Information Systems Frontiers (2019) 21:1265–1284
https://doi.org/10.1007/s10796-019-09956-4

A Meta-Analysis of Deterrence Theory in Information Security Policy Compliance Research

Simon Trang[1] · Benedikt Brendel[1]

Published online: 25 October 2019

Abstract
Enforcing information security policies is a key concern of information security managers. To deter employees from deviant behavior, organizations often implement sanction mechanisms. However, evidence from research regarding the efficiency of such a deterrence approach has been mixed. Drawing on this inconsistency, this paper examines the applicability of deterrence theory in information security policy compliance research. It is argued that contextual and methodological moderators play a crucial role when conceptualizing deterrence theory in security studies. Applying a meta-analysis, the results suggest that sanctions have an overall effect on deviant behavior. However, the results also indicate that this relationship is dependent on the study's context. Deterrence theory better predicts deviant behavior in malicious contexts, cultures with a high degree of power distance, and cultures with a high uncertainty avoidance. The meta-analysis also reveals no meaningful differences arising from the methodological context in terms of scenario-based and behavior-specific measurement.

Keywords Information security policy · Compliance behavior · Deterrence theory · Meta-analysis

1 Introduction

In a connected world of people, data, and things, organizations balance the tension between the need for fast digital growth and securing their information assets across all actors. This balancing act results in massive spending on enterprise security worldwide, estimated at near $100 billion in 2018 alone (Gartner 2018). Effective security governance and an equilibrated implementation of security measures become central for sustainable security (Schatz and Bashroush 2017; Xu et al. 2017). A key instrument for achieving sustainable information security is an information security policy (ISP). ISPs encompass sets of rules and guidelines related to the processing and use of information within an organization's boundaries of authority (Baskerville and Siponen 2002).

Enforcing an ISP within a company is a key concern of information security managers. Both employee negligence and intentional insider breaches pose significant threats in securing information (D'Arcy et al. 2009; Puhakainen and Siponen 2010). A typical measure for decreasing employees' deviation from desired behavior is based on deterrence mechanisms. For example, the widely applied information security management standard ISO 27001:2013 describes requirements for a "disciplinary process" that sanctions non-compliant behavior (ISO/IEC 2013a). The ISO 27002:2013 code of practice extends this deterrence perspective and defines a process for monitoring employees (ISO/IEC 2013b). Deterrence rhetoric also can play an important role in communicating ISP regulations, e.g., through security awareness and education training (Johnston et al. 2015; Puhakainen and Siponen 2010).

Research on ISP compliance behavior has applied a wide range of theories from various fields (Sommestad et al. 2014). One of the first research streams in this area picked up the idea of deterrence (D'Arcy and Herath 2011; Harrington 1996; Straub 1990). Building on deterrence theory from criminology research, extant literature discusses whether and how sanction mechanisms work to deter employees from deviant ISP behavior (D'Arcy and Herath 2011). While the idea of deterrence provides a strong theoretical framework, has found wide application in other areas of research, and already has been applied in practice, empirical results are mixed (D'Arcy and Herath 2011; Willison et al. 2018a, b). This even leads to speculation about the theory's merits in explaining ISP compliance behavior (D'Arcy and Herath 2011; Lowry et al. 2015).

✉ Simon Trang
simon.trang@wiwi.uni-goettingen.de

[1] University of Göttingen, Platz der Göttinger Sieben 5, 37073 Göttingen, Germany

This paper builds on two reviews of deterrence and information security studies by D'Arcy and Herath (2011) and Willison et al. (2018a, b). It aims to delve deeper into specific inconsistencies and open questions in existing empirical literature. First, contradictions exist regarding the overarching support of deterrence theory for predicting ISP compliance behavior, with deterrence constructs' effect sizes varying greatly among studies. Although many studies find a positive and significant relationship between deterrence constructs and ISP compliance (e.g., Alshare et al. 2018; Cheng et al. 2013; Humaidi et al. 2014), some investigations suggest that no significant effects exist (e.g., Cuganesan et al. 2018; Moody et al. 2018), while a few even report negative correlations (e.g., Guo et al. 2011; Li et al. 2010). Some of these dispersed empirical findings might be explained by study-specific statistical artifacts in terms of sampling and measurement error (Hunter and Schmidt 2004). As deterrence theory's general applicability to the field of ISP compliance behavior research remains unclear, we posit the following research question:

> Research question 1 (RQ1): Accounting for sampling error and reliability error, does deterrence theory – in terms of formal and informal sanction severity and certainty, as well as sanction celerity – exert an overall effect on ISP compliance behavior?

Second, extant research also criticizes the conceptualization of deterrence theory in selected areas of ISP compliance behavior (Mahmood et al. 2010; Willison et al. 2018a, b). For example, Willison et al. (2018a, b) find evidence that deterrence theory shows strength in predicting criminal or antisocial behavior, rather than good behavior. Moreover, evidence from Hovav and D'Arcy (2012) suggests that the mechanisms of deterrence theory work differently across cultures and, thus, can contribute to dispersed empirical findings. We follow these ideas and identify two specific contexts for which the nature of deterrence theory might be more suited. Building on existing literature from criminology and culture, it is argued that both the type of ISP behavior and cultural context can contribute to the mechanisms of deterrence theory in the ISP field. In doing so, we not only explain inconsistencies in existing empirical findings, but also guide future research in these directions. Thus, we pose the second research question as follows:

> Research question 2 (RQ2): Does the context, in terms of malicious vs. non-malicious and cultures with low vs. high power distance, contribute to the applicability of deterrence theory?

Third, studies on ISP compliance behavior employ different approaches for measuring research variables. This includes two typical choices for ISP studies: Scholars must decide whether to employ hypothetical scenarios or capture actual behaviors, which usually are self-reported (Moody et al. 2018). Moreover, extant studies exhibit different specificities of ISP-compliant behavior. Building on evidence from other meta-analyses (Gerow et al. 2014; Mou et al. 2017), measurement choices also might explain inconsistencies in findings among deterrence-based ISP studies. Shedding light on these effects also can help future studies when deciding on a study design. Thus, we arrive at the final research question:

> Research question 3 (RQ3): *Do methodological choices, in terms of hypothetical* vs. *real and generic* vs. *specific ISP behavior, help explain dispersed empirical findings?*

To answer these research questions, we conducted a meta-analysis, collecting and analyzing the current body of empirical correlational literature on deterrence theory and ISP compliance behavior. This study departs from other recent meta-analyses in the field of information security behavior. While Mou et al. (2017) and Sommestad et al. (2015) analyzed studies on information security behavior using protection-motivation theory, Sommestad et al. (2014) and Cram et al. (2017) examined extant literature on information security compliance on a general level. However, none of these studies provides a complete overview of deterrence theory. For example, they fail to consider all five deterrence variables in the context of ISP compliance behavior. Moreover, they do not provide specific answers to the research questions.

The paper is structured as follows. Based on the three research questions, we first derive a research model. We then describe the meta-analytical approach, which entails data collection, data coding, and data analysis. The paper continues with a presentation and discussion of the results, followed by implications for theory and practice. Finally, the paper offers some conclusions.

2 Research Model

This research focuses on insiders' compliance with information security policies. The unit of analysis is an actor who is embodied in an organizational structure, in which an information security policy defines desirable behavior. In this paper, we follow a broad definition of ISP compliance. To give this meta-review a context, we understand all behavior that leads to the violation of the CIA triad (i.e., confidentiality, integrity, and availability) regarding organizational information as behavior that deviates from an ISP, i.e., ISP non-compliance. This encompasses intentional and unintentional behavior, both with and without a malicious motive. In turn, we define ISP-compliant behavior as all deliberate behavior that follows the rules, as well as guidelines prescribed in the ISP.

In this section, we derive a research model that enables the three research questions to be answered. The model is based on deterrence theory and includes contextual and methodological moderators. The final research model is presented in Fig. 1.

2.1 Deterrence Theory

For the following, we identify sanction severity, sanction certainty, and sanction celerity as the three fundamental concepts of deterrence theory in information security compliance-behavior research.

2.1.1 Sanction Severity

Sanction severity, also called punishment or penalty, is the perceived sanction severity by an actor in violation of a policy. This primary construct of deterrence theory finds empirical support across various disciplines and levels of analysis (Paternoster 1989; Paternoster and Simpson 1996). For example, in the private domain, sanction severity finds strong support in the area of individual criminal behavior, such as violent offenses or property infractions (Pratt et al. 2006). Paternoster and Simpson (1996) applied the construct to the organizational domain, finding evidence of its relevance for several types of corporate crime, including violation of environmental standards, manipulation of data, and bribery. In this context, sanction severity describes an organizational insider's perceived degree of punishment following neglect or violation of the information security policy. The argumentation is that the insider will be more deterred from misbehavior if the perceived severity of the sanction is greater. In the context of ISP studies, this mechanism has been tested in a range of contexts, including malicious and non-malicious contexts. In this sense, sanctions are not only the most common variable in deterrence-based ISP studies (D'Arcy and Herath 2011), but also are used often as control variables in otherwise theoretically grounded studies (Siponen and Vance 2010).

The type of sanction can be further subdivided. While most studies in the field of ISP behavior focus on formal sanctions as primary input that shapes an employee's evaluation process, some studies also include informal sanctions (Guo and Yuan 2012; Johnston et al. 2015). Formal reprimands refer to formalized consequences that the organization officially enforces. Informal sanctions refer to reprimands imposed by friends, peer groups, or supervisors, such as loss of respect, co-workers' esteem toward this person, or adverse effects on career opportunities. Accordingly, we posit the following two hypotheses:

H1a: Formal sanction severity is positively related to information security compliance behavior.
H1b: Informal sanction severity is positively related to information security compliance behavior.

2.1.2 Sanction Certainty

Sanction certainty describes the perceived probability of being punished when caught. It extends the idea of sanction severity

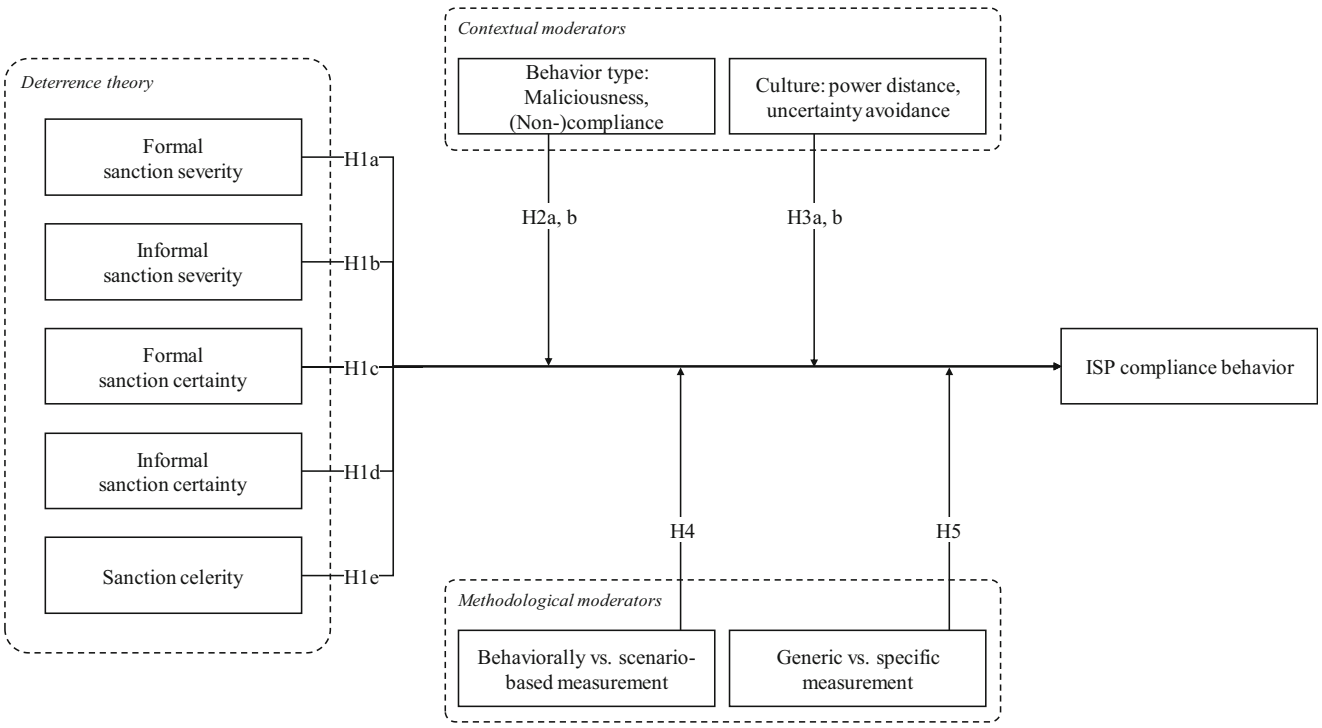

Fig. 1 Research model

in the sense that the more likely the sanction is of applying to the actor, the higher the expected cost of committing the crime, and the less likely the actor is to carry out the crime (Paternoster and Simpson 1993). As the second central construct in deterrence theory, it also finds wide empirical support across various studies and units of analysis (Pratt et al. 2006). In extant ISP compliance-behavior studies, perceived sanction certainty encompasses the detection of deviant behavior in the first place and the likelihood of the respective sanction being enforced. For example, deviant behavior can be detected through technical monitoring (e.g., analysis of logs), administrative measures (e.g., regular on-site audits), or social control through peers (Johnston et al. 2015; Workman 2009). In line with the distinction between formal and informal sanction severity, the respective certainty that these kinds of sanctions will apply can be differentiated. Accordingly, we posit the following hypotheses:

H1c: Formal sanction certainty is positively related to ISP compliance behavior.
H1d: Informal sanction certainty is positively related to ISP compliance behavior.

2.1.3 Sanction Celerity

Sanction celerity is defined as the perceived swiftness with which the punishment is enforced. The basic idea is that swift sanctions are more dreaded than delayed sanctions. From a rational-actor perspective, it can be derived that future costs through punishment are less costly than near-future costs (Paternoster and Simpson 1993). However, in criminological studies, this idea elicits scant consideration, with limited empirical evidence (Pratt et al. 2006). Supporters argue that the delayed imposition of sanctions decreases their rational evaluation (Paternoster 2010), resulting in a reduced exploitation of the general deterrent effect. However, critics maintain, for instance, that waiting for a punishment might feel as discomforting as the punishment itself (Gibbs 1975). In the field of ISP compliance research, some studies have conceptualized sanction celerity to explain deviant behavior (Hu et al. 2011; Hu and Xu 2018; Johnston et al. 2015; Lowry et al. 2015). In line with this argumentation, we posit the following hypothesis:

H1e: Sanction celerity is positively related to information security compliance behavior.

2.2 Contextual Moderators

We identify two contexts that play an important role when conducting deterrence-based studies in the ISP context. We maintain that these contexts interact with the mechanisms of deterrence theory and, thus, can help explain inconsistencies in empirical findings. Table 2 briefly defines these contexts and offers examples from extant literature.

2.2.1 Behavior Types: Malicious vs. Non-Malicious Context and Compliance vs. Non-Compliance

As mentioned above, deterrence theory originally was conceptualized in criminology to predict criminal behavior (Gibbs 1975). Studies typically have been conducted in contexts involving theft, vandalism, bribery, white-collar crimes, or price rigging (Paternoster 1989; Paternoster and Simpson 1996). While deterrence studies typically describe situations concerning criminal and malicious behavior, information security research has applied the theory to a wider range of contexts (Willison et al. 2018a, b), including classical malicious non-compliance contexts—such as software theft, purposeful virus spreading, or sabotage (Harrington 1996; Peace et al. 2003); non-malicious non-compliance contexts, such as cyber loafing (Ugrin et al. 2011); and positive outcomes, such as general ISP compliance intentions (Herath and Rao 2009b).

We contend that sanctions exert a greater influence on ISP behavior in malicious non-compliance contexts than in non-malicious non-compliance contexts. In non-malicious contexts, the deviant behavior is not driven directly by a malicious motive, and a cognitive process that formulates a rational decision is not necessarily provided. To be more specific, before people deviate, e.g., from an Internet-usage policy, they do not weigh the costs and benefits of misbehavior, but rather follow a non-malicious idea. In their review on deterrence theory and ISP compliance behavior, Willison et al. (2018a, b) conclude "that the criminal roots of DT [deterrence theory] that are pertinent to ICA [internal computer abuse] are largely overlooked in current information security literature" (para. 6). We follow the basic idea of Willison et al. (2018a, b) and posit the following hypothesis:

H2a: Sanctions exert a greater influence on ISP non-compliance behavior in malicious contexts than in non-malicious contexts.

Moreover, we draw on D'Arcy and Herath's (2011, p. 651) distinction of ISP compliance as a positive or negative outcome variable. By positive behavior, i.e., ISP compliance behavior, D'Arcy and Herath (2011, p. 651) are referring "to behavior that is supportive of IS security, such as policy compliance." By negative behavior, i.e., both malicious and non-malicious ISP non-compliance, they are referring "to behavior that is considered disruptive of IS security, such as IS misuse […] or security policy violation […]." In line with their argumentation,

we suggest that deterrence is a better predictor of non-compliant behaviors opposed to compliant behaviors for the following reason. Compliance with ISPs in contrast to deliberate violation of ISPs is less likely a process of weighing benefits and costs, but rather a process of attachment to conventional norms (Cao 2004). Thus, for compliant behaviors, the influence of sanction mechanisms is more indirect. This includes other variables such as attitude, perceived behavioral control, and subjective norms (Bulgurcu et al. 2010a; Liao et al. 2009). Accordingly, we propose the following hypothesis:

> H2b: Sanctions exert greater influence on ISP non-compliance behaviors than on ISP compliance behaviors.

2.2.2 Culture: Low Power Distance vs. High Power Distance and Low Uncertainty Avoidance vs. High Uncertainty Avoidance

Deterrence theory alone does not incorporate the idea of culture. A rational actor who weighs costs and benefits does not take societal norms into account per se. However, behavioral research generally finds broad evidence for the effects of culture on decision making (Naor et al. 2010). Few studies have examined the role of culture on deterrence-based ISP compliance behavior (Hovav and D'Arcy 2012). Understanding the influence of culture not only helps explain the empirical discrepancy among studies, but also guides further deterrence-theory development.

The power distance of a society is a central cultural dimension and was found to be systematically different between countries (Hofstede 1980; Hofstede et al. 2010). *Power distance* refers to the degree to which members of organizations or institutions accept the legitimacy of unequally distributed power (Hofstede 1980). Extant research has highlighted the role of power distance on leadership outcomes, job attitudes, and counterproductive work behavior (Bochner and Hesketh 1994; Chao et al. 2011; Kirkman et al. 2009; Lian et al. 2012). For example, differences in employees' power-distance orientation have been suggested to influence how individuals perceive and react to authority. Employees high in power-distance orientation are more likely to respect and trust supervisors (Kirkman et al. 2009). Moreover, they tend to be submissive to organizational decisions (Bochner and Hesketh 1994). We contend that countries with low power distance differ from countries with high power distance in terms of how deterrence theory works in the context of ISP compliance behavior. More specifically, we argue that a high power distance leads to greater acceptance of rules and sanctions. This includes prescribed security behaviors that require dedicated effort and simultaneously might be in conflict with individual goals or habits. In contrast, employees in countries that are low in power distance are more likely to react adversely to perceived organizational injustice:

> H3a: Sanctions exert a greater influence on ISP compliance behavior in cultures with a high power distance than in cultures with a low power distance.

Moreover, we propose that a high degree of uncertainty avoidance increases sanctions' efficacy. *Uncertainty avoidance* is defined as the degree to which members of organizations or institutions feel uncomfortable with uncertainty or ambiguity (Hofstede 1980; Hofstede et al. 2010). Researchers already have investigated uncertainty avoidance's role in the context of decision making. For example, Ladbury and Hinsz (2009) finds evidence that higher degrees of uncertainty avoidance decrease risk taking. Hwang and Lee (2012) examine uncertainty avoidance's role in forming purchase decisions. We argue that sanctions as a mechanism to deter individuals from non-compliance work better for individuals with a high degree of uncertainty avoidance, as they are more risk-averse. If individuals fear uncertainty, they prefer the safe option, i.e., remaining ISP compliant, over the riskier option, i.e., being non-compliant with the chance of getting detected and facing an uncertain outcome. Accordingly, we contend that the sanction mechanisms better explain non-compliance in cultures with a high degree of uncertainty avoidance than in cultures with a low degree of uncertainty:

> H3b: Sanctions exert a greater influence on ISP compliance behavior in cultures with high uncertainty avoidance than in cultures with low uncertainty avoidance.

2.3 Methodological Moderators

To answer the third research question, we analyze how methodological factors might affect the study's results, picking two central choices in ISP compliance research design: how to capture behavior and the behavior's specificity. By considering these methodological variables as moderators for the moderator meta-analysis, we examine possible explanations for the variations across studies (Hunter and Schmidt 2004). An overview of the two methodological moderators is provided in Table 3.

2.3.1 Behavior-Based vs. Scenario-Based Measurement

In ISP compliance studies, we find two widely applied approaches for measuring behavior. The behaviorally

anchored approach aims to capture a real actor's behavior within her or his own context, while the scenario-based measurement puts an individual in a hypothetical situation. Each approach offers its own advantages and disadvantages (Moody et al. 2018). The behavior-based approach measures behavior in a real context, questioning respondents in relation to their specific organizational situations, such as whether they expect to follow the Internet usage policy (Li et al. 2014). Thus, it has a high level of external validity. Like the discussion around laboratory and field experiments (Busk 2005), behavior-based measurements are more grounded in reality, with a richer set of true contexts – both factors that lead to improved generalizability. The scenario-based measurement describes an imaginary situation, with respondents being asked how they would act if the scenario were real. This approach allows the researcher to better specify the context under study: While theoretical assumptions on the theory are controlled for, the propositions can be tested. For example, individuals can be set in different ISP violation contexts, and prospective behavior can be measured instantly (Siponen and Vance 2010). Moreover, as the individual under study is not questioned about her or his actual deviant behavior, he or she is less likely to conceal it, and concerns over intimidation might be minimized (Harrington 1996). Both having their merits, the choice of measurement for ISP compliance studies has been discussed widely (Bulgurcu et al. 2010b; Li et al. 2014; Moody et al. 2018; Siponen and Vance 2010). Consistent with the differing arguments and perspectives, we argue the following:

> H4: Behavior-based vs. scenario-based measurement contributes to the explanation of differences found in the relationship between sanctions and ISP compliance.

2.3.2 Measurement Specificity

A choice in research design is the specificity with which the behavior is measured (Siponen and Vance 2014). For example, some scholars measure specific ISP violations, such as deviant behavior tied to software piracy, Internet use policy, or clean desk policy (Li et al. 2010; Peace et al. 2003; Ugrin et al. 2011). For them, a violation of one of these specific policies is interpreted as a violation of the general ISP. Other studies measure ISP compliance on a general level. For instance, Bulgurcu et al. (2010b) measure general intention to comply with the ISP, while Humaidi and Balakrishnan (2015) measure ISP compliance behavior in regard to respondents' compliance in daily work. On one hand, specific measurement is advantageous in that the behavior can be better accessed from the respondent's memory, as it is clear as to which violation the respondent is considering (Moody et al. 2018). In the case of general measurement, the respondents must first build a concept of the more abstract term, then aggregate different sub-dimensions. On the other hand, a more general concept allows for better generalizability (Siponen and Vance 2014). In line with these views' divergence, we propose a final hypothesis:

> H5: The degree of measurement specificity in terms of a generic vs. specific context contributes to the explanation of differences found in the relationship between sanctions and ISP compliance.

3 Meta-analysis

This study employs a random-effects "meta-analysis of correlations" to test the main effect of deterrence theory (Hunter and Schmidt 2004, p. 73ff.). Building on a subset of analyses, a moderation meta-analysis then is used to assess the contextual and methodological attributes' moderating effects.

Meta-analysis is a statistical method that systematically aggregates primary studies' quantitative results and, in doing so, allows for higher-level statistical analysis of the measures of interest (King and He 2015; Rosenthal 1991). This methodology is particularly suitable for this analysis because it not only enables integration of findings from previous studies in a rigorous and quantitative fashion, but also allows for analysis of the effects from context-dependent factors and methodological choices. This helps in understanding inconsistencies among studies and consolidating contradictory findings.

The research design comprises three basic steps. First, we chose quantitative papers in ISP settings that cover deterrence constructs. In the second step, we used these papers to extract a database of studies and calculated a quantitative measure ("effect size") for the relationship between deterrence and ISP compliance behavior. The studies then were coded for selected variables of interest, i.e., type of deterrence construct, contextual factors, and methodological factors. This database comprises the basis for the following statistical analysis, which aims to identify and analyze the moderators.

The statistical analysis is built upon a random-effects model as presented in Hunter and Schmidt (2004). Their method allows the researcher to control for both sampling error and measurement error, thereby enabling the researcher to account for typical study artifacts and find "true" correlations among the variables of interest.

3.1 Data-Collection Procedure

The meta-analysis began with the identification of studies that reported sufficient data on the association between at least one

deterrence construct and compliance behavior. The procedure for data collection included searches through scientific databases, in addition to gathering studies from prior meta-analyses, which is consistent with the recommendations of Hunter and Schmidt (Hunter and Schmidt 2004), as well as other IS meta-studies (e.g., Gerow et al. 2014; Wu and Lederer 2009).

Publications were collected from January 2000 until March 2018. We began the search for such studies in Business Source Complete (EBSCOhost), ScienceDirect (Elsevier), ProQuest Dissertations & Theses database, and the Association for Information Systems Electronic Library (AISeL). The papers included in the analysis were identified using keywords such as "information security," "information systems security," and "IT security" in conjunction with terms such as "compliance," "behavior," or "deterrence theory." We used prior meta-analyses on information security behavior as an additional source of studies, screening the research from Sommestad et al. (2014), Sommestad et al. (2015), Cram et al. (2017), and Mou et al. (2017). Meta-analyses may be biased by the file-drawer effect (Rosenthal 1979), which refers to journals' tendency to publish significant results preferentially, thereby biasing exclusive journal-centric analyses' results (Dickersin 1990). To counteract this effect, conference publications and dissertations were included in the search.

Three inclusion criteria were applied for our final sample. First, the study must report relationships between a dimension of deterrence theory and ISP compliance behavior. For example, we disqualified studies that captured generic measures of sanctions (Siponen et al. 2007). Moreover, we ensured that the dependent construct explicitly covers information security compliance behavior. For example, we decided to drop Xue et al. (2011), who focus on ERP usage compliance. Second, the study must report sufficient information for later statistical analysis – specifically, information for deriving an effect size for the deterrence-behavior relation, data regarding sample size, and a precise description of the research context. As all this information was necessary for the subsequent coding procedure, we dropped, for example, Pahnila et al. (2007), as they do not state sufficient information to derive an effect size. Moreover, we looked exclusively at correlational effects, and effects from experimentally manipulated independent variables were not considered (e.g., Chen et al. 2013). However, some studies (e.g., Johnston et al. 2015) include a factorial design with changing vignettes to achieve a higher variation in the deterrence constructs. If these studies provided pure correlational information, they were included in the analysis. Importantly, we ensured that these outcomes were not restricted by the experimental effect. Third, we checked for each study's independence across all publications. When publications reported several studies based on independent data sets, they were treated as different studies (e.g. Moody et al. 2018). If different papers used the same set of data, all correlations were saved as if they were drawn from the same study. For the later analysis, composites were built at the stage of each individual computation.

The final sample comprises 34 publications, including 35 studies, published between 2003 and 2018. The sample sizes vary from 71 to 613 and comprise a total of 10,547 observations. The full list of research papers used for the database, including sample sizes and reported correlations between the independent variables and ISP compliance behavior, can be found in Appendix Table 7. An overview on the coding of the contextual variables can be found in Appendix Table 8.

3.2 Coding of Studies and Measurement of Variables

The coding procedure began with gathering data for the deterrence-behavior relationship. To measure this relationship's effect size, we coded for the correlation between the deterrence variable and ISP compliance behavior. The deterrence variable was coded according to the five dimensions of deterrence theory (i.e., formal sanction severity, informal sanction severity, formal sanction certainty, informal sanction certainty, and sanction celerity; see Table 1). The coding procedure for each study also included capturing information for the following context and study design variables:

The contextual moderators were coded according to the definitions provided in Table 2. The variable malicious vs. non-malicious context captures whether the context in the study is criminal or malicious. The systematization follows (Willison et al. 2018a, b; see Table A1). Three categories were distinguished: non-malicious; partially malicious; and malicious. Typical non-malicious contexts involve ISP compliance intentions, ISP violation intentions, or cyber loafing, while partially malicious contexts refer to situations such as information security misuse intentions or unauthorized access (D'Arcy and Hovav 2009; Hovav and D'Arcy 2012). As the variable malicious context was assigned only once in the database – in the context of computer abuse (Peace et al. 2003) – we decided to merge the categories partially malicious and malicious. The variable low power distance vs. high power distance is based on the country in which the sample was drawn. Based on the work of Hofstede et al. (2010) and their country-level power-distance values, all countries with a power distance below 50 were regarded as low power distance, and all studies equal or above 50 were regarded as high power distance. During coding, some papers were found to have drawn their samples from different countries. While some studies provide different correlations for their distinct populations (e.g., Brown 2017), most only provide aggregated correlations across the countries involved. If the aggregate includes both low and high power distance countries (e.g., Menard et al. 2018), this was coded as mixed and not considered further in the moderation analysis.

Table 1 Summary of deterrence theory constructs

Constructs	Definition	Representative measures
Formal Sanction Severity	Formal sanction severity is defined as the degree to which formal sanctions, in response to ISP violations, are perceived as harsh or problematic.	Representative construct names: perceived severity of sanctions (Hovav and D'Arcy 2012), deterrent severity (Son 2011) Example questionnaire item: "If I [did the act in the scenario], I would probably be sanctioned" (Cheng et al. 2013).
Informal Sanction Severity	Informal sanction severity is defined as the degree to which informal sanctions, in response to ISP violations, are perceived as harsh or problematic.	Representative construct names: informal sanctions – severity (Johnston et al. 2015), informal punishment severity (Moody et al. 2018) Example questionnaire item: "How much of a problem would it create in your life if you lost the respect of your managers for violating company information security procedures?" (Moody et al. 2018)
Formal Sanction Certainty	Formal sanction certainty is defined as the degree to which formal sanctions are perceived to be expected.	Representative construct names: certainty of detection (Herath and Rao 2009a), perceived punishment certainty (Dugo 2007) Example questionnaire item: "Employee computer practices are properly monitored for policy violations" (Herath and Rao 2009a).
Informal Sanction Certainty	Informal sanction certainty is defined as the degree to which informal sanctions are perceived to be expected.	Representative construct names: informal sanctions – certainty (Johnston et al. 2015), informal punishment certainty (Moody et al. 2018) Example questionnaire item: "How likely is it that you would jeopardize your promotion prospects if management learned that you had violated company information security policy?" (Siponen and Vance 2010)
Sanction Celerity	Sanction celerity is defined as the perceived promptness with which sanctions follow policy violations.	Representative construct names: GDT celerity (Lowry et al. 2015), sanction celerity (Johnston et al. 2015) Example questionnaire item: "I would be punished quickly for policy non-compliance" (Johnston et al. 2015).

Table 2 Summary of contextual moderators

Context	Definition	Representative examples
Behavior type: Malicious vs. Non-malicious ISP non-compliance behavior	A malicious context is one in which the attacker has a malicious motive and actively circumvents security mechanisms while expecting malicious consequences for the employer. In a non-malicious context, the motive is not malicious in nature, or the context predicts good behavior (i.e., ISP compliance).	Malicious: illegal copying of software (Lee et al. 2004), stealing confidential price and cost data (Hu et al. 2011), cracking and using computer services via misidentification (Harrington 1996). Non-malicious: cyber loafing (Ugrin et al. 2011), failing to lock or log out of workstations (Siponen and Vance 2010).
Behavior type: ISP compliance vs. non-compliance	Non-compliance behavior refers to behavior that deviates from prescribed rules in the ISP. This includes both malicious and non-malicious non-compliance. Compliance behavior refers to behavior in which prescribed ISP rules are followed.	ISP compliance: general compliance intentions (Herath and Rao 2009b), intentions to comply with Internet use policy (Li et al. 2010). ISP non-compliance behavior: illegal copying of software (Lee et al. 2004), cyber loafing (Ugrin et al. 2011)
Culture: Low power distance vs. high power distance	Low and high power distances are defined according to the country-level values for power distance from Hofstede et al. (2010). Low power distance includes all countries below the standardized mean of 50; high power distance includes all countries equal to or above the threshold of 50.	Countries with low power distance: US, Finland, Germany. Countries with high power distance: China, Korea, Indonesia, Taiwan.
Culture: Low uncertainty avoidance vs. high uncertainty avoidance	Low and high uncertainty avoidance is defined according to the country-level values for uncertainty avoidance from Hofstede et al. (2010). Low uncertainty avoidance includes all countries below the standardized mean of 50; uncertainty-avoidance distance includes all countries equal to or above the threshold of 50.	Countries with low uncertainty avoidance: China, Indonesia, US Countries with high uncertainty avoidance: Finland, Germany, Korea, Taiwan

We coded the methodological moderators according to the definitions given in Table 3. The first methodological moderator, behavior-based vs. scenario-based measurement, entails whether the authors used a hypothetical scenario. The information on measurement specificity was coded as generic or specific. *Generic contexts* refer to, e.g., general ISP compliance (Siponen and Vance 2010), while *specific contexts* refer to, e.g., software piracy (Brown 2017).

3.3 Data Analysis

This study relies on Hunter and Schmidt's (2004) method of meta-analysis, providing a random-effects estimator to account for sampling error resulting from the inclusion of different study sample sizes and study artifacts. By taking study artifacts into account, reported correlations can be corrected, thereby allowing true population correlations to be compared and aggregated across studies. Moreover, we decided to apply a random-effects instead of a fixed-effects estimator. The assumption on fixed-effects estimators is that one true correlation underlies all studies. Random-effects estimators allow the true correlation to vary among studies. Since the samples of our studies reveal some heterogeneity, e.g., in terms of age or gender distribution, and this might violate the assumption of a single true underlying correlation, we decided to use the more conservative random-effects estimator.

Table 3 Summary of methodological moderators

Methodological choices	Definition	Representative examples
Behavior- vs. scenario-based measurement	In behavior-based measurement, the respondent's behavior is measured in her or his real context. Scenario-based measurement refers to studies that introduce a hypothetical scenario in which the participant is set. The scenario describes a specific behavior, and the respondent then is asked to respond to the question as if he or she were that actor.	Example item in a behavior-based measurement: "I may/may not avoid committing Internet misuse in the future if I had the opportunity" (Liao et al. 2009). Example item in a scenario-based measurement: "What is the chance that you would do what [the scenario character] did in the described scenario?" (Siponen and Vance 2010)
Generic vs. specific measurement	A generic context refers to a measurement of general compliance behavior at the level of the ISP. In a specific context, the deviant behavior refers to a dedicated subset of the ISP.	Example item in a generic context: "I intend to comply with the requirements of the ISP of my organization in the future" (Bulgurcu et al. 2010a). Example item in a specific context: "I predict I will change my password within the next week" (Johnston et al. 2015).

Based on the initial coding of all available study correlations, grouping procedures were started for the direct hypotheses and each mediation hypothesis. First, all study correlations were allocated to one of the five deterrence constructs (H1a–e). Second, these groups were divided further according to their moderation variable (H2–H5). For each analysis, the subgroups still contained correlations stemming from the same study. To avoid a bias due to dependencies among the correlations, composite correlations and composite reliabilities were calculated for each study, reporting multiple correlations within one group (Hunter and Schmidt 2004).

To calculate true population correlations, we accounted for each study's measurement reliabilities in these subgroups. Different reliabilities in independent and dependent variables are important study artifacts that can attenuate reported correlations. Due to partly incomplete information on reliability scores in study reports, an attenuation factor was calculated based on artifact distribution. Correlations and subsequent variance analyses were corrected accordingly (Hunter and Schmidt 2004).

To evaluate the hypotheses, we estimated the true mean population correlations with mean rho values, which are point estimators of the average corrected correlation in the population and are calculated based on the sample size weighted and artifact-corrected correlations from the study database. Moreover, we decomposed the observed variance in our study database by estimating sampling-error variance and true variance in population correlation. Based on the true population variance, we computed credibility intervals. Credibility intervals "refer to the distribution of parameter values" (Hunter and Schmidt 2004, p. 205), thereby providing information on true correlations' homogeneity in the population. If the credibility interval is different from zero, this indicates that the true population correlations are positive or negative. We also computed confidence intervals. *Confidence intervals* "refer to estimates of a single value – the value of rho" (Hunter and Schmidt 2004, p. 205) and are based on the standard error of the estimated mean population correlation. The approach for meta-moderation analysis is based on the analysis of subsets. We used one-tailed *t*-tests for directed and two-tailed *t*-tests for undirected hypotheses to check whether the subsets stem from the same population.

4 Results

The results for the direct relationships can be found in Table 4. The estimated mean rhos for sanction severity,

Table 4 Results of the meta-analysis on ISP compliance behavior

Predictor	$\hat{\rho}$	k	N	Var._{ρ}	SD_r	Range r	$CV_{80\%}$	$CI_{95\%}$	PVA	Fail-safe N
H1a: Formal sanction severity	.289	28	8406	.039	.175	−.066, .54	.038, .54	.224, .354	.103	68
H1b: Informal sanction severity	.227	4	976	.021	.138	.007, .488	.041, .413	.092, .362	.207	9
H1c: Formal sanction certainty	.332	33	10,286	.031	.158	.02, .695	.108, .557	.278, .386	.121	88
H1d: Informal sanction certainty	.311	4	976	.024	.144	.054, .695	.114, .508	.17, .453	.184	10
H1e: Sanction celerity	.219	4	1838	.010	.096	.079, .325	.091, .346	.125, .313	.233	8

sanction certainty, and sanction celerity are all positive. For all five deterrence constructs, both credibility and confidence intervals are different from zero, supporting H1a–e.

Regarding the substantive power, we discerned no meaningful differences between the distinction of formal and informal sanctions for both sanction severity and certainty. The respective confidence and credibility intervals overlap highly. Accordingly, no evidence indicated a specific relationship between informal sanctions compared with formal sanctions.

$\hat{\rho}$ = sample size weighted mean of corrected population correlations; k = number of (composite) correlations; N = total sample size; $\text{Var.}\rho$ = variance of true score correlation ρ; SDr = standard deviation of sample size corrected correlation r; Range r = range of uncorrected correlations; CV80% = 80% credibility interval around true score correlation ρ; CI95% = 95% confidence interval around true score correlation ρ; PVA = percentage of variance accounted for by sampling and measurement error; Orwin's fail-safe N computed with a criterion correlation of .2.

The results for the moderator analysis for the contextual moderators are presented in Table 5. The results for the methodological moderators are depicted in Table 6. Due to the low number of studies on sanction celerity, it was not possible to conduct moderator analysis for this variable. Moreover, the moderator analysis does not differentiate between formal and informal sanctions, as we found no meaningful empirical difference in the prior analysis.

We find support for hypothesis H3a. The results reveal partial support, i.e., we either find a significant difference for sanction severity or sanction certainty, for hypotheses H2a and H3b. Furthermore, our exploratory analysis regarding H4 and H5 reveals no significant differences. We also find no notable variance drops in the respective subsamples, which might indicate the relevance of a moderator (Hunter and Schmidt 2004). Finally, we find partially contradictory results for H2b. Contrary to our expectations, our analysis suggests that sanction certainty is a better predictor in studies on ISP compliance than in studies on non-ISP-compliance.

5 Discussion

5.1 Summary of Findings

With this study, we aimed to synthesize the empirical findings from existing literature in the domain of deterrence-based ISP compliance behavior. We intended to explain inconsistent findings as being due to statistical study artifacts, contextual specifics, and methodological choices, and in doing so, guide future research. Below, we summarize the findings in light of the three research questions.

The first research question (RQ1) aimed to determine any overall effect from formal and informal sanction severity and sanction certainty, as well as sanction celerity, on security-compliance behavior when considering sampling error and study artifacts. We used a random-effects estimator, accounting for both sampling and reliability error. The literature in the study database includes studies with correlations close to zero or even negative (Guo et al. 2011; Johnston et al. 2015). However, when deducting the variance for sampling error and reliability, we find an overall positive distribution of correlations for all deterrence constructs. However, the average effect sizes can only be regarded as small to medium, with sanction celerity exhibiting the lowest effect. This finding, supported by sanction celerity's limited role in criminology research (Paternoster 1989), suggests its subordinate role in explaining ISP compliance behavior.

The second research question (RQ2) dealt with the question of whether study context can further explain differences in findings regarding the effect of deterrence constructs on ISP compliance behavior. Indeed, we find evidence that a malicious context better suits deterrence theory in terms of sanction severity. If the deviant behavior is malicious (or partially malicious) in nature, the estimated effect size of sanction severity rises from small to medium. Contrary to our expectations, we find that sanction certainty has a higher correlation with behavior in ISP compliance studies than in ISP non-compliance studies. It seems that regulating security behavior with sanction certainty works better for positive behaviors than for

Table 5 Results of the meta-analysis for contextual moderators

Predictor	$\hat{\rho}$	k	N	$Var._{\rho}$	SD_r	Range r	$CV_{80\%}$	$CI_{95\%}$	PVA	Fail-safe N
H2a: Behavior type - non-malicious < (partly) malicious context*								(partially supported)		
Non-malicious: severity	.242	18	5328	.022	.139	−.045, .53	.050, .434	.178, .307	.169	40
(Partly) malicious: severity	.403	10	3078	.032	.162	.095, .540	.173, .633	.303, .503	.114	30
t = −2.535, df = 26, $p < .05$										
Non-malicious: certainty	.360	21	6262	.028	.151	.02, .680	.147, .573	.295, .425	.137	59
(Partly) malicious: certainty	.298	12	4024	.033	.163	.022, .695	.064, .531	.205, .390	.107	30
t = .998, df = 31, n.s.										
H2b: Behavior type - ISP non-compliance > ISP compliance								(partially contradictory results)		
ISP compliance: severity	.281	12	3674	.019	.129	.078, .530	.105, .456	.208, .354	.188	29
ISP non-compliance: severity	.317	16	4732	.042	.182	−.045, .540	.055, .579	.228, .406	.096	41
t = −.530, df = 26, n.s.										
ISP compliance: certainty	.411	16	4731	.021	.135	.203, .680	.225, .596	.345, .477	.170	49
ISP non-compliance: certainty	.272	17	5555	.030	.157	.020, .695	.050, .494	.197, .346	.120	40
t = 2.483, df = 31, p < .05										
H3a: Cultures - low power distance < high power distance								(supported)		
Low PD: severity	.256	15	4255	.026	.147	−.045, .500	.051, .461	.182, .331	.156	34
High PD: severity	.368	7	1774	.034	.167	.010, .530	.133, .603	.244, .491	.130	20
t = −1.455, df = 20, $p < .10$										
Low PD: certainty	.291	19	5885	.014	.113	.020, .480	.143, .440	.241, .342	.242	47
High PD: certainty	.560	8	2024	.039	.176	.149, .695	.308, .812	.438, .682	.105	30
t = −4.443, df = 25, p < .05										
H3b: Cultures - low uncertainty avoidance < high uncertainty avoidance								(partially supported)		
Low UA: severity	.287	15	3685	.023	.144	−.045, .530	.091, .483	.214, .359	.186	36
High UA: severity	.293	7	2344	.042	.181	.004, .530	.032, .554	.159, .427	.088	17
t = −0.083, df = 20, n.s.										
Low UA: certainty	.317	19	5315	.023	.142	.020, .590	.121, .513	.253, .381	.167	49
High UA: certainty	.449	8	2594	.043	.183	.054, .695	.184, .713	.322, .575	.084	26
t = −1.837, df = 25, p < .05										

$\hat{\rho}$ = sample size weighted mean of corrected population correlations; k = number of (composite) correlations; N = total sample size; $Var.\rho$ = variance of true score correlation ρ; SDr = standard deviation of sample size corrected correlation r; Range r = range of uncorrected correlations; CV80% = 80% credibility interval around true score correlation ρ; CI95% = 95% confidence interval around true score correlation ρ; PVA = percentage of variance accounted for by sampling and measurement error; Orwin's fail-safe N computed with a criterion correlation of .2.; t = t-value of unpaired t-test of ρ-values for moderators; df = degrees of freedom; p = significance level of moderator test (one-tailed t-tests for directed and two-tailed t-tests for undirected hypotheses); n.s. = not significant (i.e., $p > .10$); PD = power distance; UA = uncertainty avoidance. *The partly malicious context also includes one study that was coded as malicious.

negative behaviors. One probable explanation can be found in prospect theory and the framing of losses and gains (Kahneman and Tversky 1979). The basic assumption is that people are risk-seekers when considering losses and are risk-averse when considering gains. Thus, it can be argued that employees who frame compliance as a positive behavior are risk-averse; thus, sanction certainty is a good control for such behavior. However, more research is necessary to examine this effect further.

The results also suggest that culture plays an important role when conceptualizing deterrence theory in the ISP context. For high power-distance countries, we find a substantially higher predictive power in sanctions. The estimated effect size for these countries compared with the whole sample increased from small to medium. Moreover, we find that sanction certainty better explains ISP compliance intentions in countries with a high level of uncertainty avoidance. Overall, the contextual moderators' results support Willison, Lowry, et al.'s (2018a, b) call for a reconceptualization of deterrence theory in ISP studies. While we find deterrence theory's explanatory power to be weak at the overarching level, the results suggest that closer conceptualization can improve it substantially.

The third research question (RQ3) aimed to identify methodological moderators on the relationship between deterrence and ISP compliance behavior. We tested two typical methodological choices. First, the results indicate

Table 6 Results of the meta-analysis for methodological moderators

Predictor	$\hat{\rho}$	k	N	$Var._{\rho}$	SD_r	Range r	$CV_{80\%}$	$CI_{95\%}$	PVA	Fail-safe N
H4: Behavior-based vs. scenario-based measurement									(no support)	
Behavior: severity	.271	18	5111	.023	.141	.010, .530	.077, .464	.206, .336	.170	42
Scenario: severity	.349	10	3295	.043	.183	−.045, .540	.084, .613	.235, .462	.086	27
t = −1.15, df = 26, n.s.										
Behavior: certainty	.373	21	6273	.038	.174	.022, .695	.125, .622	.299, .447	.103	60
Scenario: certainty	.276	11	3802	.015	.117	.020, .695	.118, .434	.207, .345	.204	26
t = 1.499, df = 30, n.s.										
H5: Generic measurement vs. specific measurement									(no support)	
Generic: severity	.291	8	2398	.020	.131	.095, .500	.111, .47	.199, .382	.184	20
Specific: severity	.305	20	6008	.037	.172	−.045, .540	.059, .552	.230, .381	.107	51
t = −.199, df = 26, n.s.										
Generic: certainty	.316	12	3683	.024	.142	.022, .480	.118, .514	.236, .396	.153	31
Specific certainty	.349	20	6392	.035	.168	.020, .480	.108, .590	.275, .422	.104	55
t = −.504, df = 30, n.s.										

$\hat{\rho}$ = sample size weighted mean of corrected population correlations; k = number of (composite) correlations; N = total sample size; $Var.\rho$ = variance of true score correlation ρ; SDr = standard deviation of sample size corrected correlation r; Range r = range of uncorrected correlations; CV80% = 80% credibility interval around true score correlation ρ; CI95% = 95% confidence interval around true score correlation ρ; PVA = percentage of variance accounted for by sampling and measurement error; Orwin's fail-safe N computed with a criterion correlation of .2.; t = t-value of unpaired t-test of ρ-values for moderators; df = degrees of freedom; p = significance level of moderator test (one-tailed t-tests for directed and two-tailed t-tests for undirected hypotheses); n.s. = not significant (i.e., $p > .10$); PD = power distance; UA = uncertainty avoidance. *The partly malicious context also includes one study that was coded as malicious

no substantial differences between scenario-based and behavior-based measurements. We would like to emphasize that this remains consistent from different empirical perspectives, including the subgroup distributions' width, variance reduction due to the breakdown in groups, and differences in estimated mean effects. We also find no clear evidence for specificity of the context. While the estimated mean values suggest that sanction severity fits better in a generic context, and sanction certainty fits better in a specific context, the differences are not significant in the sample. When interpreting both moderators' results in light of the research question, we find no evidence that the methodological choice substantially contributes to the explanation of differences across studies.

5.2 Limitations and Further Research

It is important to consider certain limitations when interpreting these results. First, in some cases, the results build on a limited number of studies. This holds particularly for informal sanction severity, informal sanction certainty, and sanction celerity. Simulation studies suggest that results from group sizes below 10 should be interpreted with caution (Switzer et al. 1992). Also, the subgroup analysis frequently led to small group sizes. To account for that threat, we conducted *ex ante* power analysis, computing the fail-safe N and dividing it by the number of studies used (Gerow et al. 2014). As sanction celerity is the only relationship for which that ratio is at the threshold of 2, the associated findings should be interpreted with particular caution. More research is needed to clarify its role. Second, due to only one study being classified as having a malicious context, we decided to merge the partially malicious context into this category. Thus, the category is a conservative estimator of malicious contexts. It should be noted that more data from malicious contexts might even strengthen differences in effect sizes. Third, our analysis of correlations aimed to gain maximal empirical information on the relation between sanction constructs and ISP compliance behavior, and it included studies that did not have this direct relationship model based on theoretical framing. Accordingly, other theoretical framings and empirical information on other mediating effects were not considered as part of this analysis. A broader perspective, e.g., on rational-choice theory and further mediating effects, would be an interesting avenue to better integrate the dispersed empirical observations. Finally, limitations stemming from correlational-based meta-analyses must be considered when interpreting the results (King and He 2015). This particularly holds for the publication bias and the sampling toward empirical studies. Although we included dissertations and conference papers to counteract the "publication bias," the reader should be aware of this threat when interpreting this meta-analysis. Moreover, meta-analyses only summarize findings from quantitative studies. In the analysis, findings from other types of research are not considered.

Further research with a broader perspective on the current body of knowledge is necessary to integrate the empirical and non-empirical findings.

5.3 Theoretical and Practical Implications

With the results, we provide several implications for research and practice. This study was motivated by a need to explain inconsistencies in the empirical literature that even have led to questioning deterrence theory's applicability in ISP compliance-behavior studies (D'Arcy and Herath 2011; Lowry et al. 2015). The findings from this study support the general application of deterrence theory in the field of information security research. The results clarify that a positive effect from deterrence theory exists across extant literature. Thus, we conclude that deterrence measures as implemented in most information security management systems are justified as one tool to control for compliance and, thus, require attention from information-system research. However, building on our analyses' small-to-medium effect size, we also empirically substantiate the claim that – without further reconceptualization of deterrence theory (Willison et al. 2018a, b) – salient individual and organizational factors might provide better foundations for explaining behavior that deviates from an ISP (Lowry et al. 2015).

Moreover, we could show that Willison, Lowry, et al.'s (2018a, b) call to reconceptualize deterrence theory can be a fruitful avenue. Our analysis provides evidence for both behavior types and cultural dimensions. Such reconceptualization can help identify areas in which sanctions can control behavior. Equally important, it also can show areas in which other types of controls might be necessary to align employees' security behavior with organizational security needs. Our results indicate that malicious ISP non-compliance can be regulated by deterring deviant behavior with tight sanctions. In turn, our results suggest a limited role for sanctions in deterring non-malicious ISP non-compliance. Future research is necessary to find mechanisms to better control this kind of behavior. Moreover, we contribute to future security-behavior literature and culture (Dinev et al. 2009; Hovav and D'Arcy 2012; Rocha Flores et al. 2015). Our results suggest that insights into cultural aspects' effect on deterrence theory's core mechanisms can contribute to understanding when deterrence theory works. At the country level, we find that sanctions work better in cultures with high power distance and high levels of uncertainty avoidance. Thus, we contribute to the question of whether and how deterrence theory is culturally dependent (Hovav and D'Arcy 2012). Building on this finding and following the call of Crossler et al. (2013), we suggest that future research should concentrate on individual differences in cultural dimensions, as propensity to national cultures can differ. This is particularly relevant to information security management, as the weakest link in the security chain can make a difference.

This study also informs researchers regarding the design of future studies on deterrence theory and ISP compliance behavior. If the theoretical reasoning justifies the use of scenarios to capture information security behavior, at least from an empirical perspective, then they provide adequate results as real behavior. This result is interesting, as a widespread discussion has surfaced about which type of measurement is preferable (Moody et al. 2018). At least from an empirical perspective, we conclude that both design choices seem to be equally well-suited. Of course, theoretical considerations should guide such a decision primarily.

Practice should pay close attention to deterrence theory's limited overall predictive power. Information security management systems often build on the simple premise that severe and likely sanctions deter employees from deviant behavior, but the results suggest that overarching policy design should not adhere to this simple presumption. Deterrence's strength seems to lie in specific types of behavior in specific cultural contexts. On the contrary, the effect on daily work behavior and in Western contexts appears to be small by comparison. Other approaches, e.g., motivational and social learning approaches, might be more favorable when aiming to align daily, routinized working misbehavior with the ISP.

6 Conclusion

Spurred by contradictory findings in the empirical literature, we examined the applicability of deterrence theory in ISP compliance behavior research. By integrating existing empirical findings using random-effects and moderation meta-analyses, we found strong evidence that, overall, deterrence theory has the power to explain deviant behavior in ISP studies. The greater the sanctions, the more likely they are, and the swifter they come, the more likely employees will adhere to ISP regulations. We also demonstrated that deterrence provides a better payoff in specific contexts: Malicious contexts, those of high power-distance cultures, and those of high uncertainty-avoidance cultures increase sanctions' explanatory power. Interestingly, we find no effect from methodological choices in terms of real or scenario behavior and generic or specific behavior. With the consolidated view on existing empirical literature, we hope to offer more specific guidance for further studies that conceptualize deterrence theory in the field of ISP in promising new ways.

Appendix

Table 7 Overview of studies

Study	n	Formal sanction severity	Informal sanction severity	Formal sanction certainty	Informal Sanction certainty	Sanction celerity
(Arunothong 2014)[a]	176	−.300		−.260		
(Arunothong 2014)[a]	613	−.540		−.260		
(Aurigemma and Mattson 2017)	239	.265		.212		
(Brown 2017) – Study 1	71	.449	.488	.318	.476	
(Brown 2017) – Study 2	72	.312	.380	.437	.497	
(Bulgurcu et al. 2010a)	464			.203		
(Chen et al. 2018)	231			.480		
(Cheng et al. 2013)	185	−.530		−.420		
(D'Arcy and Hovav 2009)	507			−.130, −.120		
(D'Arcy et al. 2009)	269	−.330		−.260		
(D'Arcy and Greene 2014)	127			.360		
(D'Arcy et al. 2014)	539	−.280		−.310		−.325
(Dugo 2007)	113	−.446		−.342		
(Foth 2016)	557	.350		.400		
(Guo and Yuan 2012)[b]	306	−.060		.025		
(Guo et al. 2011)[b]	306	−.030		.015		
(Herath and Rao 2009a)[c]	312	.248		.315		
(Herath and Rao 2009b)[c]	312	.240		.320		
(Hovav and D'Arcy 2012) – Study 1	366	−.340		−.300		
(Hovav and D'Arcy 2012) – Study 2	360	−.290		−.400		
(Hu and Xu 2018)	207	−.169		−.149		−.174
(Johnston et al. 2015)	559	−.066	.221	.224	.309	.156
(Kuo et al. 2017)	262	−.480		−.700, −.690		
(H. Lee et al. 2016)	211			−.247		
(W. Li and Cheng 2013)	428	−.180		−.590		
(H. Li et al. 2014)	241	.200		.270		
(H. Li et al. 2010)	246	.170		.260		
(Liao et al. 2009)	205	.220		.219		
(Lowry et al. 2015)	533	.095		.022		.079
(Moody et al. 2018) – Study 1	274	.000	−.007	−.054	−.054	
(Moquin and Wakefield 2016)	138	.500				
(Park et al. 2017)	123	−.010				
(Peace et al. 2003)	201	.120		.230		
(Posey et al. 2011)	439			.150		
(Son 2011)	602	.150		.260		
(Son and Park 2016)	209	.530		.680		
(Yoon and Kim 2013)	162			.480		

Table depicts the studies' sample size (n) and reported correlations between the independent variable and the ISP compliance behavior; [a, b, c] same sample

Table 8 Overview on study database and coding

Study	Country	Non-criminal (1), [Partial] criminal (2)	Complaince vs. Non-compliance	General Compliance (1) vs. Specific Compliance (2)	Actual (1) vs Hypothetical (2)
(Arunothong 2014)	USA	2	2	2	2
(Arunothong 2014)	Diverse	2	2	2	2
(Aurigemma and Mattson 2017)	USA	1	1	2	1
(Brown 2017) – Study 1	USA	1	1	1	1
(Brown 2017) – Study 2	USA	1	1	1	1
(Bulgurcu et al. 2010a)	USA	1	1	1	1
(Chen et al. 2018)	USA	1	1	1	1
(Cheng et al. 2013)	China	2	2	2	2
(D'Arcy and Hovav 2009)	USA	2	2	2	2
(D'Arcy et al. 2009)	USA	2	2	2	2
(D'Arcy and Greene 2014)	USA	1	1	1	1
(D'Arcy et al. 2014)	Diverse	1	2	2	2
(Dugo 2007)	USA	2	2	1	1
(Foth 2016)	German	1	1	1	1
(Guo and Yuan 2012)	USA	1	2	2	2
(Guo et al. 2011)	USA	1	2	2	2
(Herath and Rao 2009a)	USA	1	1	1	1
(Herath and Rao 2009b)	USA	1	1	1	1
(Hovav and D'Arcy 2012) – Study 1	USA	2	2	2	2
(Hovav and D'Arcy 2012) – Study 2	Korea	2	2	2	2
(Hu and Xu 2018)	China	1	2	2	2
(Johnston et al. 2015)	Finland	1	1	2	1
(Kuo et al. 2017)	Taiwan	2	2	2	1
(H. Lee et al. 2016)	Korea	1	1	n.a.	n.a.
(W. Li and Cheng 2013)	China	1	1	2	1
(H. Li et al. 2014)	Diverse	1	1	2	1
(H. Li et al. 2010)	Diverse	1	1	2	1
(Liao et al. 2009)	Diverse	1	2	2	1
(Lowry et al. 2015)	Diverse	2	2	1	1
(Moody et al. 2018) – Study 1	Finland	1	2	2	2
(Moquin and Wakefield 2016)	USA	1	1	1	1
(Park et al. 2017)	Korea	1	2	2	1
(Peace et al. 2003)	USA	2	2	2	1
(Posey et al. 2011)	USA	2	2	1	1
(Son 2011)	USA	1	1	1	1
(Son and Park 2016)	Korea	1	1	2	1
(Yoon and Kim 2013)	Korea	1	1	1	1

References

Alshare, K., Lane, P. L., & Lane, M. R. (2018). Information security policy compliance: A higher education case study. *Information and Computer Security, 26*(1), 91–108. https://doi.org/10.1108/ICS-09-2016-0073.

Arunothong, W. (2014). *Three research essays on propensity to disclose medical information through formal and social information technologies. ProQuest Dissertations and Theses*. University of Wisconsin Milwaukee. Retrieved from https://search.proquest.com/docview/1664611536?accountid=14169

Aurigemma, S., & Mattson, T. (2017). Deterrence and punishment experience impacts on ISP compliance attitudes. *Information & Computer Security, 25*(4), 421–436. https://doi.org/10.1108/ICS-11-2016-0089.

Baskerville, R., & Siponen, M. (2002). An information security meta-policy for emergent organizations. *Logistics Information Management, 15*(5/6), 337–346. https://doi.org/10.1108/09576050210447019.

Bochner, S., & Hesketh, B. (1994). Power distance, individualism/collectivism, and job-related attitudes in a culturally diverse work group. *Journal of Cross-Cultural Psychology, 25*(2), 233–257.

Brown, D. A. (2017). *Examining the behavioral intention of individuals' compliance with information security policies. Walden Dissertations and Doctoral Studies*. Walden University. Retrieved from http://scholarworks.waldenu.edu/dissertations%0Ahttp://scholarworks.waldenu.edu/dissertations/3750/

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010a). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523–548.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010b). Quality and fairness of an information security policy as antecedents of employees' security engagement in the workplace: An empirical investigation. In *Proceedings of the 43rd Hawaii International Conference on System Sciences* (pp. 1–7). https://doi.org/10.1109/HICSS.2010.312.

Busk, P. L. (2005). Field experiment. In B. Everitt & D. Howell (Eds.), *Encyclopedia of statistics in behavioral science* (pp. 650–652). Ltd: John Wiley & Sons.

Cao, L. (2004). *Major criminological theories: Concepts and measurements*. Wadsworth Publishing.

Chao, J. M. C., Cheung, F. Y. L., & Wu, A. M. S. (2011). Psychological contract breach and counterproductive workplace behaviors: Testing moderating effect of attribution style and power distance. *International Journal of Human Resource Management, 22*(4), 763–777. https://doi.org/10.1080/09585192.2011.555122.

Chen, X., Chen, L., Wu, D., & Perspective, A. (2018). Factors that influence employees' security policy compliance: An awareness-motivation-capability perspective. *Journal of Computer Information Systems, 58*(4), 312–324. https://doi.org/10.1080/08874417.2016.1258679.

Chen,Y., Ramamurthy, K., Wen, K.-W. (2013). Organizations' Information Security Policy Compliance: Stick or Carrot Approach?, *Journal of Management. Information Systems, 29* 157–188. https://doi.org/10.25300/MISQ/2018/13853.

Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers and Security, 39*(PART B), 447–459. https://doi.org/10.1016/j.cose.2013.09.009.

Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2017). Seeing the forest and the trees: A meta-analysis of information security policy compliance literature. In *Proceedings of the 50th Hawaii International Conference on System Sciences* (pp. 4051–4060).

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers and Security, 32*, 90–101. https://doi.org/10.1016/j.cose.2012.09.010.

Cuganesan, S., Steele, C., & Hart, A. (2018). How senior management and workplace norms influence information security attitudes and self-efficacy. *Behaviour and Information Technology, 37*(1), 50–65. https://doi.org/10.1080/0144929X.2017.1397193.

D'Arcy, J., & Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. *Information Management & Computer Security, 22*(5), 474–489. https://doi.org/10.1108/IMCS-08-2013-0057.

D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. *European Journal of Information Systems, 20*(6), 643–658. https://doi.org/10.1057/ejis.2011.23.

D'Arcy, J., & Hovav, A. (2009). Does one size fit all? Examining the differential effects of IS security countermeasures. *Journal of Business Ethics, 89*(SUPPL. 1), 59–71. https://doi.org/10.1007/s10551-008-9909-7.

D'Arcy, J., Hovav, A., & Galletta, D. F. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research, 20*(1), 79–98. https://doi.org/10.1287/isre.1070.0160.

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A coping Perspective. *Journal of Management Information Systems, 31*(2), 285–318. https://doi.org/10.2753/MIS0742-1222310210.

Dickersin, K. (1990). The existence of publication Bias and risk factors for its occurrence. *The Journal of the American Medical Association, 10*(263), 1385–1359.

Dinev, T., Goo, J., Hu, Q., & Nam, K. (2009). User behaviour towards protective information technologies: The role of national cultural differences. *Information Systems Journal, 19*(4), 391–412. https://doi.org/10.1111/j.1365-2575.2007.00289.x.

Dugo, T. M. (2007). *The insider threat to Organisational information security: A structural model and empirical test*. Auburn University. Retrieved from https://etd.auburn.edu/handle/10415/1345

Foth, M. (2016). Factors influencing the intention to comply with data protection regulations in hospitals: Based on gender differences in behaviour and deterrence. *European Journal of Information Systems, 25*(2), 91–109. https://doi.org/10.1057/ejis.2015.9.

Gartner. (2018). *Gartner forecasts worldwide information security spending to exceed $124 billion in 2019*. https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019

Gerow, J. E., Grover, V., Thatcher, J., & Roth, P. L. (2014). Looking toward the future of IT-business strategic alignment through the past: A meta-analysis. *Management Information Systems Quarterly, 38*(4), 1159–1185.

Gibbs, J. P. (1975). *Crime, punishment, and deterrence*. New York: Elsevier.

Guo, K. H., & Yuan, Y. (2012). The effects of multilevel sanctions on information security violations: A mediating model. *Information and Management, 49*(6), 320–326. https://doi.org/10.1016/j.im.2012.08.001.

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace:

A composite behavior model. *Journal of Management Information Systems, 28*(2), 203–236. https://doi.org/10.2753/MIS0742-1222280208.

Harrington, S. J. (1996). The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Quarterly, 20*(3), 257–278. https://doi.org/10.2307/249656.

Herath, T., & Rao, H. R. (2009a). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106–125. https://doi.org/10.1057/ejis.2009.6.

Herath, T., & Rao, H. R. (2009b). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154–165. https://doi.org/10.1016/j.dss.2009.02.005.

Hofstede, G. (1980). *Culture's consequences: International differences in work-related values*. London: Sage Publications.

Hofstede, G., Hofstede, G. J., & Minkov, M. (2010). *Cultures and organizations: Software of the mind*. New York: McGraw-Hill.

Hovav, A., & D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea. *Information and Management, 49*(2), 99–110. https://doi.org/10.1016/j.im.2011.12.005.

Hu, Q., & Xu, Z. (2018). The role of rational calculus in controlling individual propensity toward information security policy non-compliance behavior. In *Proceedings of the 51st Hawaii International Conference on System Sciences* (pp. 3688–3697).

Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM, 54*(6), 54–60. https://doi.org/10.1145/1953122.1953142.

Humaidi, N., & Balakrishnan, V. (2015). Leadership styles and information security compliance behavior: The mediator effect of information security awareness. *International Journal of Information and Education Technology, 5*(4), 311–318. https://doi.org/10.7763/IJIET.2015.V5.522.

Humaidi, N., Balakrishnan, V., & Shahrom, M. (2014). Exploring user's compliance behavior towards health information system security policies based on extended health belief model. *2014 IEEE Conference on e-Learning, e-Management and e-Services (IC3e)*, 30–35. https://doi.org/10.1109/IC3e.2014.7081237.

Hunter, J. E., & Schmidt, F. L. (2004). *Methods of meta-analysis: Correcting error and bias in research findings* (2nd ed.). Newbury Park: SAGE Publications.

Hwang, Y., & Lee, K. C. (2012). Investigating the moderating role of uncertainty avoidance cultural values on multidimensional online trust. *Information & Management, 49*(3–4), 171–176. https://doi.org/10.1016/j.im.2012.02.003.

ISO/IEC. (2013a). *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements* (Vol. 2013).

ISO/IEC. (2013b). *ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls* (Vol. 2013).

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly, 39*(1), 113–134. https://doi.org/10.25300/MISQ/2015/39.1.06.

Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica, 47*(2), 263–291.

King, W. R., & He, J. (2015). Understanding the role and methods of meta-analysis in IS research. *Communications of the Association for Information Systems, 16*(1), 665–686. https://doi.org/10.17705/1cais.01632.

Kirkman, B. L., Chen, G., Farh, J.-L., Chen, Z. X., & Lowe, K. B. (2009). Individual power distance orientation and follower reactions to transformational leaders: A cross-level, cross-cultural examination. *Academy of Management Journal, 52*(4), 744–764.

Kuo, K., Talley, P. C., Hung, M., & Chen, Y. (2017). A deterrence approach to regulate nurses' compliance with electronic medical records privacy policy. *Journal of Medical Systems, 41*(12), 198–208.

Ladbury, J. L., & Hinsz, V. B. (2009). Uncertainty avoidance influences choices for potential gains but not losses. *Current Psychology, 28*(3), 187–193. https://doi.org/10.1007/s12144-009-9056-z.

Lee, S. M., Lee, S. G., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information and Management, 41*(6), 707–718. https://doi.org/10.1016/j.im.2003.08.008.

Lee, H., Jeon, S., & Zeelim-Hovav, A. (2016). Impact of psychological empowerment, position and awareness of audit on information security policy compliance intention. In *Proceedings of the Pacific Asia Conference on Information Systems 2016* (p. 62).

Li, W., & Cheng, L. (2013). Effects of neutralization techniques and rational choice theory on internet abuse in the workplace. In *Proceedings of the Pacific Asia Conference on Information Systems 2013* (p. 169).

Li, H., Zhang, J., & Sarathy, R. (2010). Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems, 48*(4), 635–645. https://doi.org/10.1016/j.dss.2009.12.005.

Li, H., Sarathy, R., Zhang, J., & Luo, X. (2014). Exploring the effects of organizational justice, personal ethics and sanction on internet use policy compliance. *Information Systems Journal, 24*(6), 479–502. https://doi.org/10.1111/isj.12037.

Lian, H., Ferris, D. L., & Brown, D. J. (2012). Does power distance exacerbate or mitigate the effects of abusive supervision? It depends on the outcome. *Journal of Applied Psychology, 97*(1), 107–123. https://doi.org/10.1037/a0024610.

Liao, Q., Gurung, A., Luo, X., Li, L., Gurung, A., & Li, L. (2009). Workplace management and employee misuse : Does punishment matter ? Workplace management and employee misuse : Does punishment matter ? *Journal of Computer Information Systems, 50*(2), 49–59. https://doi.org/10.1080/08874417.2009.11645384.

Lowry, P. B., Posey, C., Bennett, R., Becky, J., & Roberts, T. L. (2015). Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust. *Information Systems Journal, 25*(3), 193–273. https://doi.org/10.1111/isj.12063.

Mahmood, M. A., Siponen, M., Straub, D., Rao, H. R., & Raghu, T. S. (2010). Moving toward black hat research in information systems security: An editorial introduction to the special issue. *MIS Quarterly, 34*(3), 431–433.

Menard, P., Warkentin, M., & Lowry, P. B. (2018). The impact of collectivism and psychological ownership on protection motivation: A cross-cultural examination. *Computers and Security, 75*, 147–166. https://doi.org/10.1016/j.cose.2018.01.020.

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly, 42*(1), 285–312. https://doi.org/10.25300/MISQ/2018/13853.

Moquin, R., & Wakefield, R. L. (2016). The roles of awareness, sanctions, and ethics in software compliance. *Journal of Computer Information Systems, 56*(3), 261–270.

Mou, J., Cohen, J., & Kim, J. (2017). A meta-analytic structural equation modeling test of protection motivation theory in information security literature. In *Thirty Eighth International Conference on Information Systems* (pp. 1–20).

Naor, M., Linderman, K., & Schroeder, R. (2010). The globalization of operations in eastern and Western countries: Unpacking the relationship between national and organizational culture and its impact on manufacturing performance. *Journal of Operations Management, 28*(3), 194–205. https://doi.org/10.1016/j.jom.2009.11.001.

Pahnila, S., Siponen, M., & Mahmood, M. A. (2007). Employees' behavior towards IS security policy compliance. In *Proceedings of the Annual Hawaii International Conference on System Sciences* (pp. 156–166). https://doi.org/10.1109/HICSS.2007.206.

Park, E. H., Kim, J., & Park, Y. S. (2017). The role of information security learning and individual factors in disclosing patients ' health information. *Computers & Security, 65*, 64–76. https://doi.org/10.1016/j.cose.2016.10.011.

Paternoster, R. (1989). Decisions to participate in and desist from four types of common delinquency: Deterrence and the rational choice Perspective. *Law & Society Review, 23*(1), 7–40. https://doi.org/10.2307/3053879.

Paternoster, R. (2010). How much do we really know about criminal deterrence. *Journal of Criminal Law and Criminology, 100*(3), 765–824.

Paternoster, R., & Simpson, S. (1993). A rational choice theory of corporate crime. In R. V. Clarke & M. Felson (Eds.), *Advances in criminological theory volume 5: Routine activity and rational choice* (pp. 37–58). New Brunswick: Transaction Books.

Paternoster, R., & Simpson, S. (1996). Sanction threats and appeals to morality: Testing a rational choice model of corporate crime. *Law & Society Review, 30*(3), 549–584.

Peace, A. G., Galletta, D. F., & Thong, J. Y. L. (2003). Software piracy in the workplace: A model and empirical test. *Journal of Management Information Systems, 20*(1), 153–177. https://doi.org/10.1080/07421222.2003.11045759.

Posey, C., Bennett, R. J., Roberts, T. L., & Lowry, P. B. (2011). When computer monitoring backfires: Invasion of privacy and organizational injustice as precursors to computer abuse. *Journal of Information System Security, 7*(1), 24–47.

Pratt, T. C., Cullen, F. T., Blevins, K. R., Daigle, L. E., & Madensen, T. D. (2006). The empirical status of deterrence theory: A meta-analysis. In F. T. Cullen, J. P. Wright, & K. R. Blevins (Eds.), *Taking stock: The status of criminological theory* (pp. 367–395). Piscataway: Transaction Publishers.

Puhakainen, P., & Siponen, M. (2010). Improving Employee's compliance through information systems security training: An action research study. *MIS Quarterly, 34*(4), 757–778.

Rocha Flores, W., Holm, H., Nohlberg, M., & Ekstedt, M. (2015). Investigating personal determinants of phishing and the effect of national culture. *Information and Computer Security, 23*(2), 178–199. https://doi.org/10.1108/ICS-05-2014-0029.

Rosenthal, R. (1979). The file drawer problem and tolerance for null results. *Psychological Bulletin, 86*(3), 638–641.

Rosenthal, R. (1991). *Metaanalytic procedures for social research* (2nd ed.). California: SAGE Publications.

Schatz, D., & Bashroush, R. (2017). Economic valuation for information security investment: A systematic literature review. *Information Systems Frontiers, 19*(5), 1205–1228. https://doi.org/10.1007/s10796-016-9648-8.

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

Siponen, M., & Vance, A. (2014). Guidelines for improving the contextual relevance of field surveys: The case of information security policy violations. *European Journal of Information Systems, 23*(3), 289–305. https://doi.org/10.1057/ejis.2012.59.

Siponen, M., Pahnila, S., & Mahmood, M. A. (2007). Employees' adherence to information security policies: An empirical study. In *Proceedings of the IFIP SEC* (pp. 133–144). https://doi.org/10.1007/978-0-387-72367-9_12.

Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance. *Information Management & Computer Security, 22*(1), 42–75. https://doi.org/10.1108/IMCS-08-2012-0045.

Sommestad, T., Karlzén, H., & Hallberg, J. (2015). A meta-analysis of studies on protection motivation theory and information security behaviour. *International Journal of Information Security and Privacy, 9*(1), 26–46. https://doi.org/10.4018/IJISP.2015010102.

Son, J.-Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information and Management, 48*(7), 296–302. https://doi.org/10.1016/j.im.2011.07.002.

Son, J.-Y., & Park, J. (2016). Procedural justice to enhance compliance with non-work-related computing (NWRC) rules: Its determinants and interaction with privacy concerns. *International Journal of Information Management, 36*(3), 309–321. https://doi.org/10.1016/j.ijinfomgt.2015.12.005.

Straub, D. (1990). Effective IS Securty: An empirical study. *Information Systems Research, 1*(3), 255–276. https://doi.org/10.1287/isre.1.3.255.

Switzer, F. S., Paese, P. W., & Drasgow, F. (1992). Bootstrap estimates of standard errors in validity generalization. *Journal of Applied Psychology, 77*(2), 123–129.

Ugrin, J. C., Pearson, J. M., & Odom, M. D. (2011). Cyber-slacking: Self-control, prior behavior and the impact of deterrence measures. *Review of Business Information Systems, 12*(1), 75. https://doi.org/10.19030/rbis.v12i1.4399.

Willison, R., Lowry, P. B., & Paternoster, R. (2018a). A tale of two deterrents: Considering the role of absolute and restrictive deterrence to inspire new directions in behavioral and organizational security research. *Journal of the Association for Information Systems, 19*(12), 1187–1216 http://www.ncl.ac.uk/business-school/staff/profile/robertwillison.html%0Ahttps://seanacademic.qualtrics.com/SE/?SID=SV_7WCaP0V7FA0GWWx%0Ahttps://ssrn.com/abstract=3099392.

Willison, R., Warkentin, M., & Johnston, A. C. (2018b). Examining employee computer abuse intentions: Insights from justice, deterrence and neutralization perspectives. *Information Systems Journal, 28*(2), 266–293. https://doi.org/10.1111/isj.12129.

Workman, M. (2009). A field study of corporate employee monitoring: Attitudes, absenteeism, and the moderating influences of procedural justice perceptions. *Information and Organization, 19*(4), 218–232. https://doi.org/10.1016/j.infoandorg.2009.06.001.

Wu, J., & Lederer, A. (2009). A meta-analysis of the role of environment based voluntariness in information technology acceptance. *Management Information Systems Quarterly, 33*(2), 419–432.

Xu, F., Luo, X. R., Zhang, H., Liu, S., & Huang, W. W. (2017). Do strategy and timing in IT security investments matter? An empirical investigation of the alignment effect. *Information Systems Frontiers*, 1–15. https://doi.org/10.1007/s10796-017-9807-6.

Xue, Y., Liang, H., & Wu, L. (2011). Punishment, justice, and compliance in mandatory IT settings. *Information Systems Research, 22*(2), 400–414. https://doi.org/10.1287/isre.1090.0266.

Yoon, C., & Kim, H. (2013). Understanding computer security behavioral intention in the workplace. *Information Technology & People, 26*(4), 401–419. https://doi.org/10.1108/ITP-12-2012-0147.

Simon Trang is an Assistant Professor and holds the Chair of Information Security and Compliance at the Department of Business Administration, University of Göttingen. He received his Ph.D. in management science, specializing in management information systems, from the University of Göttingen. His work focuses on information security management, inter-organizational IT alignment, and network collaborations. He has several years of industry experience in the area of strategic IT management and information security management. His research has been published or is forthcoming in outlets such as the Journal of the Association for Information Systems, Information Systems Frontiers, the Pacific Asia Journal of the AIS, and a number of refereed conference proceedings such as International Conference on Information Systems and European Conference on Information Systems

Alfred Benedikt Brendel is an Assistant Professor ("Akademischer Rat") at the Georg-August-University of Goettingen, Germany, and the current head of the Smart Mobility Research Group (SMRG). Alfred holds a Doctor's degree in Business Information Systems from the Georg-August-University of Goettingen. His research focuses on the application of Design Science Research to solve prevailing problems. His main areas of research are smart mobility, conversational agent design, gamification, and digital nudging