]. Accordingly, classic deterrence theory concentrates on formal sanctions that are presumed to deter crime to the extent that as an individual's perceived certainty and severity of punishment increases, the probability of committing the corresponding act decreases [29]. Contemporary deterrence theory extended the classic framework by accounting for the role of informal sanctions such as expected social disapproval and self-disapproval as extralegal sources of compliance [30,31]. There has been a plethora of empirical research on the key aspects of deterrence theory, and there are exhaustive reviews in both the criminology [30] and information security [12] fields. One key finding is that the effect of sanctions on compliant behavior is not one-size-fits-all. Instead, it is imperative to acknowledge the differential deterrability present across different individuals regarding sanction threats [32].

Among the scholars that explicitly examine deterrability, Pogarsky [14] defined deterrability as responsiveness to sanction threats and classified individuals into one of three types of decision makers: acute conformists, deterrables, and incorrigibles. *Acute conformists* and *incorrigible offenders* are two distinct types of individuals who are insensitive to formal sanctions, while *deterrables* are individuals whose responsiveness to formal sanctions is between the two extreme ends. Acute conformists are those for whom informal influences, such as social disapproval and self-disapproval, already ensure compliance. The incorrigibles are individuals for whom formal sanctions are inconsequential, because they are committed offenders impervious to dissuasion. The deterrables are neither strongly committed to conformity nor deviance and as punishment certainty and/or severity increases, they become less likely to offend [14].

Policies have the ability to influence individuals' sanction threat perceptions [17]. However, this strongly depends on an individual's attitude toward both the policy and the risk to violate it [18,20,21]. Thus, in the next subsection, we develop an attitude-compliance matrix highlighting individuals' deterrability based on their information security policy compliance, as well as their attitude toward their organization's information security policy.

2.2. Disinclined and inclined compliers

In the information security context, policies are one of the key objects to which attitudes and behaviors are directed [33]. In line with Eagly and Chaiken [34], employees' *attitude toward information security policies* describes their evaluative tendency concerning the information

security policies of their organization and how favorably or unfavorably they view such policies. We refer to an attitude toward information security policies as an attitude toward an object, as defined by Zhang et al. [35] and Zhang and Sun [36], and conceptually distinct to an attitude toward behavior, which is an attitude toward behaving compliant in our case. Zhang et al. [35] and Zhang and Sun [36] demonstrate that there are different statistical effects for those different conceptualizations of attitude. Safa et al. [37], for example, highlight the importance of policy attitudes with regard to compliance behavior. However, Safa et al. [37] do not conceptually distinguish between attitude toward policies and attitude toward compliant behavior (see [35]). A positive attitude, for instance, can be the cause of a high degree of identification with the organization itself [38,39] or a general agreement with the information security policies [40]. In contrast, a negative attitude toward information security policies, by contrast, can be the cause of the general belief that they are used by the IT department to control the way employees do their information-related work [33].

With regard to the understanding of deterrability based on employee attitudes toward information security policies and information security policy compliance, we employ a group-based approach as done by Pogarsky [14] in criminology research. Thus, our structured analysis examines the attitude-behavior relationships of employees as it relates to their inclinations and subsequent actions. This approach has also been adapted in other IS contexts [41].

In our study, we observe information security policy compliance aligned with positive and negative attitudes to yield compliance inclination (i.e., attitudinally controlled intentions based primarily on an employee's attitude toward information security policies). We employ this perspective to gain a more detailed view on the deterrability implications for two groups: inclined and disinclined compliers. Further, by defining attitude as the distinguishing variable in line with previous research [41], we avoid nonlinearity problems between attitude and norm constructs as identified by Titah and Barki [42] if those two constructs are modeled as equal determinants of behavior.

Inclined compliers are employees with positive attitudes toward information security policies who comply with these policies. They are convinced of the justness and usefulness of their organization's security policies, and are willing and able to translate them into policy-consistent behavior. They adhere to these security policies either because they assess the policies' goals and intentions as positive and thus share them (private acceptance, cf. [43]), or even make them their own (mandatory) goals and thereby internalize them (internalization, cf [38].). Employees will only view the security policy-related prohibitions and requirements as not mandatory, and affirm them by free will if they consider them appropriate. In this case, compliance leads to satisfaction, and thus has a self-reinforcing character. This individual behavior requires little or no formal sanctioning system, as individuals mainly seek to comply out of "inner conviction" regardless of the expectation of consequences. Thus, inclined compliers represent one form of undeterrability (i.e., insensitivity to formal sanction threats). They comply because they believe that it is the right thing to do and not because they fear sanction threats. Similar to Pogarsky's [14] "acute conformists," inclined compliers are not susceptible to formal sanctions as they would not violate the policies even if there were no more formal sanctions.

Disinclined compliers are employees who comply with information security policies even though they have negative attitudes toward them. These are employees for whom a sanction threat is potentially influential. Similar to Pogarsky's [14] "deterrable offenders," disinclined compliers would typically violate information security policies if not for the threat of punishment. They comply because of external pressures without necessarily sharing the policies' underlying objectives and intentions. Their reasons for compliance lie therefore in the (expected) unfavorable consequences of noncompliant behavior (i.e., fear of formal/informal sanctioning). In other words, they comply with security policies to avoid punishment, but do not privately accept them. For this group, formal sanctioning systems are effective, including high detection certainty and severe punishment violations. In a social sanctioning system, employee behavior is partially shaped by the approval or disapproval of significant members of the employee's business social network (e.g., peers or team leaders) and sanctioning is often informal. If sanctioning fear declines because of a lack of surveillance or social pressure, compliance levels will likely decline because employees will act in accordance with their own negative attitudes toward these policies.

We expect that most employees are not "in the market" for serious, violating behavior and they are inclined compliers when serious system abuses are under consideration. Yet, when minor policy violations (e.g., password write-down, failure to logoff, or using public cloud services) are concerned, more people are in the margin for these kinds of behaviors and could actually be deterrable. The problem is usually not that employees are incorrigible offenders [14] who intend to harm their organization, but rather that they are not sufficiently motivated to comply with information security policies [4]. Hence, researchers and practitioners are faced with the important question of how employees can be motivated to engage in good security-related behaviors [2,44]. Against this background, deterrence studies that employ positive outcome variables such as security policy compliance have generally shown a weak deterrent effect for sanctions compared to negative outcome variables such as IS misuse [12]. Accordingly, some scholars have questionned the suitability of the deterrence theory for predicting positive user behavior and call for further research to clarify this issue [12]. We respond to this call by examining inclined and disinclined compliers to identify subgroups of employees for which sanctions can promote desirable compliance and for which subgroups they might be ineffective.

3. Research model and hypotheses

In this section, we present our research model and discuss our hypotheses. Drawing on the conceptualization of (dis)inclined compliers derived in the preceeding section, we hypothesize that there are differences in the effect of externally imposed motivating factors (formal and informal social sanctions) and self-imposed motivating factors (personal self-sanctions) on information security policy compliance among employees with a positive or negative attitude toward information security policies, $ß_1$ and $ß_2$, respectively. We also hypothesize that employees' multilevel sanction perceptions are influenced by their information security policy awareness. Fig. 1 presents our research model.

In line with prior research [12,45], we define *information security policy compliance* as the extent to which employees follow these organizational policies to appropriately use IS in their job. Organizational security policies refer to formalized guidelines on employees' roles and responsibilities in properly using and protecting organizational IS resources [2,3] and tend to rely heavily on rigid industry and/or governmental regulations [46]. Therefore, examining an insider's information security policy compliance can result in an assessment of an employee's adherence to the formally specified roles and responsibilities in these policies [46]. In our study, we focus on information security policies regarding public cloud use as one type of information security policy. By using public cloud systems (e.g., Dropbox) without formal IT department approval, employees often violate their organization's information security policy [5]. Both scholars [5] and practitioners [8] consider this violation as an information security concern for organizations that brings important information security threats such as data theft or regulatory compliance violations. In the following subsections, we detail the model constructs and describe their hypotheses.

3.1. Formal sanctions

Formal sanctions represent explicit penalties (e.g., fines, wage cuts, or negative performance reviews) resulting from certain forms of noncompliance [47]. For example, storing organizational documents on

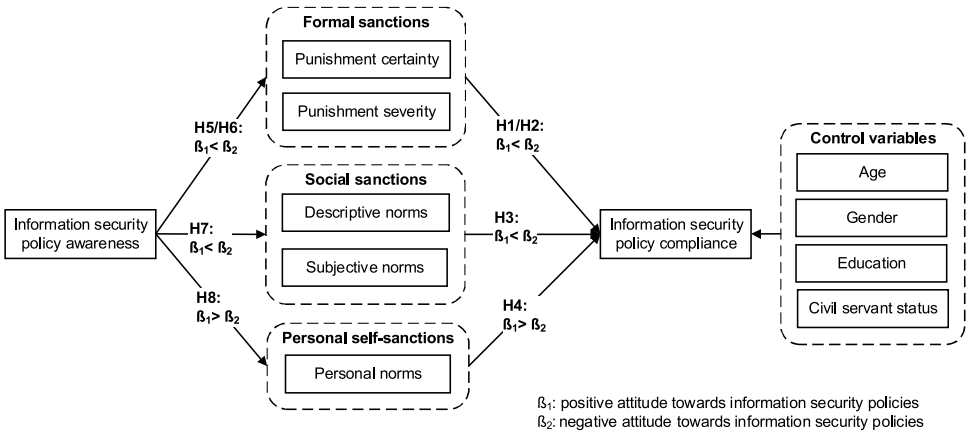

Fig. 1. Research model.

unauthorized external cloud systems could get employees fired [48]. Criminology research on deterrence has conceptualized formal sanctions as the perceived severity and certainty of punishment, which, in an organizational context, has been reframed and adapted to getting caught and punished for prohibited workplace behavior [49]. Despite the strong theoretical grounding of deterrence theory in criminology and empirical support in organizational environments [30,31], information security literature has produced mixed findings when explaining user behaviors that are either supportive (e.g., information security policy compliance) or disruptive of information security (e.g., IS misuse) [12, 50]. Some studies provide empirical support for fundamentals of deterrence theory (e.g. [51],), while others report only partial support (e.g. [52,53],). Despite partially contradictory findings within the information security field, the deterrence theory is considered a widely accepted theory, and examining the reasons why deterrent measures do not function as well as they should is considered an important endeavor [33]. Thus, in accordance with extant studies, we apply (perceived) *punishment severity* and *punishment certainty* as components of formal sanctions for engaging in noncompliant behavior.

While the majority of studies in behavioral information security have not addressed the issue whether the deterrent effect of formal sanctions may not be homogeneous across employees, criminology research findings indicate that the impact of sanctions varies among individuals [30,54]. Empirical findings on tax compliance, for instance, suggest that formal sanctions have a greater deterrent effect on tax cheating among individuals who have a negative attitude toward tax laws, and are thus presumably more motivated to cheat [55]. Thus, in line with our conceptualization of *disinclined compliers* in Section 2, we assume that formal sanction expectations are central to information security policy compliance when employees have a negative attitude toward these policies and comply because of the fear of formal sanctions for noncompliance. For example, when employees anticipate that the severity and certainty of punishment for using public cloud services will be high, they will comply with policies for cloud use despite their disinclination to do so to avoid the conseqeuences. Hence, we hypothesize:

H1. Punishment certainty has a greater effect on information security policy compliance for disinclined employees than for inclined employees.

H2. Punishment severity has a greater effect on information security policy compliance for disinclined employees than for inclined employees.

3.2. Social sanctions

In addition to formal sanctions, contemporary deterrence studies have also recognized the role of the socially mediated consequences of actions or, in other words, informal social sanctions [30]. From a deterrence point of view, the subjective value of the individually anticipated consequences of actions is not solely influenced by formal sanctions (e.g., fines), but also by informal social sanctions [31]. One example of informal social sanctions is social disapproval, which includes the condemnation by people whose opinions the individual values [56]. In an organizational context, this could be negative feedback received from peers or leaders for violating information security policies. Negative reactions of significant members in a social network to noncompliance increase the psychological costs of noncompliance, thereby reducing its attractiveness [57]. If social norms are defined as (mostly implicit) rules and standards on how to behave [34], it is clear that they can regulate behavior in different ways, although they are not expressed as formal laws or decrees. Social norms include an evaluating component in the form of social sanctioning through approval or reward and rejection or punishment.

There are two primary types of social norms [58]: descriptive and subjective. *Descriptive norms* offer information about what appears to be the most appropriate behavior based on one's own perception of how others in similar situations behave. *Subjective norms*, on the other hand, specify how employees ought to behave on the basis of their expectations of what significant members of their professional social network (e.g., peers and supervisors) would approve or disapprove of. Descriptive norms represent important social information in (uncertain) situations, while subjective norms describe the normative rules of a group-regulating behavior through a social process by either promising a reward (social approval) or punishment (social disapproval) [59]. The influence of social norms on information security policy compliant and noncompliant behavior has been documented in several studies [53,58, 60].

In mandatory settings, in which policies mandate how the focal system should or should not be used, social norms have been shown to impact system usage decisions predominantly through a compliance mechanism rather than internalization or identification [61]. While internalization and identification are associated with the alteration of an individual's belief structure, the compliance mechanism causes employees to alter their behavior simply in response to social pressure, i.e., employees comply with the social norm, especially when significant social network partners are able to reward desired or punish undesired behavior [62]. Drawing on our argumentation of disinclined compliers in section 2, we argue that informal social sanction expectations inherent in social norms and operationalized through subjective and descriptive norms are central to information security policy compliance when employees have a negative attitude toward information security policies. That is, when employees perceive that no one else uses unauthorized public cloud services to store organizational data and that

coworkers or others expect the individual to comply with organizational policies for cloud use, they will comply with the policy despite their disinclination in an effort to avoid social disapproval (e.g., negative feedback). Thus, we hypothesize:

H3. Social norms have a greater effect on information security policy compliance for disinclined employees than for inclined employees.

3.3. Personal self-sanctions

While employees might be aware of a norm and even believe that it is a social norm being held by others and associated with societal rewards and punishments, they might have little personal attachment to it. Thus, it is necessary to consider the degree to which an external norm is also a *personal norm*, i.e., a norm that is connected with an individual's self-concept and experienced as feelings of moral obligation to perform or refrain from certain behavior [63]. In contrast to social norms being enforced through social disapproval, the enforcement of personal norms occurs through self-disapproval, which emanates from within. Self-disapproval encompasses "the belief in the legitimacy of the law, moral commitment to a legal norm, internalization of norms, and conscience" ([64, p. 432] as cited in [14]). In an organizational context, this could involve an employee believing that the violation of information security policies is a serious matter or unacceptable to him or her. It follows then that certain acts of noncompliance are not committed because they are believed to be wrong [30]. Findings in criminology studies indicate that personal norms or moral standards strongly determine an individual's intention to perform illicit behavior, such as corporate crimes [31] or tax evasion [56]. Although personal norms have not received wide attention in research on behavior that is supportive of information security, a few studies have shown that personal norms positively impact information security policy compliance intentions directly [65] or indirectly through attitude toward security-related behavior [66,67].

Thus, when information security policies are internalized as part of an employee's moral reasoning, they may feel more obligated to translate them into information security policy-consistent behavior. In line with our conceptualization of inclined compliers, we expect the congruence between information security policies and an employee's moral values [31] to be stronger for employees with a positive attitude toward information security policies. For example, when employees consider violating cloud use policies by saving work-related documents in public cloud systems to be a serious matter or unacceptable, they will comply with the policy in line with their inclination and to avoid self-disapproval. Thus, we hypothesize:

H4. Personal norms have a greater effect on information security policy compliance for inclined employees than for disinclined employees.

3.4. Information security policy awareness

Information security policy awareness is defined as an employee's knowledge and understanding of the requirements prescribed in the organization's information security policies and the aims of those requirements [2]. This definition is based on the notion that awareness is a state in which an employee is aware of and ideally committed to the organization's information security objectives as often expressed in information security policies [68]. We propose that information security policies serve as an important informational basis influencing employees' multilevel sanction perceptions.

First, information security policies rely on the same deterrent mechanism as societal laws by providing information as to what is undesirable behavior and increasing sanction threat perceptions for such behavior [52,69]. In particular, employees' awareness of information security policies increases perceived punishment certainty, because policies imply the existence of enforcement through organizational security efforts (e.g., monitoring and detection activities), and perceived punishment severity, because policies suggest that penalties will be imposed for policy violations [52].

Second, information security policies may shape policy-related social norms within an organization. An organization developing and implementing information security policies signals expectations to employees through various channels such as security education, training, and awareness programs to ensure information security policy awareness and compliance [70]. Such expectations influence employees' norms regarding information security policies. For instance, employees who perceive that their organization generally values rule-following behavior as indicated by its information security policies, they more likely believe that the majority of their peers either comply with said policies or expect them to comply [71]. Thus, the awareness of information security policies helps to provide relevant ideas about descriptive and subjective norms.

Third, information security policies represent some kind of organizational imperative that also includes commitment and internalization [68]. Organizations want their employees to internalize and follow information security policies instead of just knowing but failing to apply them. Information security policy-aware employees would see a policy as something they are obliged to follow. This commitment can be an external or internal motivation [68]. This obligation belongs to the category of role responsibility and/or moral responsibility [68,72]. Role responsibility differs from the feelings of moral obligation (or personal norm, see previous section). Responsibility relates to an employee's organization duties, such as considering oneself to be responsible for enhancing the organization's information security. Moral obligation, on the other hand, is concerned with an employee's feeling that he/she should act in line with his/her value system, such as considering oneself morally obligated to information security policy compliance because rule-following is part of one's value system [71]. Yet, the degree of feeling morally obligated is also a function of responsibility [63]. Thus, personal awareness of information security policies prescribing one's responsibility leads to the formation of policy-related personal norms.

On the one hand, employees with a positive attitude toward information policies (inclined employees) regard such policies as acceptable and desirable and, thus, are more likely to acknowledge the link between feeling responsible for enhancing their organization's information security and feelings of moral obligation toward information security policy compliance. Hence, a positive attitude toward information security policies facilitates a successful transition of information security policy awareness to policy-related personal norms.

On the other hand, an employee with a negative attitude toward information security policies (disinclined employee) has assessed their goals and intentions as negative and, thus, does not share or privately accept them. Such a negative attitude allows an employee to justify the denial of responsibility to disregard their moral obligation [73]. Therefore, a negative attitude inhibits the transition of information security policy awareness to policy-related personal norms. In such a case, their commitment remains external as a form of motivation to comply [68]. Their sense of role responsibility would be channeled through the perceived risk of formal sanctions and informal (social) sanctions when not acting in line with their formally required or socially expected role. Accordingly, they would consider information security policies more as the basis of external role performance evaluations linked to rewards and punishments (tangible or social) as opposed to internal feelings of shame or disapproval. In other words, disinclined employees would be more receptive to the message inherent in a cloud use policy that there will be sanctions and others will disapprove of noncompliance than inclined employees. Thus, we propose:

H5. Information security policy awareness has a greater effect on punishment certainty for disinclined employees than for inclined employees.

H6. Information security policy awareness has a greater effect on

punishment severity for disinclined employees than for inclined employees.

H7. Information security policy awareness has a greater effect on social norms for disinclined employees than for inclined employees.

H8. Information security policy awareness has a greater effect on personal norms for inclined employees than for disinclined employees.

3.5. Control variables

Following the information security literature, we include several control variables in the research model. These variables include individual differential factors, such as *age* [52], *gender* [58], *education* [74], and *civil servant status*.

4. Research methodology

We conducted a survey to test the hypotheses. For the pilot survey, we first identified and developed suitable measures based on the literature. We conducted the pilot survey with several target audience members and then refined our final survey, which was administered online. In the following subsections, we discuss the instrument development and describe the data collection process.

4.1. Instrument development

The measurement items of the constructs are based on the extant literature to improve the reliability of the results. Table 1 presents the operationalization of the items. Items to capture formal sanctions (operationalized by punishment severity and punishment certainty) and informal social sanctions (operationalized by subjective and descriptive norms) were adapted from Herath and Rao [58]. Items to capture personal self-sanctions (operationalized by personal norms) were adapted from Ifinedo [66]. Items to capture information security policy awareness were adapted from Bulgurcu et al. [2]. Although many studies use behavioral intention as the endogenous variable, we consider self-reported behavior instead as it is often easier to self-assess than intention [75]. Some empirical studies (e.g. [76,77],) chose this approach by inquiring about employees' information security policy compliance. Thus, the two items to capture information security policy compliance measured the employees' degree of policy compliance with respect to public cloud system use at work. For each of these items, respondents assessed the extent of their agreement/disagreement using a seven-point Likert-type scale, ranging from strongly disagree (1) to strongly agree (7). The item information security policy attitude that was used to split the sample into two groups measured respondents' attitudes toward a target as defined by Eagly and Chaiken [34], specifically toward the policies on the use of public cloud services, ranging from very negative (1) to very positive (7). The object of the measure is concrete singular, meaning that it consists of one object, here the public cloud policy, which is easily and uniformly imagined, thereby supporting the use of a single item measure versus a multiple-item measure [78]. The two groups were split midway on the neutral position (4) of the seven-point scale.

4.2. Data collection

The survey was conducted among employees in public state-funded universities in Germany with regard to compliant behavior related to the usage of cloud services. University employees are employed by the state and thus a part of the public sector, which has strict privacy regulations with the intention to protect its citizens. Furthermore, employees are subject to data protection laws and the universities' central data protection authority prohibits the use of public cloud storage services such as Dropbox on the grounds of information security and privacy concerns. A web-based survey was conducted to collect data and the corresponding link was distributed to employees of state-funded universities through email. In return for participation, which was entirely voluntary and anonymous, five vouchers for online retailers were raffled among people who completed the survey and opted to participate in the lottery. As our aim in this study is to explore individuals with differing attitudes toward information security policies, our sample consists of 311 participants with either a positive or negative

Table 1
Measurement items.

Item		Scale[a]	Mean	SD
Descriptive norms (DN)				
DN1	I believe other employees comply with the policies for public cloud use and do not use services like Dropbox for work-related data.	A	2.95	1.77
DN2	I am convinced that other employees use public cloud services, such as Dropbox, at work.	B	2.83	1.78
DN3	It is likely that the majority of other employees comply with the policies for using public cloud services and do not use services like Dropbox to ensure data security and protection.	A	3.23	1.76
Information security policy attitude (ATT)				
ATT1	I feel … about the policies for the use of public cloud services at work.	C	3.84	1.74
Information security policy awareness (ISPA)				
ISPA1	I know the rules and regulations prescribed by the policies for public cloud use of my organization.	A	3.23	1.78
ISPA2	I understand the rules and regulations prescribed by the policies for public cloud use of my organization.	A	2.64	1.48
ISPA3	I know my responsibilities as prescribed in the policies for public cloud use to enhance the information security of my organization.	A	1.77	1.11
Information security policy compliance (ISPC)				
ISPC1	I comply with the policies for public cloud use at work.	A	4.58	1.81
ISPC2	I adhere to the policies regarding public cloud use at work by not saving work-related documents in public cloud services (e.g., Dropbox or similar).	A	4.14	1.94
Personal norms (PN)				
PN1	It is a serious matter if I do not comply with the policies on cloud service use and to save work-related documents in public cloud services.	A	4.79	1.84
PN2	To me, it is unacceptable to ignore my organization's policies on public cloud service use.	A	4.64	1.93
PN3	To me, using public cloud services (e.g., Dropbox) is a trivial offence.	B	3.95	1.87
Punishment certainty (PC)				
PC1	The probability that I would be sanctioned for violating public cloud service policies is low.	B	2.59	1.42
PC2	It is unlikely that using public cloud services would be detected.	B	2.54	1.39
PC3	My organization monitors compliance with the policies for cloud usage.	A	3.13	1.76
Punishment severity (PS)				
PS1	I would be disciplined if my organization knew about my behavior.	A	3.45	1.53
PS2	My organization punishes employees who break the policies for using cloud services.	A	2.8	1.34
PS3	Offenses such as using public cloud services (e.g., Dropbox, Microsoft OneDrive, and Google Drive) for work-related data would not be punished at my organization.	B	3.31	1.75
Subjective norms (SN)				
SN1	My boss thinks that I should comply with the policies for using cloud services.	A	5.11	1.79
SN2	My colleagues think that I should comply with the policies for using cloud services.	A	4.36	1.82
SN3	The IT department in my organization thinks that I should comply with the policies for using cloud services.	A	3.72	1.99

[a] A: ranging from 1 = strongly disagree to 7 = strongly agree; B: like A, but items are reverse coded; C: ranging from 1 = very negative to 7 = very positive.

attitude toward information security policies. As the mean of attitude is 3.84 (SD 1.74), this suggests that the participants have a slight tendency to possess negative attitudes toward these policies, indicating their disinclination to comply. The attitude scale is approximately symmetric with a skewness value of 0.03 (SD 0.13), but has a negative kurtosis value of -1.03 (SD 0.26), which indicates a heterogeneous distribution of our sample and emphasizes the need to conduct group-specific analyses.

Table 2 presents the demographic characteristics of our two groups: the positive information security policy attitude group and the negative information security policy attitude group. Of the participants, 99 (31.7 %) were female and 209 (67.0 %) were male. Most respondents were between 22 and 40 years of age (71.4 %). The majority of participants held a university degree (81.7 %), did not have civil servant status (84.0 %), and worked in an academic department at their institution (82.7 %). Their average years of employment at their institution was 5.17 years (SD = 6.21 years).

5. Data analyses and results

In our data analysis, we employ the Partial Least Squares (PLS) approach, which is a common regression technique for measuring both measurement and structural models [79]. PLS yields solid results for small sample sizes and can be used to test and validate explanatory models [79]. To test our hypotheses, we measured the differences in the path coefficients of the two groups of employees with either a positive or negative attitude by conducting a bootstrap-based PLS multigroup analysis [80] using SmartPLS version 3 for PLS path modeling. Initially, the reliability and validity of the measurement models of both groups were assessed followed by an evaluation of the structural models for hypotheses testing.

5.1. Measurement model testing

To assess the measurement model, we examined construct reliability, indicator reliability, convergent validity, and discriminant validity. The results are presented in Table 3. Construct reliability was assessed using composite reliability (CR) scores [81]. The CR values range from 0.7 to 0.96, which exceeds the recommended threshold of 0.7 [81]. Indicator reliability was assessed by checking the construct loadings of each indicator. Loadings above the threshold value of 0.6 ensure sufficiently high indicator reliability [82]. To assess convergent validity, we calculated the average variance extracted (AVE) [83]. The AVE of each latent variable ranges from 0.55 to 0.92, which is above the recommended threshold of 0.5. For the assessment of discriminant validity, we considered the Fornell-Larcker criterion and cross-loadings [81,82], as well as the recently proposed heterotrait-monotrait ratio (HTMT) test [84]. As shown in Table 3, the square root of the AVE of every construct is higher than the correlation coefficients among the constructs [81,83]. Further assessment using the cross-loadings confirms the results of the analysis of the Fornell-Larcker criterion, as all indicators load higher on their respective construct than on other constructs. In addition, the stricter HTMT ratio demonstrates discriminant validity, as all the HTMT values of our constructs are smaller than 0.9 [84,85] and significantly different from 1 as per the statistical test for HTMT inference (i.e., neither of the confidence intervals derived through bootstrapping included the value 1 [84]). Thus, the three criteria for discriminant validity are satisfied, indicating that our measurements of all constructs in the model are distinct from each other.

Finally, to assess common method variance (CMV), we used the marker-variable technique [86,87]. We selected respondents' personal innovativeness, which was measured with three items taken from Agarwal and Karahanna [88], as the marker variable and its average correlation with other variables in the study ($r_M = 0.098$ and $r_M = 0.095$ for the positive and negative information security policy attitude group, respectively) was used as the CMV estimate. We calculated CMV-adjusted correlations and *t*-statistics [87]. The mean change in correlations due to this adjustment was 0.071 and 0.078 for the positive and negative information security policy attitude group, respectively. The results of the significance tests showed that none of the uncorrected significant correlations became nonsignificant after controlling for CMV, suggesting that a CMV bias is unlikely to be of concern in this study.

5.2. Structural model testing

To assess the structural model, we examined the R^2 values and estimates for the path coefficients. We found that our model explains 51.2 % and 47.6 % of the variance in information security policy compliance for employees with a positive and negative attitude, respectively, indicating that the exogenous variables have a moderate explanatory power [79].

To test our hypotheses, we conducted a PLS-MGA [80]. By applying PLS-MGA, we can test for significant differences between identical models for different a priori-specified groups, which are, in our case, employees with a positive or negative attitude toward information

Table 2
Demographic characteristics of sample.

		Positive information security policy attitude ($n = 141$)		Negative information security policy attitude ($n = 170$)	
Measure	Item	Count	%	Count	%
Gender	Female	35	24.8	63	37.1
	Male	104	73.8	105	61.8
	Not specified	2	1.4	2	1.2
Age (years)	18–20	2	1.4	7	4.1
	21–30	54	38.3	71	41.8
	31–40	46	32.6	52	30.6
	41–50	24	17.0	26	15.3
	51–60	11	7.8	12.	7.1
	> 60	3	2.1	2	1.2
Highest level of education	Not specified	1	0.7	0	0
	Secondary general school	0	0.0	1	0.6
	Intermediate secondary school	0	0.0	3	1.8
	Special upper secondary school	1	0.7	3	1.8
	Grammar school classes A-level	14	9.9	20	11.8
	University degree	116	82.3	138	81.2
	Other degree	10	7.1	5	2.9
Civil servant status	Yes	29	20.6	19	11.2
	No	112	79.4	149	87.6
	Not specified	0	0.0	2	1.2
Occupation	Academic department	127	90.1	130	76.5
	Administrative department	13	9.2	30	17.6
	Not specified	1	0.7	10	5.9

Table 3
Measurement model.

Positive information security policy attitude ($n = 141$)

Construct	Loadings	CR	AVE	Cross-Correlations and Square Root of AVE and HTMT Values (in Parentheses)[b]						
				1	2	3	4	5	6	7
1. Descriptive norms	0.88–0.91	0.90	0.75	**0.86**						
2. Information security policy awareness	0.60–0.88	0.70	0.55	0.41 (0.47)	**0.74**					
3. Information security policy compliance	0.95–0.97	0.96	0.92	0.13 (0.29)	0.40 (0.79)	**0.96**				
4. Personal norms	0.85–0.92	0.93	0.81	0.42 (0.49)	0.32 (0.62)	0.69 (0.76)	**0.9**			
5. Punishment certainty	0.62–0.87	0.81	0.59	0.34 (0.43)	0.16 (0.45)	0.29 (0.34)	0.30 (0.36)	**0.83**		
6. Punishment severity	0.67–0.94	0.79	0.66	0.46 (0.63)	0.24 (0.67)	0.32 (0.41)	0.38 (0.48)	0.56 (0.82)	**0.81**	
7. Subjective norms	0.71–0.99	0.87	0.77	0.24 (0.25)	0.36 (0.79)	0.32 (0.29)	0.36 (0.34)	0.29 (0.37)	0.37 (0.52)	**0.88**

Negative information security policy attitude ($n = 170$)

Construct	Loadings	CR	AVE	Cross-Correlations and Square Root of AVE and HTMT Values (in Parentheses)[b]						
				1	2	3	4	5	6	7
1. Descriptive norms	0.90–0.93	0.94	0.84	**0.91**						
2. Information security policy awareness	0.70–0.81	0.72	0.57	0.48 (0.56)	**0.75**					
3. Information security policy compliance	0.91–0.92	0.92	0.84	0.33 (0.70)	0.18 (0.38)	**0.92**				
4. Personal norms	0.78–0.84	0.86	0.67	0.14 (0.16)	0.00 (0.1)	0.45 (0.56)	**0.82**			
5. Punishment certainty	0.73–0.80	0.86	0.75	0.25 (0.32)	0.37 (0.86)	0.21 (0.28)	0.13 (0.18)	**0.87**		
6. Punishment severity	0.78–0.88	0.81	0.69	0.25 (0.34)	0.21 (0.49)	0.35 (0.50)	0.20 (0.31)	0.26 (0.38)	**0.83**	
7. Subjective norms	0.87–0.95	0.91	0.83	0.21 (0.23)	0.16 (0.36)	0.46 (0.55)	0.35 (0.41)	0.24 (0.31)	0.26 (0.38)	**0.91**

[b] Values on the diagonal (bold) display the square root of AVE, whereas off-diagonal values are the correlations among latent constructs. HTMT values are displayed in parentheses.

security policies. Unlike standard approaches to testing moderation, which examine a single structural relationship at a time, PLS-MGA is a simple, straightforward, and efficient way to assess moderation across all model relationships simultaneously [89,90]. Additionally, the identified differences can be used to highlight the potential error if subpopulations are considered as a single homogeneous group because these differences may not be apparent when studied as a whole [91]. Finally, by gaining insight into group differences, strategy implementation (e.g., policies and training programs) based on the outcomes can be more specific for the heterogeneous groups [89].

Before comparing group-specific path coefficients, we need to assess measurement invariance [92], which adds an additional level of accuracy to our findings [89]. Using the measurement invariance of a composite model (MICOM) assessment, we establish partial measurement invariance (see Appendix A), which allows us to compare the path coefficients [92].

Next, we estimate the PLS structural model for both groups, including the path coefficients and significance levels (see third and fourth columns of Table 4). Each group was subjected to a bootstrap analysis with 5000 bootstrap samples. Then, each path coefficient estimate of the group of those with a positive attitude toward information security policies (β_1) was compared to the estimate of those with a negative attitude toward information security policies (β_2). The number of positive and zero differences divided by the total number of comparisons indicates the probability of β_1 being greater than β_2. The results are significant at the 5% level if p-values are smaller than 0.05 or larger than 0.95 [80]. The results of the PLS-MGA are in the fifth column of Table 4.

Regarding formal sanctions, we find that the path between punishment severity and information security policy compliance is significantly stronger for disinclined employees ($|\beta_1\text{-}\beta_2| = 0.17$, $p < 0.05$), but not the path from punishment certainty to information security policy compliance. Thus, we find evidence to support H2 but not H1. In terms of informal (social) sanctions, there are significant differences between the influences of descriptive norms ($|\beta_1\text{-}\beta_2| = 0.25$, $p < 0.01$) and subjective norms ($|\beta_1\text{-}\beta_2| = 0.18$, $p < 0.05$) on information security policy compliance with both being stronger for disinclined employees. Thus, we find evidence to support H3. For personal self-sanctions, the path from personal norms to information security policy compliance is significantly stronger for inclined employees ($|\beta_1\text{-}\beta_2| = 0.32$, $p > 0.999$);

Table 4
Multigroup analysis test results.

	Path[c]	Coefficients		PLS-MGA	
		Positive security policy attitude (β_1)	Negative security policy attitude (β_2)	Coefficients diff. ($\|\beta_1\text{-}\beta_2\|$)	Hypotheses
Formal sanctions	PC→ISPC	0.07 n.s.	0.02 n.s.	0.05 n.s.	H1: $\beta_1 < \beta_2$ (rejected)
	PS→ ISPC	−0.04 n.s.	0.13*	0.17*	H2: $\beta_1 < \beta_2$ (supported)
Informal sanctions	DN→ ISPC	0.12 n.s.	0.36***	0.24**	H3: $\beta_1 < \beta_2$ (supported)
	SN→ ISPC	0.06 n.s.	0.23**	0.18*	
Self-sanctions	PN→ ISPC	0.60***	0.28***	0.32***	H4: $\beta_1 > \beta_2$ (supported)
Information security policy awareness	ISPA→PC	0.16*	0.37***	0.22*	H5: $\beta_1 < \beta_2$ (supported)
	ISPA→PS	0.24***	0.21***	0.03 n.s.	H6: $\beta_1 < \beta_2$ (rejected)
	ISPA→DN	0.13 n.s.	0.33***	0.19*	H7: $\beta_1 < \beta_2$ (partially supported)
	ISPA→SN	0.36***	0.16*	0.20*	
	ISPA→PN	0.19*	−0.08 n.s.	0.28**	H8: $\beta_1 > \beta_2$ (supported)

*** $p < 0.001$.
** $p < 0.01$.
* $p < 0.05$, n.s. = not significant.
[c] ISPC = information security policy compliance, PC = punishment certainty, PS = punishment severity, DN = descriptive norms, SN = subjective norms, PN = personal norms, ISPA = information security policy awareness.

and therefore, our evidence provides support for H4. In terms of information security policy awareness, the path from awareness to punishment certainty is significantly stronger for disinclined employees ($|\beta_1$-$\beta_2| = 0.22$, $p < 0.05$), but not the path from awareness to punishment severity. Thus, our evidence provides support for H5 but not H6. The path from information security policy awareness to descriptive norms is significantly stronger for disinclined employees ($|\beta_1$-$\beta_2| = 0.19$, $p < 0.05$), but not the path from awareness to subjective norms. Thus, our evidence provides partial support for H7. As expected, the path from information security policy awareness to personal norms is significantly stronger for inclined employees ($|\beta_1$-$\beta_2| = 0.28$, $p > 0.992$); therefore, our evidence provides support for H8. Finally, in testing our structural model, several control variables (age, gender, level of education, and civil servant status) for information security policy compliance were considered based on the information security literature [2,52,58]. None were significant for either group, and were also not significantly different based on the PLS-MGA.

To check the robustness of our results, we also accounted for endogeneity that could arise from omitted variables in the PLS path model. Our assessment of endogeneity in Appendix B follows Hult et al.'s [93] systematic procedure for addressing endogeneity in partial least squares-structural equation modeling (PLS-SEM) and indicates that endogeneity is not present, which supports the robustness of the structural model results [93].

6. Discussion

In this paper, we apply a group-based approach to examine deterrability [14] by employing a model of security policy compliance that integrates formal, social, and personal sanctions along with information security policy awareness. We test whether their impacts differ depending on the degree to which employees have a positive or negative attitude toward information security policies. In the following, we discuss our key findings, its implications for theory and practice, as well as limitations and interesting avenues for further research.

6.1. Key findings

Our results confirm the role and importance of deterrability in information security studies by finding that information security policy compliance among employees grouped according to whether they had a positive or negative attitude toward information security policies, is differently influenced by externally imposed (formal and informal social sanctions) and internally imposed (personal self-sanctions) motivating forces.

Specifically, our group-based approach reveals that information security policy compliance of inclined employees (i.e., those with a positive attitude) is mainly driven by their personal norms (H4) and not by perceptions of formal sanctions (H1, H2) or informal social sanctions (H3). These findings provide strong support of our conceptualization of inclined compliers. In particular, similar to acute conformists [14], they are undeterrable in that they are insensitive to formal sanctions. Instead, their information security policy compliance is largely shaped by their own personal conviction of whether or not a behavior is appropriate. This internal driver is sustainable in that it is present regardless of sanction expectations. We also find that information security policy awareness had a stronger association with personal norms for inclined employees (H8). Thus, knowing one's responsibility as laid down in the information security policies leads to feelings of moral obligation in these employees.

Our results also show that disinclined compliers (i.e., those with a negative attitude who comply nevertheless) are deterrable. Yet, the deterrent effect of formal sanctions is predominantly exerted through punishment severity (H2) rather than punishment certainty (H1) when employees have a negative attitude toward information security policies. Moreover, the deterrent effect of informal social sanctions appears to play an important role in their compliance. This implies that although these disinclined compliers may have a less positive impression of information security policies and are less inclined to adhere to them, they alter their behavior to comply in response to their perceived behavior of colleagues (i.e., descriptive norms), as well as to the expectations of supervisors and colleagues (i.e., subjective norms) (H3). Our findings concur with the criminology literature, where informal social sanctions have been found to have stronger deterrent effects on deviant behavior than formal ones [94]. Finally, we find partial support of information security policy awareness on formal and informal (social) sanction perceptions being stronger for disinclined employees. Regarding formal sanctions, we find a differential impact of awareness on punishment certainty with the path being stronger for disinclined employees (H5), but no significant differences for punishment severity (H6). However, the subsequent differential influence of severity on compliance being stronger for disinclined employees indicates differences in the underlying process through which information security policy awareness impacts information security policy compliance. In terms of informal (social) sanctions, as expected, information security policy awareness had a stronger association with descriptive norms for disinclined employees, but contrary to expectation, a weaker association with subjective norms (H7). One potential explanation is that disinclined employees may have generalized from their own negative attitude toward the information security policy to the views of the larger group, thereby creating a false consensus effect regarding what others expect [95]. Individuals may project their views because they have little insight into the prevalent subjective norm, while they know their view very well.

6.2. Theoretical contributions

In this paper, we consider the conditions under which sanctions affect information security policy compliance. In particular, we focus on understanding the concept of deterrability to examine for which subgroups of employees sanctions can actually exert a useful deterrent effect and for which not.

To isolate the deterrent effect of three different types of sanctions, we examine two groups that vary in their deterrability: employees with a positive attitude who subsequently comply ("inclined compliers") and employees with a negative attitude who comply nonetheless ("disinclined compliers"). Differentiating between these two groups provides an initial explanation of the inconsistent results of the deterrent effect (or lack thereof) of sanctions in early information security research. Specifically, while the inconsistent conclusions from studies that questioned (e.g., [53,96,97]) or supported (e.g. [10,49,98],) the role of formal sanctions suggest that the picture is still blurry when not considering employees' (un)deterrability, our results support the assertion that formal sanctions do matter for disinclined compliers but not for inclined ones. Similarly, our study also suggests that other than formal sanctions, informal sanctions, such as social disapproval, influence compliance decisions for disinclined compliers but not for inclined compliers. The behavior of inclined compliers appears bounded by a form of informal constraint rather than by the fear of external sanctions, both formal and informal (social) ones. Accordingly, our results not only support the argument that personal self-sanctions as part of personal norms may have an influence equal to that of formal sanctions in general [31], but are even enough to ensure the compliance of inclined employees.

With these findings, we extend the literature by showing that the effectiveness of formal and informal sanctions on compliance is contingent on one's (dis)inclination; thereby forming a foundation for future research. For example, the number of inclined employees could be a good indicator to find out whether a certain policy is considered acceptable by a portion of the workforce. In this case, network externalities [99] could apply, and inclined employees could influence those that are disinclined to comply. Further research could examine the influence that inclined compliers can have on their peers.

The differences also highlight the potential error if both compliance groups (inclined and disinclined) are considered a single homogeneous group. These differences may not be apparent in aggregate data where an average effect of sanctions on policy compliance might contribute more to confuse than to provide insight on the deterrence process and the ability of sanctions to encourage compliant behavior. Research involving a "one size fits all" mentality does not account for employee preferences; and it would be interesting to explore how security training programs, tailored to either creating a positive attitude or focusing on a sanctioning rhetoric, persuade different employee groups into compliance.

We also examine differences between inclined and disinclined compliers beyond the deterrent effects of sanctions on compliance by connecting information security policy awareness to sanctions. Some studies suggest that policies rely on the same deterrent mechanism as societal laws and an awareness thereof increases formal sanction perceptions [52]. Yet, the effect of information security policy awareness on informal (social) sanctions and personal self-sanctions is barely explored in information security research. We show that group-based differences affect information security policy awareness on multilevel sanction perceptions to some degree (except for punishment severity and other than expected for subjective norms). Employees appear to be differently receptive to the messages delivered in information security policies. Such policies could either serve as a deterrence mechanism increasing external sanction perceptions or as a responsibility mechanism for forming internal feelings of moral obligation. Thus, we encourage further research to draw on our findings and examine additional factors other than attitude that intensify the differences in these two mechanisms.

6.3. Practical implications

The consideration of deterrability is important as a means to make organizational information security policies more effective. As these policies similar to societal laws are based on the idea that potential policy violators are deterred by the threat of punishment, information security managers need to understand the limitations of this approach [5]. Deterrence-based information security policies and security education training and awareness (SETA) programs to respond to this rising phenomenon can only be effective to the extent that employees are deterrable. As dealing with business-managed IT and unapproved cloud solutions has turned into a key challenge for security managers [25], they are required to learn new tactics to educate their employees and increase their information security policy awareness. Our research acknowledges that raising employees' information security policy awareness is an initial step to motivate employee compliance. However, when designing these policies and training employees in an effort to raise their awareness, practitioners need to pay attention to whether their employees are more receptive to a deterrence message or a sense of responsibility message. The key implication is that actions taken to increase information security policy compliance should pay attention to the different ways employees are inclined or disinclined to comply.

For example, initiatives aimed at addressing deterrence through formal sanctions, such as the announcement that employees' computer activities could be monitored and that they will be punished for using public clouds, will most likely remain ineffective for employees with a positive attitude toward security policies because they are not deterred by punishments. Disciplinary actions can be detrimental and costly to an organization. First, organizational resources are wasted if only some employees feel addressed by these initiatives [4]. Second, in certain cases enforcing coercive security policy changes may even act as a trigger event or catalyst for negative attitudes and undesired behaviors [100]. If employees strive to follow policies because of their intrinsic motivation, sanction threats may reduce their positive attitude toward policies. This "crowding out" of intrinsic behavior through external rewards or punishments has been established for numerous behavioral areas, such as tax compliance [101]. Instead, the results of our study regarding the strength of the relationship between personal norms and information security policy compliance for employees with a positive attitude toward information security policies suggest a different approach. They indicate that specific measures should support the alignment of personal norms with information security policies (and overcome discrepancies between policies and personal norms). Thus, organizations are advised to form close links between information security policies' objectives and their employees' internal values to foster inclined compliance. Periodic SETA programs should strive to have employees recognize the necessity and usefulness of the information security policies' prohibitions and requirements. The key point here is to convince employees that the protection of confidential data is also in their best interest. The importance of data protection for the organization's existence and hence, their job security needs to be demonstrated, along with showing that these policies also serve to protect the employees' personal data. In addition, organizations could resort to ethics training to increase employees' morality levels to the extent that they may feel morally obliged to follow information security policies. The success of these morality campaigns in reducing illicit behavior has been supported by criminology research as well [31].

Yet, when employees have a negative attitude, SETA programs aimed at addressing deterrence through formal or informal sanctions will promote information security policy compliance of those who are disinclined to comply. Our findings imply that formal sanctions levered through punishment severity rather than punishment certainty may be more suitable for employees with a negative attitude toward information security policies. To encourage compliant behavior among these employees, the content of information security policies should clearly delineate the punishment for security policy-violating behaviors. Moreover, our results also indicate a significant impact of informal social sanctions. The expectations of supervisors and peers, as well as the perceived behavior of the latter play a more important role in influencing one's security-related behaviors than formal sanctions when employees have a negative attitude toward information security policies. Hence, compliance should not be enforced solely top-down through formal sanctions, but rather modeled on a daily basis by employees at all levels, including supervisors and the IT department. Role models for employees could be trained and educated to advocate compliant behavior [102]. Given the strong role of descriptive norms, this raises the interesting question regarding the (non-) effectiveness of information security campaigns that warn about an increase in disruptive security-related behaviors (e.g., choosing a weak password and surfing on private websites at work) to raise awareness of security issues and threats. In doing so, they spread information that these behaviors are widespread. By communicating the message "many of your colleagues do undesirable things," the organization is simultaneously communicating the strong normative message "many colleagues are doing it" [59].

6.4. Limitations and future research

The following limitations of our study could be addressed in future research. First, our study could be limited because of self-reported compliance as we could not observe information security policy compliance with objective data, but asked participants whether they complied with the organizational policies for using public clouds. We encourage researchers to analyze actual public cloud usage in organizations. However, organizations are often unwilling to disclose this information to researchers, a difficulty frequently being discussed in extant information security research [103]. Still, tackling this issue with case studies would be useful to verify and build on our findings in a richer way.

Second, regarding the conceptual view on attitudes, we focused on attitude valence (i.e., the positive or negative nature of attitude). However, with respect to a longitudinal setting, we acknowledge that

the concept of attitudinal quality or attitude strength [104,105] might be particularly important especially when the degree of deterrence varies over time, as stronger attitudes are more resistant to attitude change [106]. By introducing the concept of attitude strength in a longitudinal setting with different degrees of deterrence, we are well aware that the identified group characteristics can vary with respect to deterrability.

Third, we acknowledge that the degree of (dis)inclined compliance based on attitude toward information security policies may not be static but could change with regard to the security policy under consideration. For example, employees might favor the password protection policy as it helps secure their accounts but might be frustrated by the cloud use policy as it limits their ability to share files. Thus, they might not need to be deterred from sharing their password with others, but possibly need to be from using public cloud systems. This suggests a dynamic tension between attitudes and sanction threat responsiveness that future research could investigate to assess the degree of intra-individual consistency in deterrability [107].

Fourth, with regard to methodological limitations, the classification of (dis)inclined compliers is based on a single-item measure of attitude toward information security policies. Future research seeking to expand and refine this classification may also consider other variables, such as habit, as representative for (dis)inclination to comply or not comply. When security habits and attitudes correspond, they may lead to the same behavioral outcome, but when they do not correspond, the behavioral outcome may depend on the strength of the habit and/or attitude. Additional groups of habit-driven employees could be identified to examine deterrability, because the deterrence effect of sanctions could be more effective when compliance behavior is not habitual but requires thought processes and is intentional [108]. Finally, given that we focus on the driving factors and the attitudes of these distinct groups that are (dis)inclined to comply, we also encourage researchers to examine other distinct groups, such as individuals with a positive attitude who fail to comply with information security policies ("inclined non-compliers") and individuals with a negative attitude who consequently do not comply ("disinclined non-compliers").

7. Conclusion

Our inquiry into deterrability is important, not only for the theoretical understanding of information security policy compliance behavior and deterrence theory, but also as a means to make information security policies more effective. As information security policies similar to societal laws are based on the idea that potential policy violators are deterred by the threat of punishment [52], scholars and practitioners need to understand the limitations of this approach. By comparing inclined and disinclined compliers, we found that the deterrent effect of multilevel sanctions varied between employees holding a positive and those holding a negative attitude toward information security policies. Our findings regarding inclined compliers point to another avenue where information security policies do not only serve as a deterrence mechanism attempting to alter formal sanction perceptions but also as a matter which employees are obliged to follow based on a sense of personal responsibility. In addition, providing insight into the inconsistent results of prior deterrence-related information security research, our group-based perspective focusing on individuals' deterrability opens up new avenues to examine the value of multilevel sanctions in information security management.

CRediT authorship contribution statement

Lennart Jaeger: Conceptualization, Methodology, Validation, Formal analysis, Data curation, Writing - original draft, Writing - review & editing, Visualization. **Andreas Eckhardt:** Conceptualization, Writing - original draft, Writing - review & editing, Supervision. **Julia Kroenung:** Conceptualization, Investigation, Writing - review & editing.

Appendix A. Measurement invariance

To assess measurement invariance, we follow the measurement invariance of composite models (MICOM) assessment procedure, which involves three steps [92]. In the first step, we establish configural invariance by ensuring an identical setup of both measurement and structural models, as well as identical data treatment and algorithm settings for the model estimations in SmartPLS. For the second and third step, we use the permutation algorithm of SmartPLS. The results of the second step ensure compositional invariance (see Table A1) as none of the correlation *c* values differs significantly from one. The results of the third step do not support full measurement invariance, because the mean values and variances are not equal between groups. Yet, to

Table A1
MICOM results.

Composite	*c* value (= 1)	$CI_{95\%}$	Step 2. Compositional invariance?
Descriptive norms	1.000	[0.997; 1.000]	Yes
Information security policy awareness	0.948	[0.884; 1.000]	Yes
Information security policy compliance	1.000	[1.000; 1.000]	Yes
Personal norms	0.999	[0.998; 1.000]	Yes
Punishment certainty	0.983	[0.965; 1.000]	Yes
Punishment severity	0.998	[0.946; 1.000]	Yes
Subjective norms	0.990	[0.988; 1.000]	Yes
Composite	**Difference of mean value (= 0)**	**$CI_{95\%}$**	**Step 3a. Equal mean values?**
Descriptive norms	0.633	[-0.218; 0.218]	No
Information security policy awareness	0.350	[-0.224; 0.243]	No
Information security policy compliance	1.132	[-0.233; 0.234]	No
Personal norms	0.967	[-0.226; 0.237]	No
Punishment certainty	0.244	[-0.240; 0.227]	No
Punishment severity	0.278	[-0.232; 0.249]	No
Subjective norms	0.479	[-0.251; 0.198]	No
Composite	**Logarithm of variances ratio (= 0)**	**$CI_{95\%}$**	**Step 3b. Equal variances?**
Descriptive norms	0.198	[-0.256; 0.254]	Yes
Information security policy awareness	−0.064	[-0.334; 0.360]	Yes
Information security policy compliance	−0.629	[-0.218; 0.234]	No
Personal norms	−0.681	[-0.233; 0.202]	No
Punishment certainty	0.054	[-0.269; 0.266]	Yes
Punishment severity	−0.188	[-0.267; 0.266]	Yes
Subjective norms	−0.281	[-0.277; 0.292]	No

compare path coefficients between groups, partial measurement invariance is sufficient [92].

Appendix B. Assessment of endogeneity

To assess potential endogeneity, we follow Hult et al.'s [93] procedure for addressing endogeneity in PLS-SEM, using the Gaussian copula approach [109]. This approach controls for endogeneity by directly modeling the correlation between the endogenous variable and the error term by means of a copula [93]. We consider both the independent variables of our original model, as well as their interaction terms with attitude toward information security policies as possibly exhibiting endogeneity (see Papies et al. [110] on interaction terms in the Gaussian copula approach). We use the latent variable scores of the original PLS model estimation as input to calculate the Gaussian copula of the partial regressions in the structural model [93]. To run the analyses, we used the REndo package of the R program [111], the boot package [112], and the R code provided by Hult et al. [93]. We find that neither of the Gaussian copulas is significant. Specifically, we find nonsignificant copulas of 0.07 for attitude (p-value = 0.52), 0.07 for descriptive norms (p-value = 0.81), -0.125 for information security policy awareness (p-value = 0.76), 0.02 for personal norms (p-value = 0.61), 0.16 for punishment certainty (p-value = 0.61), 0.10 for punishment severity (p-value = 0.65), and -0.02 for subjective norms (p-value = 0.56). Moreover, considering the interaction terms as potentially endogenous yields nonsignificant copulas of 0.09 for the interaction term of attitude with descriptive norms (p-value = 0.58), 0.11 for information security policy awareness (p-value = 0.76), 0.035 for personal norms (p-value = 0.035), -0.11 for punishment certainty (p-value = 0.64), -0.19 for punishment severity (p-value = 0.44), and 0.13 for subjective norms (p-value = 0.35). Hence, we conclude that endogeneity is not present, which supports the robustness of the structural model results [93].

Appendix C. Supplementary data

Supplementary material related to this article can be found, in the online version, at doi:https://doi.org/10.1016/j.im.2020.103318.

References

[1] R. Willison, M. Warkentin, Beyond deterrence: an expanded view of employee computer abuse, MIS Q. 37 (2013) 1–20.
[2] B. Bulgurcu, H. Cavusoglu, I. Benbasat, Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness, MIS Q. 34 (2010) 523–548.
[3] D.W. Straub, R.J. Welke, Coping with systems risk: security planning models for management decision making, MIS Q. 22 (1998) 441–469.
[4] A.C. Johnston, M. Warkentin, A.R. Dennis, M. Siponen, Speak their language: designing effective messages to improve employees' information security decision making, Decis. Sci. 50 (2019) 245–284.
[5] M. Silic, J.B. Barlow, A. Back, A new perspective on neutralization and deterrence: predicting shadow IT usage, Inf. Manage. 54 (2017) 1023–1037.
[6] K.P.M.G. Oracle, Oracle and KPMG Cloud Threat Report 2019, 2019 (accessed 10 September 2019), https://www.oracle.com/cloud/cloud-threat-report/.
[7] K.P.M.G. Harvey Nash, CIO Survey 2019: A Changing Perspective, 2019 (accessed 10 September, https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/07/harvey-nash-kpmg-cio-survey-2019.PDF.
[8] McAfee, Navigating a Cloudy Sky: Practical Guidance and the State of Cloud Security, 2018 (accessed 29 August 2019, https://www.mcafee.com/enterprise/en-us/solutions/lp/cloud-security-report.html.
[9] McAfee, Cloud Adoption and Risk Report 2019, 2019 (accessed 29 August 2019), https://info.skyhighnetworks.com/WPCloudAdoptionRiskReport2019_BannerCloud-MFE.html.
[10] J.S.-C. Hsu, S.-P. Shih, Y.W. Hung, P.B. Lowry, The role of extra-role behaviors and social controls in information security policy effectiveness, Inf. Syst. Res. 26 (2015) 282–300.
[11] M. Warkentin, R. Willison, Behavioral and policy issues in information systems security: the insider threat, Eur. J. Inf. Syst. 18 (2009) 101–105.
[12] J. D'Arcy, T. Herath, A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings, Eur. J. Inf. Syst. 20 (2011) 643–658.
[13] B.A. Jacobs, Deterrence and deterrability, Criminology 48 (2010) 417–441.
[14] G. Pogarsky, Identifying "deterrable" offenders: implications for research on deterrence, Justice Q. 19 (2002) 431–452.
[15] F. Zimring, G. Hawkins, Deterrence and marginal groups, J. Res. Crime Delinq. 5 (1968) 100–114.
[16] D.S. Nagin, G. Pogarsky, An experimental investigation of deterrence: cheating, self-serving bias, and impulsivity, Criminology 41 (2003) 167–194.
[17] G. Pogarsky, T.A. Loughran, The policy-to-Perceptions link in deterrence: time to retire the clearance rate, Criminol. Public Policy 15 (2016) 777–790.
[18] D.S. Nagin, G. Pogarsky, Integrating celerity, impulsivity, and extralegal sanction threats into a model of general deterrence: theory and evidence, Criminology 39 (2001) 865–892.
[19] H. Li, X.R. Luo, J. Zhang, R. Sarthy, Self-control, organizational context, and rational choice in Internet abuses at work, Inf. Manage. 55 (3) (2018) 358–367.
[20] V. Braithwaite, Dancing with tax authorities: motivational postures and non-compliant actions, in: V. Braithwaite (Ed.), Taxing Democracy: Understanding Tax Avoidance and Evasion, Aldershot, Ashgate, 2003, pp. 15–39.
[21] D. McBarnet, When compliance is not the solution but the problem: from changes in law to changes in attitude, in: V. Braithwaite (Ed.), Taxing Democracy: Unterstanding Tax Avoidance and Evasion, Ashgate, Aldershot, 2003, pp. 229–244.
[22] Tom Macaulay, How to Ensure GDPR Compliance in the Cloud, 2018. https://www.computerworlduk.com/cloud-computing/how-ensure-gdpr-compliance-in-cloud-3663797/.
[23] BSI, Information and Cyber Challenges in the Public Sector: Survey 2018, 2018 (accessed 10 September 2019), https://www.bsigroup.com/globalassets/localfiles/en-ie/csir/resources/whitepaper/uk-engb-survey-wp-challenges-public-sector-cloud.pdf.
[24] J. Cook, Turning the Tide: How the Public Sector Can Win the Battle Against Shadow IT, 2017. https://www.publictechnology.net/articles/opinion/turning-tide-how-public-sector-can-win-battle-against-shadow-it.
[25] CIO, What Should Public Sector CIOs Do About' shadow IT', 2015. https://www.cio.com.au/article/566649/what-should-public-sector-cios-do-about-shadow-it/.
[26] M.R. Geerken, W.R. Gove, Deterrence: Some theoretical considerations, Law Soc. Rev. 9 (1975) 497–513.
[27] M.L. Erickson, J.P. Gibbs, G.F. Jensen, The deterrence doctrine and the perceived certainty of legal punishments, Am. Sociol. Rev. (1977) 305–317.
[28] K.R. Williams, R. Hawkins, Perceptual research on general deterrence: a critical review, Law Soc. Rev. (1986) 545–572.
[29] J.P. Gibbs, Crime, Punishment, and Deterrence, Elsevier, New York, 1975.
[30] T.C. Pratt, F.T. Cullen, K.R. Blevins, L.E. Daigle, T.D. Madensen, The empirical status of deterrence theory: a meta-analysis, in: F.T. Cullen, J. Wright, K. Blevins (Eds.), Taking Stock: The Status of Criminological Theory, Transaction Publishers, New Brunswick, 2006, pp. 367–396.
[31] R. Paternoster, S. Simpson, Sanction threats and appeals to morality: testing a rational choice model of corporate crime, Law Soc. Rev. 30 (1996) 549–583.
[32] A.R. Piquero, R. Paternoster, G. Pogarsky, T. Loughran, Elaborating the individual difference component in deterrence theory, Annu. Rev. Law Soc. Sci. 7 (2011) 335–360.
[33] K.H. Guo, Y. Yuan, N.P. Archer, C.E. Connelly, Understanding nonmalicious security violations in the workplace: a composite behavior model, J. Manag. Inf. Syst. 28 (2011) 203–236.
[34] A.H. Eagly, S. Chaiken, The Psychology of Attitudes, Harcourt Brace Jovanovich, College Publishers, Fort Worth, TX, 1993.
[35] P. Zhang, S.N. Aikman, H. Sun, Two types of attitudes in ICT acceptance and use, Int. J. Hum.-Compu. Int. 24 (2008) 628–648.
[36] P. Zhang, H. Sun, The complexity of different types of attitudes in initial and continued ICT use, J. Assoc. Inf. Sci. Technol. 60 (2009) 2048–2063.
[37] N. Sohrabi Safa, R. von Solms, S. Furnell, Information security policy compliance model in organizations, Comput. Secur. 56 (2016) 70–82.
[38] H.C. Kelman, Compliance, identification, and internalization: three processes of attitude change, J. Confl, Resolut. 2 (1958) 51–60.
[39] H.-R. Kim, M. Lee, H.-T. Lee, N.-M. Kim, Corporate social responsibility and employee–company identification, J. Bus. Ethics 95 (2010) 557–569.
[40] C.M. Tam, I.W.H. Fung IV, A.P.C. Chan, Study of attitude changes in people after the implementation of a new safety management system: the supervision plan, Construct. Manag. Econ. 19 (2001) 393–403.
[41] J. Kroenung, A. Eckhardt, T. Kuhlenkasper, Conflicting behavioral paradigms and predicting IS adoption and non-adoption – the importance of group-based analysis, Comput. Hum. Behav. 67 (2017) 10–22.
[42] R. Titah, H. Barki, Nonlinearities between attitude and subjective norms in information technology acceptance: A negative synergy? MIS Q. 33 (2009) 827–844.
[43] M. Deutsch, H.B. Gerard, A study of normative and informational social influences upon individual judgment, J. Abnorm. Psychol. 51 (1955) 629–636.
[44] Y. Chen, K. Ramamurthy, K.-W. Wen, Organizations' information security policy compliance: stick or carrot approach? J. Manag. Inf. Syst. 29 (2014) 157–188.
[45] Y. Xue, H. Liang, L. Wu, Punishment, justice, and compliance in mandatory IT settings, Inf. Syst. Res. 22 (2011) 400–414.
[46] A.J. Burns, T.L. Roberts, C. Posey, R.J. Bennett, J.F. Courtney, Intentions to comply versus intentions to protect: a VIE theory approach to understanding the influence of insiders' awareness of organizational SETA efforts*, Decis. Sci. 50 (2017) 179–221.
[47] P. Puhakainen, M. Siponen, Improving employees' compliance through information systems security training: an action research study, MIS Q. 34 (2010) 757–778.

[48] S. Matteson, Why Your Company Needs Clear Security Policies: a Cautionary Tale, 2017. https://www.techrepublic.com/article/why-your-company-needs-clear-security-policies-a-cautionary-tale/.
[49] J. D'Arcy, S. Devaraj, Employee misuse of information technology resources: testing a contemporary deterrence model, Decis. Sci. 43 (2012) 1091–1124.
[50] Q. Hu, Z. Xu, T. Dinev, H. Ling, Does deterrence work in reducing information security policy abuse by employees? Commun. ACM 54 (2011) 54–60.
[51] D.W. Straub, Effective IS security: an empirical study, Inf. Syst. Res. 1 (1990) 255–276.
[52] J. D'Arcy, A. Hovav, D. Galletta, User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach, Inf. Syst. Res. 20 (2009) 79–98.
[53] M. Siponen, A. Vance, Neutralization: new insights into the problem of employee information systems security policy violations, MIS Q. 34 (2010) 487–502.
[54] R.E. Mann, R.G. Smart, G. Stoduto, E.M. Adlaf, E. Vingilis, D. Beirness, R. Lamble, M. Asbridge, The effects of drinking-driving laws: a test of the differential deterrence hypothesis, Addiction 98 (2003) 1531–1536.
[55] W.J. Scott, Deterrence and Income Tax Cheating: Testing Interaction Hypotheses in Utilitarian Theories, J. Appl. Behav. Sci. 17 (1981) 395–408.
[56] M. Wenzel, An analysis of norm processes in tax compliance, J. Econ. Psychol. 25 (2004) 213–228.
[57] H.G. Grasmick, R.J. Bursik Jr., Conscience, significant others, and rational choice: extending the deterrence model, Law Soc. Rev. 24 (1990) 837–861.
[58] T. Herath, H.R. Rao, Protection motivation and deterrence: a framework for security policy compliance in organisations, Eur. J. Inf. Syst. 18 (2009) 106–125.
[59] R.B. Cialdini, Descriptive social norms as underappreciated sources of social control, Psychometrika 72 (2007) 263–268.
[60] M. Hartmann, L. Jaeger, A. Eckhardt, Do Me a Favor: The Role of Social Relations for Information Security In-and Extra-Role Behavior, in: Proceedings of the 39th International Conference on Information Systems, San Francisco, CA, 2018.
[61] V. Venkatesh, F.D. Davis, A theoretical extension of the technology acceptance model: four longitudinal field studies, Manag. Sci. 46 (2000) 186–204.
[62] P.R. Warshaw, A new model for predicting behavioral intentions: an alternative to Fishbein, J. Mark. Res. 17 (1980) 153–172.
[63] S.H. Schwartz, Normative influences on altruism, Adv. Exp. Soc. Psychol. 10 (1977) 221–279.
[64] H.G. Grasmick, B.S. Blackwell, R.J. Bursik Jr, Changes in the sex patterning of perceived threats of sanctions, Law Soc. Rev. 27 (1993) 679–705.
[65] H. Li, J. Zhang, R. Sarathy, Understanding compliance with internet use policy from the perspective of rational choice theory, Decis. Support Syst. 48 (2010) 635–645.
[66] P. Ifinedo, Information systems security policy compliance: an empirical study of the effects of socialisation, influence, and cognition, Inf. Manage. 51 (2014) 69–79.
[67] I.M.Y. Woon, A. Kankanhalli, Investigation of IS professionals' intention to practise secure development of applications, Int. J. Hum.-Comput. St. 65 (2007) 29–41.
[68] M.T. Siponen, A conceptual foundation for organizational information security awareness, Inform. Manag. Comput. Secur. 8 (2000) 31–41.
[69] A. Hovav, J. D'Arcy, Applying an extended model of deterrence across cultures: an investigation of information systems misuse in the U.S. And South Korea, Inf. Manage. 49 (2012) 99–110.
[70] Q. Hu, T. Dinev, P. Hart, D. Cooke, Managing employee compliance with information security policies: the critical role of top management and organizational culture, Decis. Sci. 43 (2012) 615–660.
[71] A. Yazdanmehr, J. Wang, Employees' information security policy compliance: a norm activation perspective, Decis. Support Syst. 92 (2016) 36–46.
[72] H.L.A. Hart, Responsibility and Retribution, Oxford University Press, Oxford, 1968.
[73] S.H. Schwartz, J.A. Howard, Explanations of the moderating effect of responsibility denial on the personal norm-behavior relationship, Soc. Psychol. Q. 43 (1980) 441–446.
[74] F. Zahedi, A. Abbasi, Y. Chen, Fake-website detection tools: identifying elements that promote individuals' use and enhance their performance, J. Assoc. Inf. Syst. 16 (2015) 448–484.
[75] B.-Y. Ng, A. Kankanhalli, Y.C. Xu, Studying users' computer security behavior: a health belief perspective, Decis. Support Syst. 46 (2009) 815–825.
[76] J.-Y. Son, Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies, Inf. Manage. 48 (2011) 296–302.
[77] M. Siponen, M.A. Mahmood, S. Pahnila, Employees' adherence to information security policies: an exploratory field study, Inf. Manage. 51 (2014) 217–224.
[78] L. Bergkvist, J.R. Rossiter, The predictive validity of multiple-item versus single-item measures of the same constructs, J. Mark. Res. 44 (2007) 175–184.
[79] W.W. Chin, The partial least squares approach to structural equation modeling, in: G.A. Marcoulides (Ed.), Modern Methods for Business Research, Lawrence Erlbaum Associates, Mahwah, NJ, 1998, pp. 295–336.
[80] J. Henseler, PLS-MGA: a non-parametric approach to partial least squares-based multi-group analysis, in: W.A. Gaul, A. Geyer-Schulz, L. Schmidt-Thieme, J. Kunze (Eds.), Challenges at the Interface of Data Analysis, Computer Science, and Optimization, Springer, Karlsruhe, 2012, pp. 495–501.
[81] J.F. Hair, W.C. Black, B.J. Babin, R.E. Anderson, R.L. Tatham, Multivariate Data Analysis, Pearson Prentice Hall Upper Saddle River, NJ, 2006.
[82] J. Hulland, Use of partial least squares (PLS) in strategic management research: a review of four recent studies, Strat. Manag. J. 20 (1999) 195–204.
[83] C. Fornell, D.F. Larcker, Evaluating structural equation models with unobservable variables and measurement error, J. Mark. Res. 18 (1981) 39–50.
[84] J. Henseler, C.M. Ringle, M. Sarstedt, A new criterion for assessing discriminant validity in variance-based structural equation modeling, J. Acad. Mark. Sci. 43 (2015) 115–135.
[85] A.H. Gold, A. Malhotra, A.H. Segars, Knowledge management: an organizational capabilities perspective, J. Manag. Inf. Syst. 18 (2001) 185–214.
[86] M.K. Lindell, D.J. Whitney, Accounting for common method variance in cross-sectional research designs, J. Appl. Psychol. 86 (2001) 114–121.
[87] N.K. Malhotra, S.S. Kim, A. Patil, Common method variance in IS research: a comparison of alternative approaches and a reanalysis of past research, Manag. Sci. 52 (2006) 1865–1883.
[88] R. Agarwal, E. Karahanna, Time flies when you're having fun: cognitive absorption and beliefs about information technology usage, MIS Q. 24 (2000) 665–694.
[89] L. Matthews, Applying multigroup analysis in PLS-SEM: a step-by-step process, in: H. Latan, R. Noonan (Eds.), Partial Least Squares Path Modeling: Basic Concepts, Methodological Issues and Applications, Springer International Publishing, Cham, 2017, pp. 219–243.
[90] J.F. Hair Jr., G.T.M. Hult, C. Ringle, M. Sarstedt, A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM), SAGE Publications, 2016.
[91] C. Schlaegel, M. Sarstedt, Assessing the measurement invariance of the four-dimensional cultural intelligence scale across countries: a composite model approach, Eur. Manag. J. 34 (2016) 633–649.
[92] J. Henseler, C.M. Ringle, M. Sarstedt, Testing measurement invariance of composites using partial least squares, Int. Mark. Rev. 33 (2016) 405–431.
[93] G.T.M. Hult, J.F. Hair Jr, D. Proksch, M. Sarstedt, A. Pinkwart, C.M. Ringle, Addressing endogeneity in international marketing applications of partial least squares structural equation modeling, J. Int. Mark. 26 (2018) 1–21.
[94] C.R. Tittle, R. Paternoster, Social Deviance and Crime: an Organizational and Theoretical Approach, Roxbury Publishing Company, Los Angeles, CA, 2000.
[95] L. Ross, D. Greene, P. House, The "false consensus effect": an egocentric bias in social perception and attribution processes, J. Exp. Soc. Psychol. 13 (1977) 279–301.
[96] P.B. Lowry, C. Posey, R.B.J. Bennett, T.L. Roberts, 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, Info. Systems J. 25 (2015) 193–273.
[97] M. Warkentin, A.C. Johnston, J. Shropshire, The influence of the informal social learning environment on information privacy policy compliance efficacy and intention, Eur. J. Inf. Syst. 20 (2011) 267–284.
[98] A.C. Johnston, M. Warkentin, M.T. Siponen, An enhanced fear appeal rhetorical framework: leveraging threats to the human asset through sanctioning rhetoric, MIS Q. 39 (2015) 113–134.
[99] D. Katz, The motivational basis of organizational behavior, Syst. Res. 9 (1964) 131–146.
[100] F. Bélanger, S. Collignon, K. Enget, E. Negangard, Determinants of early conformance with information security policies, Inf. Manage. 54 (2017) 887–901.
[101] L.P. Feld, B.S. Frey, Tax compliance as the result of a psychological tax contract: the role of incentives and responsive regulation, Law Policy 29 (2007) 102–120.
[102] L. Jaeger, C. Ament, A. Eckhardt, The closer you get the more aware you Become–A case study about psychological distance to information security incidents, in: Proceedings of the 38th International Conference on Information Systems, Seoul, South Korea, 2017.
[103] R.E. Crossler, A.C. Johnston, P.B. Lowry, Q. Hu, M. Warkentin, R. Baskerville, Future directions for behavioral information security research, Comput. Secur. 32 (2013) 90–101.
[104] J.A. Krosnick, R.E. Petty, Attitude strength: Antecedents and Consequences, Psychology Press, New York, 1995.
[105] M.W. Erber, S.D. Hodges, T.D. Wilson, Attitude strength, attitude stability, and the effects of analyzing reasons, in: R.E. Petty, J.A. Krosnick (Eds.), Eds.), Attitude Strength: Antecedents and Consequences, Psychology Press, New York, 1995, pp. 433–454.
[106] E.M. Pomerantz, S. Chaiken, R.S. Tordesillas, Attitude strength and resistance processes, J. Pers, Soc. Psychol. 69 (1995) 408–419.
[107] J.A. Bouffard, M.L. Exum, N. Niebuhr, Examining the stability and predictors of deterrability across multiple offense types within a sample of convicted felons, J. Crim. Justice 57 (2018) 76–88.
[108] D. Beyleveld, Identifying, explaining and predicting deterrence, Br. J. Criminol. 19 (1979) 205–224.
[109] S. Park, S. Gupta, Handling endogenous regressors by joint estimation using copulas, Mark. Sci. 31 (2012) 567–586.
[110] D. Papies, P. Ebbes, H.J. van Heerde, Addressing endogeneity in marketing models. Advanced Methods for Modeling Markets, Springer, 2017, pp. 581–627.
[111] R. Gui, M. Meierer, R. Algesheimer, R. Package REndo, Fitting Linear Models With Endogenous Regressors Using Latent Instrumental Variables (Version 1.2), 2017. https://cran.r-project.org/web/packages/REndo/.
[112] A. Canty, B. Ripley, R Package Boot: Bootstrap Functions (Version 1.3-20), 2017 (accessed 29 August 2019, https://cran.r-project.org/web/packages/boot/.

Lennart Jaeger is a research associate at the EBS University of Business and Law in Oestrich-Winkel, Germany. He graduated in Information Systems from Goethe University, Frankfurt. His research interests include behavioral and organizational aspects of information security. His research has been published in the proceedings of several IS conferences, such as ICIS, ECIS, PACIS, and HICSS. He received Best Paper Awards by ECIS 2018 and SIGADIT.

Andreas Eckhardt is a professor at the German Graduate School of Management and Law (GGS) in Heilbronn, and a visiting professor of Information Systems at the University of Innsbruck. He received his Ph.D. in Information Systems from Goethe University Frankfurt. His research on IT adoption and user behavior, behavioral security, digital innovation, technostress, and E-HRM has been published in two books, several book chapters, conference proceedings, and scientific journals including the Journal of Information Technology, Journal of Strategic Information Systems, European Journal of Information Systems, Information & Management, Business & Information Systems Engineering, and MIS Quarterly Executive. He is the recipient of numerous awards for his research, teaching, and community work, among others the Magid Igbaria Outstanding Paper Award and the ECIS Best Research in Progress Paper Award. He is Past Chair of the AIS Special Interest Group on Adoption and Diffusion of Information Technology (SIGADIT), and member of the AIS Diversity & Inclusion Committee.

Julia Kroenung is a professor at the EBS University of Business and Law in Oestrich-Winkel, Germany. Her research focuses on e-government, human behavior, and IS, social inclusion, and individual IS adoption. Her research has been published in several scientific journals including Journal of the Association for Information Systems, Information & Management, Computers in Human Behavior, Journal of Information Technology Theory and Application, International Journal of Electronic Business, Cogent Business & Management, and in the proceedings of leading IS conferences, such as the International Conference on Information Systems.