Journal Pre-proof

Effects of Sanctions, Moral Beliefs, and Neutralization on Information Security Policy Violations Across Cultures

Anthony Vance, Selvoy J. Boyer Fellow, Mikko T. Siponen, Detmar W. Straub

PII: S0378-7206(17)30701-2

DOI: https://doi.org/10.1016/j.im.2019.103212

Reference: INFMAN 103212

To appear in: *Information & Management*

Received Date: 11 August 2017

Revised Date: 18 September 2019

Accepted Date: 20 September 2019

Please cite this article as: Vance A, Fellow SJB, Siponen MT, Straub DW, Effects of Sanctions, Moral Beliefs, and Neutralization on Information Security Policy Violations Across Cultures, *Information and amp; Management* (2019), doi: https://doi.org/10.1016/j.im.2019.103212

Effects of Sanctions, Moral Beliefs, and Neutralization on Information Security Policy Violations Across Cultures

Anthony Vance

Danny & Elsa Lui Distinguished Associate Professor
Information Technology Management
Shidler College of Business
University of Hawaii at Manoa

Associate Professor

Selvoy J. Boyer Fellow

Information Systems Department
Marriott School of Management
790 TNRB

Brigham Young University

Provo, UT 84602

USA

Phone: +1 801-361-2531

Email: anthony@vance.name

Mikko T. Siponen

Department of Computer Science and Information Systems,

University of Jyväskylä

FI-40014 Jyväskylä

Finland

Detmar W. Straub

Professor and IBIT Research Fellow

Fox School of Business

Temple University

Regents Professor Emeritus

University System of Georgia & Georgia State University

ABSTRACT

A principal concern of organizations is the failure of employees to comply with information security policies (ISPs). Deterrence theory is one of the most frequently used theories for examining ISP violations, yet studies using this theory have produced mixed results. Past research has indicated that cultural differences may be one reason for these inconsistent findings and have hence called for cross-cultural research on deterrence in information security. To address this gap, we formulated a model including deterrence, moral beliefs, shame, and

neutralization techniques and tested it with the employees from 48 countries working for a large multinational company.

Keywords: Information security policy violations, information security, national culture, deterrence, shame, neutralization, moral beliefs

1 INTRODUCTION

Employees' noncompliance with information security policies (ISPs) has been recognized as a common and important problem in organizations (Siponen and Vance 2010; Willison and Warkentin 2013). To address this issue, information security scholars have tested different theoretical models, of which deterrence theory and protection motivation theory are among the most commonly used theoretical perspectives (D'Arcy and Herath 2011; Siponen and Vance 2014). However, with some exceptions (Hovav and D'Arcy 2012; Karjalainen et al. 2013), previous research on ISP violations has been conducted using subjects from a single country only. Consequently, our knowledge of the extent to which these local findings can be generalized across countries is limited. This information is important because IS security behavior is a worldwide, rather than local, problem. For example, in the context of protection motivation theory, results have been shown to vary between the US and Korea (Chen and Zahedi 2016). Moreover, one reason for the inconsistent findings of studies based on deterrence theory is believed to be cultural differences (D'Arcy and Herath 2011)—a claim that is empirically untested.

The facts that ISP violations are a worldwide problem and that previous research has found or suggested cultural differences among these theories stress the need to examine whether the models of ISP violations are generally consistent across cultures (Chen and Zahedi 2016; D'Arcy and Herath 2011). When selecting candidate theories for this type of cross-cultural investigation, deterrence theory is perhaps at the top of the list for two reasons. First, it is one of the most used theories in IS research (Cram et al. 2017), and second, it is believed that one of the reasons for the inconsistent findings in studies using deterrence theory in the context of ISPs is cultural differences (D'Arcy and Herath 2011).

Against this backdrop, we tested an integrated theoretical model incorporating the two types of sanctions explained by deterrence theory: (1) formal and (2) informal sanctions. Additionally, we included three rival theoretical nomologies: shame, moral beliefs, and

neutralization techniques. The combination of these three theory bases offers a contrast to the effects of sanctions. We added neutralization theory—which was introduced to the IS field by Siponen and Vance (2010)—to the model because recent studies have highlighted it as a factor that might explain why deterrence is ineffective (Barlow et al. 2018; Barlow et al. 2013; Siponen and Vance 2010; Willison and Warkentin 2013). In addition, moral beliefs, as suggested, for example, by D'Arcy and Herath (2011), are a viable competing explanation for deterrence theory. We empirically evaluated our model using a sample of employees from 48 countries working for a large multinational company.

Second, drawing on cultural psychology, our model led us to theorize that the factors of espoused national culture—namely, power distance, uncertainty avoidance, and individualism/collectivism—will moderate the effects of sanctions. Our results have the potential to contribute to IS research and practice by showing the extent to which popular IS security theories are empirically supported across national borders.

The rest of the paper is organized as follows: The current literature on employee compliance is explored briefly in the second section to demonstrate that most previous studies of ISP violations and computer abuse focus only on a single country. We then present the research model and respective research hypotheses. The fourth section describes the research method adopted for this study, followed by the results in the fifth section. In the final section, we discuss the implications for research and practice, along with the limitations of the study and directions for future research.

2 PREVIOUS RESEARCH ON ISP COMPLIANCE

Crossler et al. (2013) observed that most studies on security behavior only collect data from within a single country. Exceptions include Aurigemma et al. (2018), Chen and Zahedi (2016), and Dinev (2009), who found that national culture significantly influenced various security behaviors outside the context of ISP compliance. For ISP compliance specifically, Cram et al. (2019) found in their review of the ISP compliance literature that most research has also been conducted in single countries, such as Finland, the People's Republic of China, the Republic of Korea, and the US. Consequently, these studies have demonstrated that their models can be applied in one cultural setting but not across cultures.

Further, Cram et al. (2019) found significant differences in detection certainty and normative beliefs between the regions of Asia-Pacific and Europe/North America, as well as differences in response cost and threat severity between Europe and Asia-Pacific/North America. These differences suggest the need to test models of ISP compliance across cultures.

For this reason, Crossler et al. (2013) has called for research that examines ISP compliance across cultures. The four exceptions to this monoculture exploration of IS security policy compliance are Hovav and D'Arcy (2012), Kam et al. (2015), Karjalainen et al. (2013), and Menard et al. (2018) (see Table 1). All four of these studies demonstrate that differences in culture substantially influence security-related attitudes and intentions.

Table 1. Previous Cross-cultural Research on ISP Compliance

Study	Cultural comparison	Theory	Countries
Hovav and D'Arcy (2012)	Contrasted how deterrence constructs and moral beliefs explained misuse intention across two cultures.	Deterrence theory	South Korea and the US
Kam et al. (2015)	Examined how factors relating to organizational culture influenced employees' compliance with ISPs across two national cultures.	Cross value framework	South Korea and the US
Karjalainen et al. (2013)	Qualitatively compared how learning paradigms influence policy compliance across national cultures.	Learning paradigms	China, Finland, Switzerland, and the UAE
Menard et al. (2018)	Showed the impact of collectivism on intention to protect information that is consistent with the encouraged policy.	Protection motivation theory	China and the US

Although each of these studies has increased our understanding of the influence of culture on ISP compliance, gaps remain. First, with the exception of the qualitative study of Karjalainen et al. (2013), these studies did not measure individual-level cultural differences, instead using the Hofstede (2001) country indices to paint a broad brushstroke across each of the two studied countries instead of measuring cultural differences at the individual level. The problem with the Hofstede indices is that they suffer from the ecological fallacy that country means are used to explain individual behavior (Straub et al. 2002). At best, country averages provide only a gross estimator of effects. A superior approach measures the espoused cultural values at the individual level (Srite and Karahanna 2006). As Crossler et al. (2013, p. 94) explained:

> Hofstede's measures generalize an entire country to culturally have certain traits as compared to other countries. However, individuals within each country vary in their own traits in that particular area (Srite and Karahanna, 2006). Relying on a country-level assessment of an individual's culture could result in inaccurate findings if the individual's propensity to that cultural value did not match the overall values of the country.

Second, only D'Arcy and Hovav (2012) examined how the effects of deterrence theory differ across cultures. In a model comparing the US and the Republic of Korea, D'Arcy and Hovav (2012) found significant differences between employee violations in the two countries.

The influence of perceived certainty was stronger for Korean respondents, whereas the effect of perceived severity was stronger for respondents from the US. Additionally, Korean respondents reported higher misuse intentions overall. Interestingly, they found no difference in the effect of moral beliefs between the two countries. Although these results provide initial support for cultural differences and the effects of deterrence theory between these two countries, more research is needed to determine whether the inconsistent findings of deterrence theory across studies are because of cultural differences (D'Arcy and Herath 2011).

Third, most of the studies listed in Table 1 compare cultural differences in ISP compliance only between two countries, and only Karjalainen et al. (2013) compare differences across three countries. This means that our view of how cultural differences influence ISP compliance is still narrow. Thus, there is a need to understand how theories of IS compliance perform across various cultures (Crossler et al. (2013).

Fourth, the studies listed in Table 1 do not examine the effects of neutralization, shame, and moral beliefs (with the exception of Hovav and D'Arcy (2012)). Determining which models apply across cultures is needed to gain a full understanding of the role of sanctions (Chen and Zahedi 2016; Karjalainen et al. 2013). Solving this riddle empirically is important. Whether this claim is empirically valid offers an important avenue for future research and practice on IS security behavior that applies deterrence theory. If deterrence theory does not effectively apply across cultures, then researchers' goal of formulating explanations for employees' information security behavior should shift to alternative theoretical frameworks, which include moral beliefs or neutralization techniques (Siponen and Vance 2010; Vance et al. 2015).

We address these gaps by examining constructs from three theoretical models (deterrence theory, neutralization techniques, and moral belief) across employees from 48 countries. In doing so, we endeavor to make the first empirical test to determine which of these three theories generalizes best across cultures. We also aim to shed light on whether previous inconsistent results from other studies regarding deterrence theory can be explained by cultural differences.

3 THEORETICAL FRAMEWORK

Based on the aforementioned aim of the current study (section 2), our model consists of the following: (1) deterrence theory (formal and informal sanctions); (2) moral beliefs; (3) shame; and (4) neutralization. Moreover, drawing on cultural psychology, we theorize that the effects of deterrents will be moderated by factors of espoused national culture—namely, power distance,

uncertainty avoidance, and individualism/collectivism. Our research model is presented in Figure 1. We describe each component of our model in the following sections.

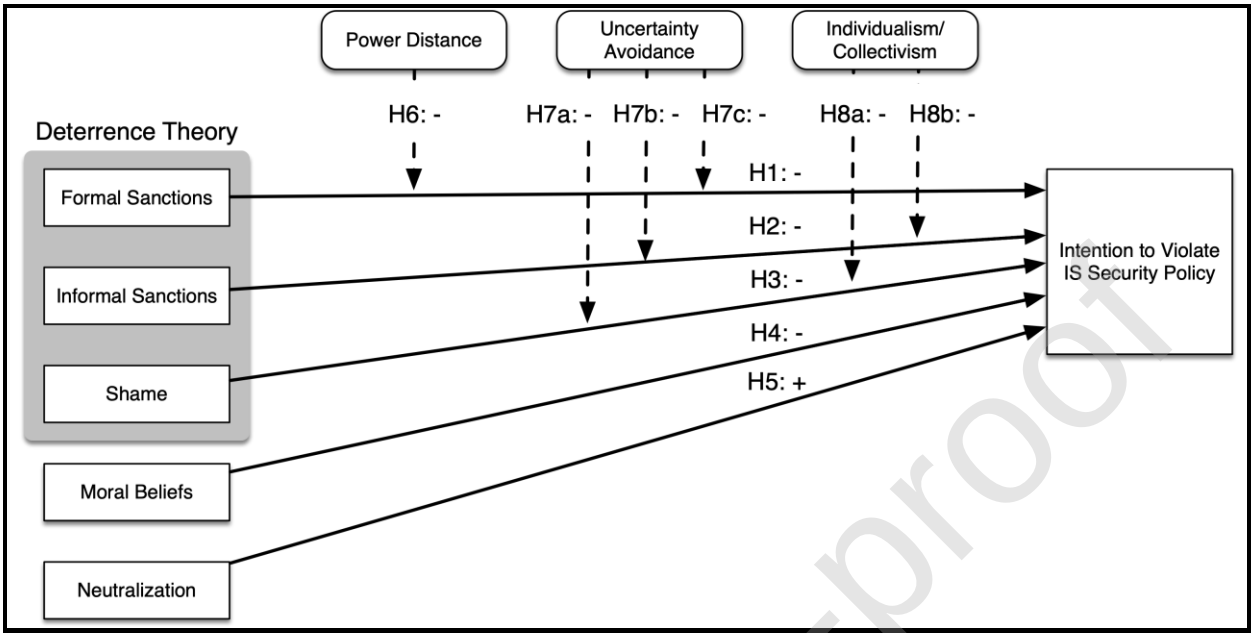

Figure 1: Research Model

3.1 Deterrence Theory

Deterrence theory assumes that people are self-interested actors who want to maximize utility and minimize disutility, such as those imposed by sanctions. Deterrence theory holds that individuals calculate the disutility of sanctions by considering their likelihood and severity (Becker 1974). A third calculation factor—the speed at which sanctions are implemented—was originally proposed by Beccaria but has received less attention from criminologists and IS scholars for both theoretical and methodological reasons (Nagin and Pogarsky 2001).

In IS, deterrence theory has been one of the most dominant theoretical perspectives used to study ISP compliance (Cram et al. 2017; D'Arcy and Herath 2011). However, despite this wide application, support for deterrence effects has been mixed. In their thorough review of the literature, D'Arcy and Herath (2011) observed that one factor leading to the mixed support of deterrence theory may be that studies have been performed in different countries. These mixed findings also motivate the current study of the cross-cultural analysis of deterrence theory.

Most research using deterrence theory has examined the role of formal sanctions, which are concrete penalties imposed by society (e.g., fines or imprisonment for criminal acts) or by employers (e.g., demotions or employment termination for policy violations). More recently,

scholars have also examined other deterrents, such as informal sanctions (Piquero and Tibbetts 1996), and have found them to be effective measures when it comes to dissuading individuals from engaging in deviant or undesirable behaviors. Here, informal sanctions refer to the disapproval of influential people for a given action (Paternoster and Simpson 1996). Accordingly, we incorporate the effects of formal sanctions and informal sanctions in our cross-cultural model, as follows:

H1: *Formal sanctions negatively affect intention to violate the ISP.*

H2: *Informal sanctions negatively affect intention to violate the ISP.*

3.2 Shame

Shame has been theorized and studied in the fields of criminology and psychology. In criminology, shame is sometimes regarded as a part of deterrence theory, working as a kind of self-imposed sanction (D'Arcy and Herath 2011). However, other scholars in criminology have questioned if shame fits within the theoretical framework of deterrence theory, which describes calculated pain avoidance (Akers and Sellers 2004). Given the criminology and deterrence background, we have included shame as a construct in our model. In fact, research on shame has been an active stream for the past 25 years (Kim et al. 2011; Lansky 1995); scholars have viewed shame as a universally applicable concept that functions through a self-assessment emotion (Tangney 1995). Shame is often conceptualized as a self-conscious emotion, one that results from feelings of worthlessness (Tibbetts 1997). More specifically, this self-conscious emotion can result from the difference between one's evaluation of oneself and the ideal picture of oneself. Based on previous research on shame, we hypothesize that shame could influence IS security behavior across cultures, as follows:

H3: *Shame negatively affects intention to violate the ISP.*

3.3 Moral Belief

Moral belief is based on the view that what people regard as morally right or wrong influences their intention and behavior (Hare 1965; Kohlberg 1981). The theoretical background of moral belief is grounded in the philosophy of ethics (e.g., Kantian ethics, universal prescriptivism, utilitarianism, information ethics; for a review, see (Siponen and Vartiainen 2002)) or religious ethics, such as the *agape*-based situational ethics of Fletcher (1966). However, within IS security research, previous work on moral beliefs has largely been conceptual, focusing on the debate as to whether an ethical discussion has any value in IS security. Kowalski (1990) was the first to suggest that ethics could be a common language for

computer users. Leiwo and Heikkuri (1998) criticized this view based on cultural relativism, claiming that ethical values differ from one culture to another and that they are incommensurable. On account of Hume's thesis of "no ought from is," Siponen (2002) argued that one cannot derive a normative theory from empirical observations. However, the Humean doctrine does not mean that we cannot study how moral beliefs or different ethical doctrines affect people's thinking (i.e., moral psychology). In moral psychology, the main focus has been on building and testing maturity models of moral reasoning as a process and how people can progress toward a higher level of maturity of moral reasoning through training interventions. The best known of these models is Kohlberg's (1984) theory of cognitive moral development. In turn, James Rest adapted Kohlberg's model to develop a quantitative instrument—the Defining Issues Test (DIT)—which has been widely adopted (Rest 1994). Myyry et al. (2009) tested Rest's DIT instrument in the ISP compliance context but failed to show that moral reasoning explains compliance intentions. However, although Rest has integrated different stages of Kohlberg's model together in DIT, it does not measure each stage of moral reasoning in terms of Kohlberg's (1984) stages.

Here, we argue that although individuals hold various moral beliefs and use various moral reasoning processes, there is a general moral belief behind these varying moral reasoning processes, and that the strength of this moral belief varies. The strongest statement regarding the influence of moral beliefs comes from Hare (1965), who viewed them as overriding, surpassing all other concerns, such as maximizing individual utility.

As an example of the overriding nature of moral belief, suppose that a person values money and that hacking online bank accounts could yield more money. Deterrence theory holds that this person would attempt to hack online bank accounts as long as the person's perception of sanction severity and certainty are sufficiently low for this crime. In contrast, the moral belief theories suggest that even if the certainty and severity of the sanctions are very low, a person will not hack the bank if he or she views this behavior to be morally wrong. If this is the case, we can claim that moral belief has overridden other concerns, such as individual utility maximization through financial gain (Hare 1965). Rest (1994) referred to this influence as moral motivation and claimed that it varies from person to person. We postulate that although the exact methods of moral reasoning may vary, concern for what is morally right and wrong is universal across cultures. For example, the method for moral reasoning can be egoistic or utilitarian. However, two people—one using the universality thesis and the second using utilitarian moral thinking—can arrive at different conclusions about the same moral issue because they use different

methods of moral thinking. However, despite their use of a different method for moral decision making, both of them may have a concern for morality. Based on this reasoning, we do not hypothesize that the relationship between moral beliefs and intention to violate the ISP is moderated by Hofstede's cultural dimensions. Given the universal nature of moral beliefs across cultures, we hypothesize the following:

H4: *Moral belief negatively affects intention to violate the ISP.*

3.4 Neutralization Theory

A competing theory to deterrence theory is neutralization, which was originally proposed by Sykes and Matza (1957), who identified five types of neutralization techniques: (1) denial of responsibility, (2) denial of injury, (3) denial of victim, (4) condemnation of the condemners, and (5) appeal to higher loyalties. Other neutralization techniques have been identified and studied in later studies (Maruna and Copes 2005; Willison and Warkentin 2013). Previous work in the field of criminology and IS indicates that employees may use neutralization techniques to rationalize their policy violations, allowing them to minimize the perceived harm of their actions (Piquero et al. 2005; Sykes and Matza 1957; Willison and Warkentin 2013). To be more precise, neutralization theory describes the use of various techniques to rationalize away or neutralize the wrongness of an act in a given situation, thereby allowing the commission of said act. Past IS research has shown that this rationalizing behavior may reduce the deterring effect of sanctions (Barlow et al. 2018; Barlow et al. 2013; D'Arcy and Herath 2011; Siponen and Vance 2010; Willison and Warkentin 2013).

In the context of ISP violations, Siponen and Vance (2010) found strong support for the effect of neutralization over and above that of formal and informal sanctions. Additionally, Willison and Warkentin (2013) posited that ISP compliance may especially be subject to the effects of neutralization techniques. For Sykes and Matza (1957), neutralization techniques are excuses and justifications to avoid moral guilt. In line with this research, we argue that these rationalizations occur in every culture, and for this reason, we do not hypothesize that the relationship between neutralization techniques and intention to violate the ISP is moderated by Hofstede's cultural dimensions. Accordingly, we hypothesize the following:

H5: *Neutralization positively affects intention to violate the ISP*.

3.5 Culture

In identifying patterns of values found in national cultures, Hofstede argued that culture is "the collective programming of the mind which distinguishes the members of one human group from another" (2001, p. 260). Although there have been criticisms of Hofstede's work, we find the values he identified as being a reasonable set for use across cultures.

Although personal values may be shared by many individuals within a national culture, it is important to note that "individuals vary greatly in the degree in which they espouse … values dictated by a single cultural group" (Straub et al. 2002, p. 18). Clearly, cultural values can be aggregated to the level of an entire culture, such as when we speak broadly about the existence of a Chinese cultural value of respect for one's ancestors, for example. Nevertheless, there will always be a distribution within countries regarding the strength of these values. Therefore, attributing country-level values to an individual (without measuring these values at the individual level) may be ecologically invalid (Robinson 1950). For this reason, gathering the individual cultural values that are espoused by individuals is a superior way of capturing cultural values (Srite and Karahanna 2006). Following this logic, we conceptualize the influence of culture at the individual level, consistent with Srite and Karahanna (2006).

We next hypothesize that the cultural values of individualism/collectivism, power distance, and uncertainty avoidance moderate the effects of formal sanctions, informal sanctions, and shame. Although other cultural dimensions have been identified by Hofstede (e.g., masculinity vs. femininity, long-term orientation, indulgence vs. restraint) and others (e.g., performance orientation, humane orientation, and assertiveness orientation of the GLOBE study; House et al. (2004)), we selected these three cultural values as moderators because we believe they are the most relevant to the area of ISP compliance. This view is supported by Crossler et al. (2013), who, in their review of the ISP literature, concluded that "current studies may need to be adapted to account for cross-cultural differences," specifically "uncertainty avoidance, collectivism-individualism, and power distance relationships" (p. 94).

3.5.1 Power Distance

Power distance refers to the extent to which status inequality is accepted as normal within a culture (Hofstede 2001) or the degree "to which employees accept that they have less power than their superiors" (Srite and Karahanna 2006, p. 687). The starting point for power distance is human inequality, which manifests through prestige and power (Hofstede 2001). Hofstede (2001) maintained that basic relationships between managers and subordinates in

organizations are influenced by the degree that power distance is upheld as a value in the national culture of the employees.

We theorize that power distance will moderate the degree to which the perceptions of formal sanctions influence the intention to violate the ISP. This is because one aspect of cultures that have a high power distance is the accepted use of sanctions, as Carl et al. stated:

> At one end of the spectrum, from a power distance perspective, is the use of coercive power, which focuses on the threat or application of punishments to enforce the leader's wishes. Organizational examples include the power to reprimand, suspend, demote, fine, or dismiss an employee. We tend to associate a domineering, autocratic leadership style with this leadership type (2004, p. 535).

Furthermore, Lian et al. (2012) found that individuals from cultures with a high level of power distance were more likely to accept abusive supervision, which includes the use of formal sanctions. These findings confirmed the speculations of Tepper (2007), who believed that a high level of power distance engenders an environment in which abusive supervision is socially acceptable.

Given these findings, we expect that formal sanctions will have greater efficacy for individuals who display high levels of power distance. This is because these individuals are more likely to view the use of formal sanctions as legitimate and socially acceptable, hence submitting to the threat of sanctions. Accordingly, we hypothesize the following:

H6: *The relationship between formal sanctions and intention to violate the ISP is moderated by the espoused national cultural value of power distance such that the relationship is stronger for individuals with higher espoused power distance cultural values.*

3.5.2 Uncertainty Avoidance

Uncertainty avoidance refers to "the degree to which members of a society feel uncomfortable with uncertainty and ambiguity" (Hofstede 2001, p. 83). According to Hofstede (2001), individuals from cultures that exhibit high uncertainty avoidance tend to minimize instances of uncertainty that arise through unexpected or unstructured situations. However, Hofstede found that individuals from cultures with low levels of uncertainty avoidance have less difficulty with ambiguity and lack of structure.

Additionally, research has shown that uncertainty avoidance is strongly associated with perceptions of risk (Doney et al. 1998; Sully de Luque and Javidan 2004). For example, research has shown that risk-taking behaviors (Weber and Hsee 1998), risk preferences (Weber and Milliman 1997), and probability judgments about uncertain events differ by national culture (Yates, 1998). Other research has shown that perceptions of gains and losses vary by uncertainty avoidance values that are inherent in the national culture (Bontempo et al. 1997). In the realm of IS, Srite and Karahanna (2006) showed that the relationship between social norms and intention to use IT is moderated by uncertainty avoidance. This finding indicates that uncertainty avoidance may also explain other behaviors involving normative behavior, such as ISP compliance.

In the context of ISP violations, we theorize that people who highly espouse the cultural value of uncertainty avoidance will be more responsive to the threat of formal and informal sanctions, as well as to shame. This is because the efficacy of the sanctions (whether formal or informal) is based on individuals' perceptions of the probability and severity (i.e., risk) of those sanctions (Paternoster and Simpson 1996). Furthermore, people who espouse high levels of uncertainty avoidance (who value certainty) are concerned with future consequences and eschew risk (Sully de Luque and Javidan 2004). Thus, we expect that the efficacy of sanctions will vary with individuals' tolerance of risky situations, which will be influenced by their espoused level of uncertainty avoidance. Similarly, we also hypothesize that the influence of shame will be greater for individuals with higher espoused uncertainty avoidance cultural values. Accordingly, we hypothesize the following:

H7a: *The relationship between formal sanctions and intention to violate the ISP is moderated by the espoused national cultural value of uncertainty avoidance such that the relationship is stronger for individuals with higher espoused uncertainty avoidance cultural values.*

H7b: *The relationship between informal sanctions and intention to violate the ISP is moderated by the espoused national cultural value of uncertainty avoidance such that the relationship is stronger for individuals with higher espoused uncertainty avoidance cultural values.*

H7c: *The relationship between shame and intention to violate the ISP is moderated by the espoused national cultural value of uncertainty avoidance such that the relationship is stronger for individuals with higher espoused uncertainty avoidance cultural values.*

3.5.3 Individualism/Collectivism

An important factor that may differentiate one employee from another is an employee's relative orientation when it comes to individualism versus collectivism. The fundamental difference between individualists and collectivists lies in how one constructs him- or herself (Wasti 2003). Individualists (also known as ideocentrics) perceive themselves as independent from a larger group, place a high priority on personal goals and objectives, and engage in thoughts, behaviors, and emotions oriented to their own beliefs with relatively little reference to others (Markus and Kitayama 1991). Conversely, collectivists view themselves as dependent on a larger group and place a high priority on the needs and welfare of the whole above their individual needs and desires. Studies have found that an ideocentric worldview will lead to actions that are distinct from a more collectivist perspective; collectivists are more likely to suppress their own individual desires and goals in favor of promoting and supporting the goals of the collective group.

An employer (organization) can be seen as a collective group. Collectivists may act altruistically and would be more likely to demonstrate stewardship behavior (House et al. 2004), whereas individualists may introduce greater transaction costs, which are associated with agency relationships, because they will be more likely to act as agents. Individualists will generally act in the interests of the organization when the right combination of governance mechanisms (e.g., rewards and sanction) and social influence are present (House et al. 2004).

The extent to which an organization can encourage alignment between its employees' actions and the actions that ensure organizational security is an important determinant of overall enterprise security, especially given that compliant insider actions are paramount in ensuring security (Warkentin and Willison 2009). Furthermore, governance mechanisms that recognize this important distinction will be more effective in ensuring that organizational goals are achieved. In the context of ensuring the security of organizational data and IT systems, an individual whose social behavior is primarily guided by personal goals is more inclined to exhibit a different decision process than collectivist individuals. If true, this would indeed require a customized approach to personnel managerial actions.

The powerful forces of shame, sanctions, and moral beliefs have been theorized as forces that can provide strong direct impacts on the dependent variable (intention to violate ISPs), whereas the relative degree of individualism/collectivism is presumed to dampen or heighten those direct effects. The roles of shame and informal sanctions are closely related to the concept of social norms or social influence; it is the collective that influences individual

behavior, especially among individuals who hold a more collective cultural value. For such individuals, the norms of the collective body have greater salience, and these individuals have been found to be more compliant with these norms (Bond and Smith 1996; Hui and Triandis 1985; Markus and Kitayama 1991; Triandis 1989). Accordingly, the following hypotheses are presented:

H8a: *The relationship between informal sanctions and intention to violate the ISP is moderated by the espoused national cultural value of individualism/collectivism such that the relationship is stronger for individuals with espoused collectivistic cultural values.*

H8b: *The relationship between shame and intention to violate the ISP is moderated by the espoused national cultural value of individualism/collectivism such that the relationship is stronger for individuals with espoused collectivistic cultural values.*

4 METHOD

To empirically examine ISP violations, we employed an experimental scenario method that gave subjects a hypothetical situation; this was followed by asking them how likely they would behave in the same way under similar circumstances. We chose this method because it is common in ISP compliance research (Siponen and Vance 2014). Because of this, our research is somewhat comparable with many of the previous studies using deterrence theory and neutralization. The scenario method provides a less threatening way of measuring ISP intentions than asking employees to self-report their own violations directly (Barlow et al. 2013; D'Arcy et al. 2009; Guo et al. 2011; Hu et al. 2011; Siponen and Vance 2010). Furthermore, scenarios provide a way to increase generalizability by incorporating a variety of situations into multiple scenarios (Siponen and Vance 2014). Finally, our model can be regarded as an extension of Siponen and Vance (2010), and accordingly, our measures are in line with that study.

The current research was conducted at and in collaboration with a large multinational corporation, and the scenarios were developed together with the research team and the company's information security manager. For this reason, the scenarios were not replications of previous scenarios, such as in Siponen and Vance (2010). Accordingly, we developed six scenarios describing different ISP violations (see Table A1 of Appendix A) in collaboration with the security manager of the target organization (described in section 4.2). All of the scenarios described violations of the target organization's ISP (described in 4.2) and were problematic in

terms of employee compliance, according to the professional opinion of the information security manager.

Given our objective to study constructs previously examined by ISP studies, the items were drawn from the literature (see Table A2 of Appendix A). Consistent with Siponen and Vance (2010), we calculated composite deterrence measures by multiplying responses to severity and certainty items together for each deterrence construct. This yielded sanction measures that "reflected both the risk and cost of perceived punishment" (Nagin and Paternoster 1993, p. 481).

Following the guidelines of Petter et al. (2007), we applied the four decision rules of Jarvis et al. (2003) to our instrument prior to data collection to determine whether the items were reflective or formative in nature. This process showed that the neutralization technique items were formative because they: (1) cause the formation of the construct, (2) are not interchangeable, (3) do not necessarily covary, and (4) do not have the same antecedents and causes. All other items in the instrument were identified as reflective. This designation is consistent with Siponen and Vance (2010), who found empirical support for the formative measurement of neutralization. In this study, the overall cultural study design followed the same design as the seminal culture study by Srite and Karahanna (2006). In addition to questions relating to the theoretical antecedents in our model, we also gathered data on subject demographics, such as age, gender, and years of work experience.

4.1 Pretest and Pilot Test

To ensure the validity of our instrument, we performed both a pretest and a pilot test (Boudreau et al. 2001). First, a paper-based pretest was administered to 86 graduate and undergraduate students at a large Finnish university. We then made changes to the instrument to improve the reliability and validity of the instrument, such as by removing items belonging to the constructs of moral beliefs (one item), individualism/collectivism (one item), and uncertainty avoidance (three items). With these items removed, we piloted our experimental instrument in its final form to approximately 400 international students studying at the same Finnish university. The students were solicited via email to take the survey and were entered into a prize drawing for doing so. Of this sampling frame, 71 people completed the final questionnaire (a response rate of 17%). The results of the pilot test analysis indicated that additional items could be dropped but that all constructs exhibited sufficient factorial validity (e.g., the square root of the average variance extracted were larger than correlations with any other construct in the model)

and reliability (i.e., Cronbach's α above .84) for at least two items per construct. With these results, we proceeded with our primary data collection.

4.2 Primary Data Collection

Primary data were collected from a large multinational corporation. An invitation to fill out the web-based instrument was posted by management across a variety of corporate intranets. There was no way to know how many employees saw the intranet message, but the company estimated that 5,000 employees worldwide saw it. Participation in the survey was voluntary. Incentives were given to the subjects, who were told they would be entered into a prize drawing upon survey completion. Participating in the drawing was optional. Participation in the drawing asked identifiable information, but this information was not connected to the survey responses. Employees were informed about this.

After 3 weeks, we collected responses from 615 employees in 48 countries (see Appendix B for the frequency of subjects by country). Given the number of employees who potentially could have responded, the response rate was 12%. However, because not all employees regularly visit the corporate intranets, it is reasonable that the population from which the sampling frame was drawn was far less than 5,000, even perhaps below 4,000. Therefore, the response rate was likely in excess of 12%, perhaps as much as 20% or more of those who viewed the invitation.

In general, a low response rate is not a serious problem as long as the sample received is representative of the population. To test for this, we assessed the nonresponse bias. Here, late subjects are frequently assumed to be similar to nonsubjects (Armstrong and Overton 1977), so we compared those who responded in the first week of the survey (early subjects) to those who answered during the final week of the survey (late subjects). An independent *t*-test comparing intention to violate the security policy (the dependent variable) for these two groups showed no significant difference (t = -1.264, df = 399, p = .207). We therefore concluded that the nonresponse bias was not likely to be a significant factor in our analysis.

5 RESULTS

We analyzed our theoretical model using partial least squares (PLS) with SmartPLS version 3.2.7 (Ringle et al. 2015). We chose a components-based structural equation modeling (SEM) technique rather than a covariance-based SEM technique because of its ability to handle formative constructs (Ringle et al. 2012). We rigorously validated our model according to the

standards for PLS research (Gefen et al. 2011), which we document in Appendices C. The tests for common methods bias are discussed in Appendix D.

The results of our theoretical model testing are depicted in Figure 2.

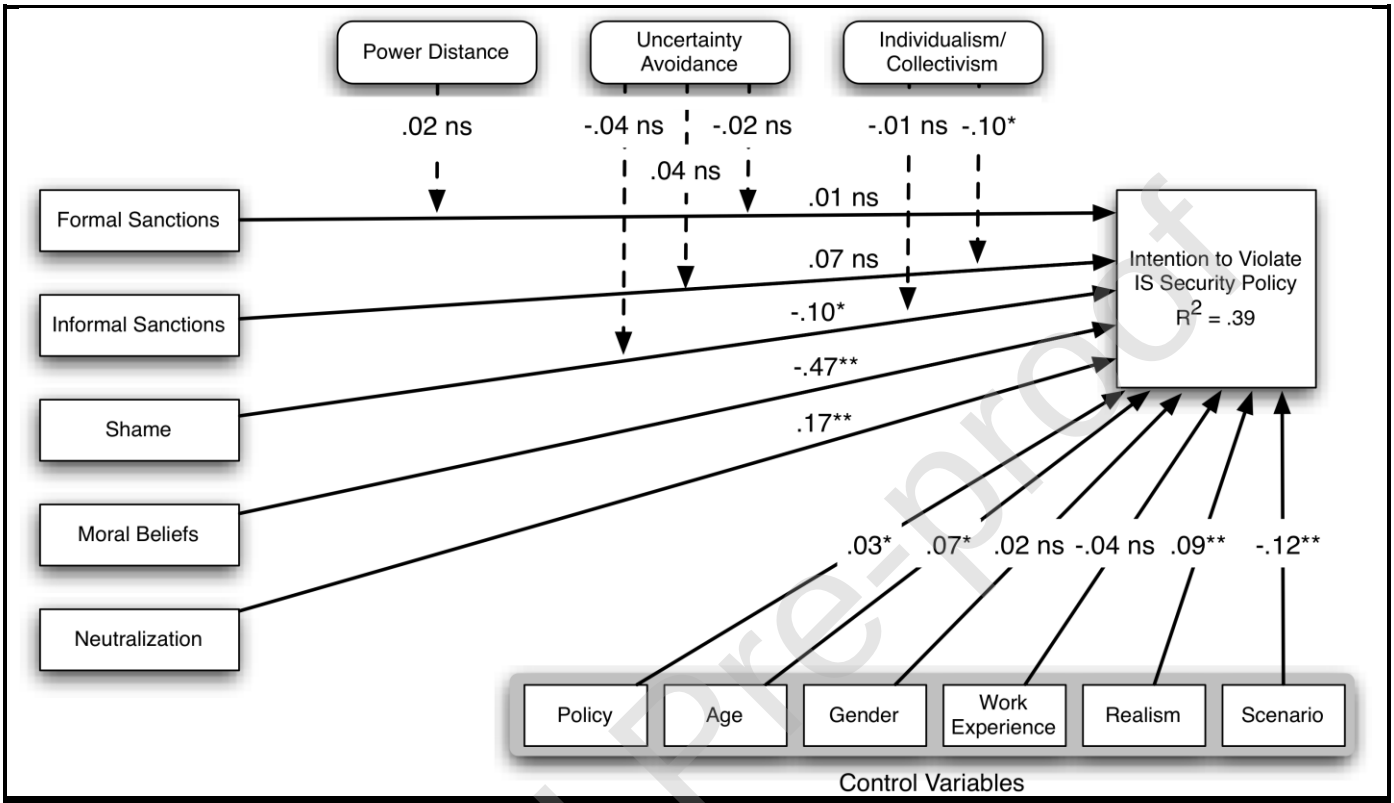

Figure 2. Research Model Showing the Results of the PLS Analysis.
N.B.: ns = Not significant, * p <.05, ** p <.005

5.1 Planned and Unplanned Control Variables

We controlled the effects of three demographic variables (age, gender, and work experience) for intention to violate the ISP. Additionally, because we found perceived realism and intention to be significantly correlated (r = .14, p < .001), we controlled for the perceived realism of the scenarios as well.

We also controlled for the type of scenarios received. Each participant randomly received one of six scenarios. A one-way ANOVA (F = 11.22, p < .001) showed that the average of the intention items varied significantly across all of the scenarios received ("reading confidential documents" had the highest average at 2.99, followed by "using unencrypted portable media" at 2.81, "sharing passwords" at 2.73, "failing to report a computer virus" at 2.03,

"allowing children to play on a laptop" at 1.69, and "using portable media from an unknown source" at 1.31).

Finally, we randomly included text in the scenarios, stating that the character in the scenario recognized that the behavior in question was an ISP violation (see Table A1 in Appendix A). This allowed us to determine the effect of the subject knowing that an ISP violation was involved (Siponen and Vance 2014). Collectively, these variables explained 4.9% of the variance of *intention*. However, only perceived realism and scenario type had significant path coefficients (.09 and -.12, respectively, $p < .005$). When entered into the model alone, the control variables together explained only .029% of the variance in intention to violate the ISP.

5.2 Deterrence Effects

For the deterrence constructs in the model, formal and informal sanctions were hypothesized to negatively influence intention to violate the ISP. In our empirical test of the model, formal and informal sanctions were not significant; thus, H1 and H2 were not supported.

We next examined the additive explanatory contribution of the deterrence constructs by modeling the change in R^2. To perform this test, the size of the effect of adding a moderating relationship to the model was calculated as: $f^2 = (R^2_{\text{Direct model}} - R^2_{\text{Moderation Model}})/(1 - R^2_{\text{Moderation Model}})$ (Chin et al. 2003). Next, a pseudo f-test was calculated by multiplying the effect size (f^2) by ($n - k - 1$), where n is the sample size and k is the number of independent variables (Mathieson et al. 2001). Our results showed that R^2 significantly increased ($p < .001$) by .053 to .130, representing a small effect size of .055 (Cohen 1988).

5.3 Neutralization, Shame, and Moral Beliefs

Our model indicated that shame negatively influences the intention to violate the ISP. The results show that the effect of shame was significant (-.12, $p < .025$), supporting H3. We also theorized that moral beliefs and neutralization would directly influence intention to violate the ISP. As theorized, moral beliefs had a strong negative influence on intention (-.47, $p < .001$), by far the largest effect in the model. Thus, H4 was supported. Also, neutralization had a strong positive effect on intention and was also significant (.20, $p < .001$), supporting H5. When neutralization was added to the model, R^2 significantly increased ($p < .001$) by .093 to .223, representing a small-to-medium .12 effect size (Cohen 1988). Finally, when moral beliefs were added to the model, R2 increased from .140 to .363, an effect size of .220, again a small-to-medium effect, but the largest additive effect in our model (Cohen 1988).

To summarize, the standardized beta coefficient for neutralization was .20, less than half the magnitude of moral beliefs (-.47). Shame was significant at a weaker effect of -.12, but both formal and informal sanctions were insignificant at .01 and .07, demonstrating weak effects. Thus, deterrence did not perform well in our model, but moral beliefs had a powerful effect, as did neutralization (with a moderate effect).

5.4 Moderation Effects

We also hypothesized that three cultural factors would negatively moderate the deterrence effects of the model. We tested these moderating effects using the product indicator approach established by Chin et al. (2003). First, power distance was hypothesized to negatively moderate the effect of formal sanctions on intention. However, this effect was not significant; thus, H6 was not supported. Second, uncertainty avoidance was hypothesized to negatively moderate the effects of formal sanctions, informal sanctions, and shame. Therefore, H7a–H7c were also not supported. Third, individualism/collectivism was hypothesized to negatively moderate the effects of informal sanctions and shame. The moderating effect on shame was insignificant, failing to support H8a. However, the moderating effect on informal sanctions was significant, supporting H8b.

To evaluate the strength of the moderating effect, we calculated the change in R^2, or the additional variance explained by the moderating effect beyond what was explained by the direct effects (Carte and Russell 2003). Although the size of the effect was small (.02) (Cohen 1988), the change in R^2 was significant ($F = 13.49$, $p < .005$). For comparison, in their 30-year review of moderating effect sizes, Aguinis et al. (2005) found that the median effect size of moderation effects was .002. Therefore, we conclude that that individualism/collectivism had a significant and substantive moderating effect on the relationship between informal sanctions and intention.

Finally, as an exploratory test, we tested whether power distance, uncertainty avoidance, and individualism/collectivism moderate the effects of moral beliefs or neutralization. However, no significant moderating effect was found despite a post-hoc power analysis showing that we had power well above the .80 recommended threshold. This suggests that the effects of these constructs are stable across these studied cultural dimensions.

6 DISCUSSION

The key contribution of the current paper is the examination of to what extent moral belief, neutralization, deterrence theory, and shame may explain employees' intention to violate

ISP across cultures and how some cultural variables may moderate sanctions and shame. More precisely, we highlight the below findings.

First, prior studies have had inconsistent findings when applying deterrence theory to ISP violations, which may be partially attributable to cultural differences (D'Arcy and Herath 2011). As a result, the examination of whether cultural differences explain the mixed findings of past deterrence studies has been called for (D'Arcy and Herath 2011). The current study, involving 615 individuals in 48 countries, shows that the relationship between both (1) formal and (2) informal sanctions and intention to violate the ISP are not statistically significant. That is, neither formal nor informal sanctions effectively explain employees' intention to comply with the ISP. However, the exception is informal sanctions for those who espouse a high collectivistic cultural value, as people in Asian countries tend to do.

Second, our findings indicate that moral belief had a negative influence on intention to violate—the strongest effect in our model. In other words, people who viewed the violation of an ISP as morally wrong reported low intention to violate. Previous studies in the area of criminology have found that viewing the crime as morally wrong is associated with a low intention to commit the crime. However, these studies have been local in single countries (Bachman et al. 1992; Elis and Simpson 1995; Paternoster and Simpson 1996). Hovav and D'Arcy (2012) tested the effects of moral beliefs on intention to misuse IS and found no difference in its effects in South Korea or the US. Our results expand on this finding by showing that "moral beliefs" is the strongest effect in our multinational sample. One possible theoretical explanation for the moral belief results comes from Hare's (1961) doctrine of overriding, which states that moral concerns have a special value in that they override nonmoral concerns, including the assessment of egoistic benefits and sanctions.

Third, our results indicate that across cultures, neutralization techniques are strong predictors of employee intention to violate an ISP. Although Siponen and Vance (2010) found similar findings in Finland, mirroring single-country studies in criminology (Maruna and Copes 2005), to our knowledge, no previous study has examined neutralization via multiple countries. Examining this is important because neutralization is theorized to be potentially influenced by culture (Maruna and Copes 2005) because a neutralization technique is "adopted because of its public acceptability. Socialization teaches us which motives are acceptable for which actions" (Cohen 2001, p. 59). The current study takes a step in examining this issue. Our results show that the effect of neutralization on ISP violations holds across our multinational sample. In doing

so, we also respond to the call of Willison and Warkentin (2013) for more research on how neutralization influences ISP violations.

Fourth, our results show that across cultures, shame negatively affects employee intention to violate an ISP. Previously, only one study in the field of IS has examined the effect of shame on ISP violations (Siponen and Vance 2010). However, to the best of our knowledge, no study whether in IS or criminology, has examined the effect of shame across different cultures; instead, these studies have examined shame in the context of a single country (Braithwaite 1989; Elis and Simpson 1995; Grasmick and Bursik 1990; Nagin and Paternoster 1993; Paternoster and Simpson 1996).

Fifth, we found that of the three moderating cultural dimensions examined, only individualism/collectivism was statistically significant. That is, for subjects who reported a high degree of espoused collectivism, informal sanctions had a significant negative effect on ISP violation intentions. In contrast, the influence of informal sanctions was statistically insignificant for those low in espoused collectivism. This is the first study in the IS field to examine the moderating effects of culture on ISP violation intentions.

Our finding that none of the other hypothesized moderating effects were statistically significant, despite having sufficient statistical power, is not entirely surprising given that prior studies have found that deterrence constructs become insignificant when more powerful predictors, such as neutralization, are added to the model (Siponen and Vance 2010). In a meta-analysis of the ISP compliance literature, Cram et al. (2019) found that deterrence constructs had some of the weakest effects of the theoretical constructs. In contrast, moral beliefs had one of the strongest effects on ISP compliance. Against this backdrop, the nonsignificant moderating results contribute to the literature because they show that deterrence theory poorly explains employees' intention to violate an ISP in the face of a range of culture values for the three relevant cultural dimensions in our multinational sample.

6.1 Implications for Management and Future Research

Although we will avoid making any conclusive implications for practice based on a single study, our research hints at the fact that formal and informal sanctions could be ineffective across cultures, especially outside of collectivistic countries, such as China. Importantly, the implications of the current study highlight the potential value of moral persuasion, appeal to shame, and develop a counter argument against neutralization techniques when it comes to improving employees' ISP violation behavior. Having said this, the use of moral persuasion or

appeal to shame has to be carefully considered in practice because of the ethical issues that may arise.

Our findings also have potential implications for future research. First, we highlight the need for future research to test different theories across cultures in the area of IS. Given that ISP violations are an international phenomenon, it is desirable to test to what extent our theories and models are effective across countries and cultures.

Second, again, although we avoid making any conclusive implications for practice based on one study, our results raise the question of the role of deterrence theory in explaining or preventing ISP violation. Future research could examine the role of deterrence theory in different ISP violations to understand the extent to which they are important in different ISP violations. Furthermore, for shame, future research can examine shame-related concepts, such as embarrassment (Tibbetts 1997). Regarding neutralization, further research can examine what kind of neutralization techniques users invoke in the area of IS security.

Third, an important issue of IS research is to design interventions based on various theories and examine their effect (Siponen and Baskerville 2018) in different cultures. Action research or experimentation can be used to examine this issue.

Fourth, although moral belief seems to have a large influence on ISP violation intentions, we still have no understanding of what specific moral qualifiers influence behavior. In other words, the research on moral belief should be extended to examine what moral theories affect users' IS decisions. That is, asking moral beliefs ("It is morally right to do what [the scenario character] did"), albeit useful as a starting point, should be followed by research that examines what kind of moral thinking employees use in various ISP violations. Thus, future research should examine which ethical theories (e.g., utilitarianism, universality thesis) explain user IS security behavior and which ethical theories are effective as moral persuasions that change users' behavior; in addition, how ethical theories affect users' behavior should be analyzed across cultures. Finally, future research can also look at how violation types (e.g., malicious vs. nonmalicious) might explain inconsistent results (Willison and Warkentin 2013).

6.2 Limitations

First, although this study with respondents from 48 countries demonstrated strong geographic generalizability compared with previous studies, its organizational generalizability was low because respondents were all employees of a single multinational company. On the

one hand, the use of a sampling frame from a single organization could ensure that organizational effects such as organizational culture are kept relatively stable across countries, potentially reducing noise in the data. Indeed, Hofstede (2001) formulated his theory based on data from a single organization. However, further research is needed to study the interplay between national and organizational cultures.

An additional possible limitation is the measurement of intentions rather than actual employee behavior. However, there is a strong correlation between intention and behavior, and we see no theoretical rationalization that ISP violation behavior would be different than anonymously reported intention. Also, we followed previous research on ISP violations that used the scenario-based approach, which measures intention rather than actual behavior. Although this may provide some comparability with our results to the research on intention (Siponen and Vance 2014), our scenarios were designed together with the company representative and therefore were specific to the organization, which may also limit the generalizability of the study to some degree.

7 CONCLUSION

Because IS compliance is a global phenomenon, IS scholars need to evaluate their models across cultures. However, previous research has largely examined ISP violation behavior within a single country, leaving the effects of culture unaccounted for. Furthermore, the inconsistent findings of deterrence theory, which has been the leading theory for explaining ISP violation behavior, have been attributed to cultural differences.

This study investigated this research gaps by testing a model using deterrence theory, along with the predictors of moral belief, neutralization, and shame; this was done using a multinational sample of 615 respondents in 48 countries. In addition, we tested for the moderating effects of three cultural dimensions: power distance, uncertainty avoidance, and individualism/collectivism. Our results indicate that informal sanctions have significant effects for those who espouse a collectivist cultural value. In contrast, the effects of moral belief, neutralization techniques, and shame were significant across our multinational sample, suggesting culture does not affect these predictors. The findings also show that the influence of formal sanctions was insignificant across all cultures in our data. Our study contributes to the literature by taking another step toward examining the problem of ISP violations across cultures, providing a number of avenues for future research.

8 REFERENCES

Aguinis H, Beaty JC, Boik RJ, and Pierce CA (2005) Effect Size and Power in Assessing Moderating Effects of Categorical Variables Using Multiple Regression: A 30-Year Review. *Journal of Applied Psychology* (90:1):94-107.

Akers RL, and Sellers C (2004) Criminological Theory, Los Angeles, CA: Roxbury Publishing Company.

Armstrong JS, and Overton TS (1977) Estimating Nonresponse Bias in Mail Surveys. *Journal of marketing research*):396-402.

Aurigemma S, and Mattson T (2018) Exploring the Effect of Uncertainty Avoidance on Taking Voluntary Protective Security Actions. *Computers & Security* (73):219-234.

Bachman R, Paternoster R, and Ward S (1992) The Rationality of Sexual Offending: Testing a Deterrence/Rational Choice Conception of Sexual Assault. *Law and Society Review*):343-372.

Bagozzi RP, and Yi Y (1991) Multitrait-Multimethod Matrices in Consumer Research. *Journal of Consumer Research* (17:4):426-439.

Barlow JB, Warkentin M, Ormond D, and Dennis A (2018) Don't Even Think About It! The Effects of Antineutralization, Informational, and Normative Communication on Information Security Compliance. *Journal of the Association for Information Systems* (19:8):689-715.

Barlow JB, Warkentin M, Ormond D, and Dennis AR (2013) Don't Make Excuses! Discouraging Neutralization to Reduce It Policy Violation. *Computers & Security* (39, Part B):145-159.

Becker GS (1974) Crime and Punishment: An Economic Approach, in *Essays in the Economics of Crime and Punishment*, NBER, 1-54.

Bollen K, and Lennox R (1991) Conventional Wisdom on Measurement: A Structural Equation Perspective. *Psychological Bulletin*).

Bond MH, and Smith PB (1996) Cross-Cultural Social and Organizational Psychology. *Annual Review of Psychology* (47:1):205-235.

Bontempo RN, Bottom WP, and Weber EU (1997) Cross-Cultural Differences in Risk Perception: A Model-Based Approach. *Risk analysis* (17:4):479-488.

Boudreau M-C, Gefen D, and Straub DW (2001) Validation in Information Systems Research: A State-of-the-Art Assessment. *Mis Quarterly*):1-16.

Braithwaite J (1989). *Crime, Shame and Reintegration*, Cambridge University Press: Cambridge, UK.

Carl D, Gupta V, Javidan MJC, leadership,, and of oTGs (2004) Power Distance. (62):513-563.

Carte TA, and Russell CJ (2003) In Pursuit of Moderation: Nine Common Errors and Their Solutions. *Mis Quarterly*):479-501.

Chen Y, and Zahedi FM (2016) Individuals' Internet Security Perceptions and Behaviors: Polycontextual Contrasts between the United States and China. *MIS Quarterly* (40:1):205-222.

Chin WW, Marcolin BL, and Newsted PR (2003) A Partial Least Squares Latent Variable Modeling Approach for Measuring Interaction Effects: Results from a Monte Carlo Simulation Study and an Electronic-Mail Emotion/Adoption Study. *Information systems research* (14:2):189-217.

Cohen J (1988). *Statistical Power Analysis for the Behavioral Sciences*, (2nd ed.) Lawrence Erlbaum Associates: Hillsdale, NJ.

Cohen S (2001). *States of Denial*, Polity: Cambridge.

Cook TD, and Campbell DT (1979). *Quasi Experimentation: Design and Analytical Issues for Field Settings*, Rand McNally: Chicago.

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

Cram WA, Proudfoot JG, and D'Arcy J (2017) Organizational Information Security Policies: A Review and Research Framework. *European Journal of Information Systems* (26:6):605-641.

Crossler RE, Johnston AC, Lowry PB, and Hu Q (2013) Future Directions for Behavioral Information Security Research. *Computers & Security* (32:1).

D'Arcy J, and Herath T (2011) A Review and Analysis of Deterrence Theory in the Is Security Literature: Making Sense of the Disparate Findings. *European Journal of Information Systems* (20:6):643-658.

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

Diamantopoulos A, and Winklhofer HMJJomr (2001) Index Construction with Formative Indicators: An Alternative to Scale Development. (38:2):269-277.

Dinev T, Goo J, Hu Q, and Nam K (2009) User Behavior toward Preventive Technologies: Cultural Differences between the United States and South Korea. *Information Systems Journal* (19:4):391–412.

Doney PM, Cannon JP, and Mullen MR (1998) Understanding the Influence of National Culture on the Development of Trust. *Academy of management review* (23:3):601-620.

Elis LA, and Simpson SS (1995) Informal Sanction Threats and Corporate Crime: Additive Versus Multiplicative Models. *Journal of Research in Crime and Delinquency* (32:4):399-424.

Fletcher JF (1966). *Situation Ethics: The New Morality*, Westminster John Knox Press.

Fornell C, and Larcker D (1981) Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research* (18:1):39-50.

Gefen D, and Straub D (2005) A Practical Guide to Factorial Validity Using Pls-Graph: Tutorial and Annotated Example. *Communications of the AIS* (16:Article 5):91-109.

Gefen D, Straub DW, and Rigdon EE (2011) An Update and Extension to Sem Guidelines for Admnistrative and Social Science Research. *Management Information Systems Quarterly* (35:2):iii-xiv.

Grasmick H, and Bursik R (1990) Conscience, Significant Others, and Rational Choice: Extending the Deterrence Model. *Law and Society Review* (24:3):837-862.

Guo KH, Yuan Y, Archer NP, and Connelly CE (2011) Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model. *Journal of Management Information Systems* (28:2):203-236.

Hare RM (1961). *The Language of Morals*, Clarendon Press Oxford.

Hare RM (1965). *Freedom and Reason*, Oxford University Press.

Hofstede G (2001). *Culture's Consequences: Comparing Values, Behaviors, Institutions and Organizations across Nations*, Sage: Thousand Oaks, Ca.

House R, Hanges P, Javidan M, Dorfman P, and Gupta V (2004). *Culture, Leadership, and Organizations: The Globe Study of 62 Societies*, Sage: Thousand Oaks, CA.

Hovav A, and D'Arcy J (2012) Applying an Extended Model of Deterrence across Cultures: An Investigation of Information Systems Misuse in the Us and South Korea. *Information & Management* (49:2):99-110.

Hu Q, Xu Z, Dinev T, and Ling H (2011) Does Deterrence Work in Reducing Information Security Policy Abuse by Employees? *Communications of the ACM* (54:6):54-60.

Hui CH, and Triandis HC (1985) Measurement in Cross-Cultural Psychology a Review and Comparison of Strategies. *Journal of cross-cultural psychology* (16:2):131-152.

Jarvis CB, MacKenzie SB, and Podsakoff PM (2003) A Critical Review of Construct Indicators and Measurement Model Misspecification in Marketing and Consumer Research. *Journal of consumer research* (30:2):199-218.
Kam H, Katerattanakul P, and Hong S. (2015) A Tale of Two Cities: Policy Compliance of the Banks in the United States and South Korea. Münster, Germany.
Karjalainen M, Siponen MT, Puhakainen P, and Sarker S. (2013) One Size Does Not Fit All: Different Cultures Require Different Information Systems Security Interventions.
Kim S, Thibodeau R, and Jorgensen RS (2011) Shame, Guilt, and Depressive Symptoms: A Meta-Analytic Review. *Psychological bulletin* (137:1):68.
Kock N (2015) Common Method Bias in Pls-Sem: A Full Collinearity Assessment Approach. *International Journal of e-Collaboration* (11:4):1-10.
Kock N, and Lynn GS (2012) Lateral Collinearity and Misleading Results in Variance-Based Sem: An Illustration and Recommendations. *Journal of the Association for Information Systems* (13:7):546-580.
Kohlberg L (1981). *The Philosophy of Moral Development: Moral Stages and the Idea of Justice*, Harper & Row: San Francisco.
Kohlberg L, Ricks D, and Snarey J (1984) Childhood Development as a Predictor of Adaptation in Adulthood. *Genetic Psychology Monographs*).
Kowalski S (1990) Computer Ethics and Computer Abuse: A Longitudinal Study of Swedish University Students.
Lansky MR (1995) Shame and the Scope of Psychoanalytic Understanding. *The American Behavioral Scientist* (38:8):1076.
Leiwo J, and Heikkuri S (1998) An Analysis of Ethics as Foundation of Information Security in Distributed Systems. IEEE, 213-222.
Lian H, Ferris DL, and Brown DJ (2012) Does Power Distance Exacerbate or Mitigate the Effects of Abusive Supervision? It Depends on the Outcome. *Journal of Applied Psychology* (97:1):107.
Markus HR, and Kitayama S (1991) Culture and the Self: Implications for Cognition, Emotion, and Motivation. *Psychological review* (98:2):224.
Maruna S, and Copes H (2005) What Have We Learned from Five Decades of Neutralization Research? *Crime and justice*):221-320.
Mathieson K, Peacock E, and Chin W (2001) Extending the Technology Acceptance Model: The Influence of Perceived User Resources. *The DATABASE for Advances in Information Systems* (32:3):86-112.
Menard P, Warkentin M, Lowry PBJC, and Security (2018) The Impact of Collectivism and Psychological Ownership on Protection Motivation: A Cross-Cultural Examination. (75):147-166.
Myyry L, Siponen M, Pahnila S, Vartiainen T, and Vance A (2009) What Levels of Moral Reasoning and Values Explain Adherence to Information Security Rules&Quest; an Empirical Study. *European Journal of Information Systems* (18:2):126-139.
Nagin DS, and Paternoster R (1993) Enduring Individual Differences and Rational Choice Theories of Crime. *Law and Society Review*):467-496.
Nagin DS, and Pogarsky G (2001) Integrating Celerity, Impulsivity, and Extralegal Sanction Threats into a Model of General Deterrence: Theory and Evidence. *Criminology* (39):865.
Nunnally JC (1967). *Psychometric Theory*, McGraw-Hill: New York, NY.
Paternoster R, and Simpson S (1996) Sanction Threats and Appeals to Morality: Testing a Rational Choice Model of Corporate Crime. *Law and Society Review*):549-583.
Pavlou P, Liang H, and Xue Y (2007) Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective. *MIS Quarterly* (31:1):105-136.

Petter S, Straub D, and Rai A (2007) Specifying Formative Constructs in Information Systems Research. *Mis Quarterly*):623-656.
Piquero A, and Hickman M (1999) An Empirical Test of Tittle's Control Balance Theory. *Criminology* (37:2):319-342.
Piquero A, and Tibbetts S (1996) Specifying the Direct and Indirect Effects of Low Self-Control and Situational Factors in Offenders' Decision Making: Toward a More Complete Model of Rational Offending. *Justice quarterly* (13:3):481-510.
Piquero AR, MacDonald J, Dobrin A, Daigle LE, and Cullen FT (2005) Self-Control, Violent Offending, and Homicide Victimization: Assessing the General Theory of Crime. *Journal of Quantitative Criminology* (21:1):55-71.
Podsakoff PM, MacKenzie SB, Lee J, and Podsakoff NP (2003) Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies. *Journal of Applied Psychology* (88:5):879-903.
Podsakoff PM, MacKenzie SB, and Podsakoff NP (2012) Sources of Method Bias in Social Science Research and Recommendations on How to Control It. *Annual review of psychology* (63):539-569.
Rest JR (1994) Background: Theory and Research. *Moral development in the professions: Psychology and applied ethics*):1-26.
Ringle CM, Sarstedt M, and Straub D (2012) A Critical Look at the Use of Pls-Sem in Mis Quarterly. *MIS Quarterly (MISQ)* (36:1).
Ringle CM, Wende S, and Becker J-M (2015) Smartpls 3: Bönningstedt, Germany.
Robinson WS (1950) Ecological Correlations and the Behavior of Individuals. *American Sociological Review* (15:3):351-357.
Siponen M, and Baskerville R (2018) Intervention Effect Rates as a Path to Research Relevance: Information Systems Security Example. *Journal of the Association for Information Systems* (19:4):247-265.
Siponen M, and Vance A (2010) Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly* (34:3):487-A412.
Siponen M, and 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.
Siponen MT, and Vartiainen T (2002) Teaching End-User Ethics: Issues and a Solution Based on Universalizability. *Communications of the Association for Information Systems* (8:1):422-443.
Srite M, and Karahanna E (2006) The Role of Espoused National Cultural Values in Technology Acceptance. *MIS quarterly* (30:3):679-704.
Straub D, Loch K, Evaristo R, Karahanna E, and Srite M (2002) Toward a Theory-Based Measurement of Culture. *Journal of Global Information Management (JGIM)* (10:1):13-23.
Straub DW, Boudreau M, and Gefen D (2004) Validation Guidelines for Is Positivist Research. *Communications of the Association for Information Systems* (13:24):380-427.
Sully de Luque M, and Javidan M (2004) Uncertainty Avoidance, in *Culture, Leadership, and Organizations: The Globe Study of 62 Societies,* R. J. House, Hanges, P. J., Javidan, M., Dorfman, P. W., & Gupta, V. (ed.), 602-653.
Sykes GM, and Matza D (1957) Techniques of Neutralization: A Theory of Delinquency. *American sociological review* (22:6):664-670.
Tangney JP (1995) Recent Advances in the Empirical Study of Shame and Guilt. *The American Behavioral Scientist* (38:8):1132-1145.
Tepper BJ (2007) Abusive Supervision in Work Organizations: Review, Synthesis, and Research Agenda. *Journal of Management* (33:3):261-289.

Thurman QC (1984) Deviance and the Neutralization of Moral Commitment: An Empirical Analysis. *Deviant Behavior* (5:1-4):291-304.
Tibbetts SG (1997) Shame and Rational Choice in Offending Decisions. *Criminal Justice and Behavior* (24:2):234-255.
Triandis HC (1989) The Self and Social Behavior in Differing Cultural Contexts. *Psychological review* (96:3):506-520.
Vance A, Benjamin Lowry P, and Eggett D (2015) Increasing Accountability through User-Interface Design Artifacts: A New Approach to Addressing the Problem of Access-Policy Violations. *MIS Quarterly* (39:2):345-366.
Warkentin M, and Willison R (2009) Behavioral and Policy Issues in Information Systems Security: The Insider Threat. *European Journal of Information Systems* (18:2):101-105.
Wasti SA (2003) Organizational Commitment, Turnover Intentions and the Influence of Cultural Values. *Journal of Occupational and Organizational Psychology* (76:3):303-321.
Weber EU, and Hsee C (1998) Cross-Cultural Differences in Risk Perception, but Cross-Cultural Similarities in Attitudes Towards Perceived Risk. *Management science* (44:9):1205-1217.
Weber EU, and Milliman RA (1997) Perceived Risk Attitudes: Relating Risk Perception to Risky Choice. *Management Science* (43:2):123-144.
Willison R, and Warkentin M (2013) Beyond Deterrence: An Expanded View of Employee Computer Abuse. *MIS Quarterly* (37:1):1-20.

The Effects of Sanctions, Moral Beliefs, and Neutralization on Information Security Policy Violations Across Cultures

Anthony Vance is the Danny & Elsa Lui Distinguished Associate Professor in the Information Technology Management Department at the Shidler College of Business of the University of Hawaii at Manoa, as well as Associate Professor of Information Systems at the Marriott School of Business of Brigham Young University. He earned Ph.D. degrees in Information Systems from Georgia State University, USA; the University of Paris— Dauphine, France; and the University of Oulu, Finland. His previous experience includes working as a security consultant at Deloitte and as a research professor in the Information Systems Security Research Center at the University of Oulu.

His research focuses on behavioral and neuroscience applications to information security. His work is published in outlets such as *MIS Quarterly*, *Information Systems Research*, *Journal of Management Information Systems*, *Journal of the Association for Information Systems*, *European Journal of Information Systems*, *Journal of the American Society for Information Science and Technology*, and *Proceedings of the ACM Conference on Human Factors in Computing Systems* (CHI). He currently is an associate editor at *MIS Quarterly* and serves on the editorial board of *Journal of the Association for Information Systems*.

Mikko Siponen (mikko.t.siponen@jyu.fi) is a professor in the Department of Computer Science and Information Systems at the University of Jyväskylä. He holds a Ph.D. in philosophy from the University of Joensuu, Finland, and a Ph.D. in information systems (IS) from the University of Oulu, Finland. His research interests include IS security, IS development, computer ethics, and philosophical aspects of IS. Mikko has published 45 articles in journals such as MIS Quarterly, Journal of the Association for Information Systems, Information & Management, European Journal of Information Systems, Information & Organization, Communications of the ACM, IEEE Computer, IEEE IT Professional, and others. He has received over €5 million of research funding from corporations and numerous funding bodies.

Detmar W. Straub is Institute for Business and Information Technology Distinguished Professor in Management Information Systems at the Fox School of Business. Previously, he

was Georgia Regents' Professor and the J. Mack Robinson Distinguished Professor of Information Systems at Georgia State University. Detmar has conducted research in the areas of global IT sourcing, computer security, e-Commerce, technological innovation, international IT studies, and IS research methods. He holds a DBA (Doctor of Business Administration) in MIS from Indiana and a PhD in English from Penn State.

Detmar has more than 195 publications appearing in journals such as MIS Quarterly, Management Science, Information Systems Research, Journal of MIS, Journal of AIS, Decision Sciences Journal, Organization Science, European Journal of Information Systems, Communications of the ACM, Information & Management, Communications of the AIS, IEEE Transactions on Engineering Management, DATA BASE, OMEGA, Academy of Management Executive, and Sloan Management Review.

Online Appendices

Appendix A. Scenarios and Instrumentation

A key step in designing scenarios is to ensure that they are realistic and commonplace (Piquero and Hickman 1999). To ensure that the designed scenarios were realistic in content, we consulted with security managers of the target organization to select violations of actual information security policies (ISPs) published by the organization. Moreover, of these scenarios, we further selected scenarios that were either thought to represent common violations or were highly concerning to management. After the scenarios were chosen, the content of each scenario was reviewed by four IT security experts. After multiple iterative rounds of review and revision, a consensus was reached that the scenarios were realistic in form and detail. The final scenarios are listed in Table A1.

Table A1. Hypothetical scenarios

Violation	**Scenario**
Reading confidential documents	Don goes to the shared office printer after work hours, and notices printed pages on the printer marked "Confidential" which were apparently printed by another employee. No one else is in the room. [The ISP prohibits reading confidential information, but] Don is curious to see who the documents belong to and quickly reads through the documents.
Failing to report a computer virus	Gina is browsing possible questionable websites at work, and the anti-virus program alerts that a virus has been installed on her computer. [Although the ISP requires that viruses be removed by IT support staff,] Gina decides to take care of the virus problem by herself.
Allowing children to play with laptop	John takes his work laptop computer home to work. While he takes a break, his children ask to use the laptop. [His company's ISP prohibits sharing work computers with others. However,] John lends his children his laptop.
Using unencrypted portable media	Peter is working on a report that requires the analysis of sensitive data. [Because of the sensitive nature of corporate data, the company has an ISP prohibiting the copy of corporate data to unencrypted portable media, such as USB drives. However,] Peter will travel for several days and would like to analyze the corporate database on the road. Peter copies the corporate database to his portable USB drive and takes it off company premises.
Using portable media from an unknown source	Travis finds a USB drive lying on a table in the lobby. [His company's IS security policy prohibits using portable media from unknown sources, but] he is curious to see who it belongs to. He takes it back to his computer and inserts the drive into his USB port. A dialog box appears and then disappears before Travis can read what it said. The USB drive contains several files, but no files that could identify its owner.
Sharing passwords	Heather uses a file server at work that she can access by typing in her password. [The company has an ISP that passwords must not be shared.] However, Heather is on a business trip and one of her co-workers needs a file on the file server. Heather shares her password with her co-worker.

Note: Text enclosed by brackets explicitly states that the behavior in question is an ISP violation. This text was randomly inserted into scenarios to control for the effect of recognizing an ISP violation.

Table A2. Measurement Items				
Construct	Item Code	Text	Scale	Source
Intention	Intention1 Mean: 2.247 STD: 2.818	What is the chance that you would do what [the scenario character] did in the described scenario?	No chance 0 to 10 100% chance	Nagin and Paternoster (1993)
	Intention2 Mean: 2.27 STD: 2.936	I would act in the same way as [the scenario character] did if I was in the same situation.	No chance 0 to 10 100% chance	Nagin and Paternoster (1993)†
Formal Sanctions —certainty	FormCertA Mean: 4.393 STD: 3.081	How likely is it that you would be formally sanctioned (punished) if management learned that you did what [the scenario character] did?	No chance 0 to 10 100% chance	Siponen and Vance (2009)
	FormCertB* Mean: 7.119 STD: 2.569	I would receive sanctions at work if I did what [the scenario character] did.	No chance 0 to 10 100% chance	Siponen and Vance (2009)
	FormCertC Mean: 5.02 STD: 2.94	How likely is it that you would be sanctioned if management learned you had done what [the scenario character] did?	No chance 0 to 10 100% chance	Siponen and Vance (2009)
Formal Sanctions —severity	FormSevA Mean: 6.251 STD: 2.741	How much of a problem would it create in your life if you were formally reprimanded for doing what [the scenario character] did?	No problem at all 0 to 10 A very big problem	Siponen and Vance (2009)
	FormSevB* Mean: 7.119 STD: 2.569	How much of a problem would it be if you received sanctions at work for doing what [the scenario character] did?	No problem at all 0 to 10 A very big problem	Siponen and Vance (2009)
	FormSevC Mean: 6.886 STD: 2.709	How much of a problem would it create in your life if you were formally sanctioned for doing what [the scenario character] did?	No problem at all 0 to 10 A very big problem	Siponen and Vance (2009)
Informal sanctions —certainty	InformCertA Mean: 5.075 STD: 3.053	How likely is it that you would lose the respect and good opinion of your colleagues for doing what [the scenario character] did?	No chance 0 to 10 100% chance	Siponen and Vance (2009)
	InformCertB* Mean: 5.166 STD: 2.972	How likely is it that your career would be adversely affected if management learned that you had done what [the scenario character] did?	No chance 0 to 10 100% chance	Siponen and Vance (2009)
	InformCertC Mean: 5.512 STD: 2.976	How likely is it that you would lose the respect and good opinion of your manager for doing what [the scenario character] did?	No chance 0 to 10 100% chance	Siponen and Vance (2009)
Informal sanctions —severity	InformSevA Mean: 6.603 STD: 2.887	How much of a problem would it create in your life if your career was adversely affected for doing what [the scenario character] did?	No problem at all 0 to 10 A very big problem	Siponen and Vance (2009)

	InformSevB* Mean: 7.021 STD: 2.83	How much of a problem would it create in your life if you lost the respect and good opinion of your colleagues for doing what [the scenario character] did?	No problem at all 0 to 10 A very big problem	Siponen and Vance (2009)
	InformSevC Mean: 6.608 STD: 2.818	How much of a problem would it create in your life if you lost the respect of your managers for doing what [the scenario character] did?	No problem at all 0 to 10 A very big problem	Siponen and Vance (2009)
Shame —certainty	ShameCertA Mean: 5.358 STD: 3.603	I would be ashamed if colleagues knew that I had done what [the scenario character] did.	No chance 0 to 10 100% chance	Siponen and Vance (2009)
	ShameCertB Mean: 5.185 STD: 3.414	How likely is it that you would be ashamed if others knew that you had done what [the scenario character] did?	No chance 0 to 10 100% chance	Siponen and Vance (2009)
	ShameCertC Mean: 5.985 STD: 3.361	How likely is it that you would be ashamed if managers knew that you had done what [the scenario character] did?	No chance 0 to 10 100% chance	Siponen and Vance (2009)
Shame —Severity	ShameSevA Mean: 5.468 STD: 2.96	How much of a problem would it be if you felt ashamed that your colleagues knew you had done what [the scenario character] did?	No problem at all 0 to 10 A very big problem	Siponen and Vance (2009)
	ShameSevB Mean: 5.737 STD: 2.982	How much of a problem would it be if you felt ashamed that others knew you had done what [the scenario character] did?	No problem at all 0 to 10 A very big problem	Siponen and Vance (2009)
	ShameSevC Mean: 5.696 STD: 2.938	How much of a problem would it be if you felt ashamed that managers knew you had done what [the scenario character] did?	No problem at all 0 to 10 A very big problem	Siponen and Vance (2009)
Moral Inhibitions	MoralA (r) Mean: 2.272 STD: 2.667	How morally wrong would it be to do what [the scenario character] did in the scenario?	Not right at all 0 to 10 100% right	Paternoster and Simpson (1996)
	MoralB (r) Mean: 2.745 STD: 2.915	It is morally right to do what [the scenario character] did.	Not right at all 0 to 10 100% right	Paternoster and Simpson (1996)†
Neutralization techniques (formative construct)	Appeal to higher loyalties Mean: 2.343 STD: 1.594	It is all right to violate a company ISP to get a job done.	Strongly Disagree 1 to 7 Strongly Agree	(Thurman 1984)
	Condemnation of the condemners Mean: 2.871 STD: 1.871	It is not as wrong to a violate company ISP that is unreasonable.	Strongly Disagree 1 to 7 Strongly Agree	(Thurman 1984)

	Defense of necessity Mean: 2.715 STD: 1.881	It is okay to a violate company ISP under circumstances where it seems like you have little other choice.	Strongly Disagree 1 to 7 Strongly Agree	(Thurman 1984)
	Denial of injury Mean: 2.40 STD: 1.725	It is OK to violate a company ISP if no harm is done.	Strongly Disagree 1 to 7 Strongly Agree	(Thurman 1984)
	Denial of responsibility Mean: 2.432 STD: 1.71	It is OK to violate a company ISP if you aren't sure what the policy is.	Strongly Disagree 1 to 7 Strongly Agree	Thurman (1984)
	Metaphor of the ledger Mean: 2.754 STD: 1.722	I feel my general adherence to company ISPs compensates for occasionally violating a policy.	Strongly Disagree 1 to 7 Strongly Agree	Siponen and Vance (2009)
Individualism/Collectivism	IC1* Mean: 4.369 STD: 1.696	Being accepted as a member of a group is more important than having autonomy and independence.	Strongly Disagree 1 to 7 Strongly Agree	Srite and Karahanna (2006)
	IC2 Mean: 4.483 STD: 1.681	Being accepted as a member of a group is more important than being independent.	Strongly Disagree 1 to 7 Strongly Agree	Srite and Karahanna (2006)
	IC3* Mean: 5.767 STD: 1.378	Group success is more important than individual success.	Strongly Disagree 1 to 7 Strongly Agree	Srite and Karahanna (2006)
	IC4 Mean: 5.153 STD: 1.549	Being loyal to a group is more important than individual gain.	Strongly Disagree 1 to 7 Strongly Agree	Srite and Karahanna (2006)
	IC5* Mean: 3.767 STD: 1.732	Individual rewards are not as important as group welfare.	Strongly Disagree 1 to 7 Strongly Agree	Srite and Karahanna (2006)
Power Distance	PD1* Mean: 2.367 STD: 1.364	Managers should make most of the decisions without consulting subordinates.	Strongly Disagree 1 to 7 Strongly Agree	Srite and Karahanna (2006)
	PD2* Mean: 1.686 STD: 1.303	Managers should not ask subordinates for advice because they might appear less powerful.	Strongly Disagree 1 to 7 Strongly Agree	Srite and Karahanna (2006)
	PD3 Mean: 3.512 STD: 1.777	Decision-making power should stay with top management in the organization and not be delegated to lower level employees.	Strongly Disagree 1 to 7 Strongly Agree	Srite and Karahanna (2006)

	PD4 Mean: 2.59 STD: 1.533	Employees should not question their manager's decisions.	Strongly Disagree 1 to 7 Strongly Agree	Srite and Karahanna (2006)
	PD5* Mean: 2.876 STD: 1.88	A manager should perform work which is difficult and important and delegate tasks which are repetitive and mundane to subordinates.	Strongly Disagree 1 to 7 Strongly Agree	Srite and Karahanna (2006)
	PD6* Mean: 3.272 STD: 1.883	Higher level managers should receive more benefits and privileges than lower level managers and professional staff.	Strongly Disagree 1 to 7 Strongly Agree	Srite and Karahanna (2006)
	PD7* Mean: 2.467 STD: 1.639	Managers should be careful not to ask the opinions of subordinates too frequently, otherwise the manager might appear to be weak and incompetent.	Strongly Disagree 1 to 7 Strongly Agree	Srite and Karahanna (2006)
Uncertainty Avoidance	UA1 Mean: 5.85 STD: 1.229	Rules and regulations are important because they inform workers what the organization expects of them.	Strongly Disagree 1 to 7 Strongly Agree	Srite and Karahanna (2006)
	UA2 Mean: 5.857 STD: 1.342	Order and structure are very important in a work environment.	Strongly Disagree 1 to 7 Strongly Agree	Srite and Karahanna (2006)
	UA3* Mean: 5.541 STD: 1.565	It is important to have job requirements and instructions spelled out in detail so that people always know what they are expected to do.	Strongly Disagree 1 to 7 Strongly Agree	Srite and Karahanna (2006)
* Dropped to improve reliability or construct validity; (r) reversed; † Derived from the original item to allow reliability testing.				

Appendix B. List of Respondents by Country

Table B1. Frequency of Respondents by Country

Country	Frequency	Percent
Finland	239	38.8
India	62	10.1
Italy	49	8
Netherlands	38	6.2
Spain	23	3.7
US	20	3.2
Norway	16	2.6
United Kingdom	16	2.6
France	15	2.4
Korea, Republic of	12	1.9
Philippines	12	1.9
Switzerland	10	1.6
China	8	1.3
Denmark	8	1.3
Russian Federation	8	1.3
Sweden	8	1.3
Germany	7	1.1
Guatemala	6	1
Singapore	6	1
Mexico	5	0.8
Portugal	5	0.8
Azerbaijan	4	0.6
Canada	4	0.6
Japan	3	0.5
Turkey	3	0.5
Indonesia	2	0.3
Poland	2	0.3
Taiwan	2	0.3
Not reported	2	0.3
Australia	1	0.2
Cameroon	1	0.2
Colombia	1	0.2
Croatia	1	0.2
Dominican Republic	1	0.2

Table B1. Frequency of Respondents by Country		
Country	**Frequency**	**Percent**
Ecuador	1	0.2
Estonia	1	0.2
Greece	1	0.2
Guyana	1	0.2
Hong Kong	1	0.2
Hungary	1	0.2
Kenya	1	0.2
Korea, Democratic People's Republic Of	1	0.2
Malaysia	1	0.2
Morocco	1	0.2
Pakistan	1	0.2
Panama	1	0.2
Slovakia	1	0.2
Ukraine	1	0.2
Vietnam	1	0.2
Total	615	100

Because the largest home country reported by respondents was Finland at 38.8%, we performed two tests to determine whether there were significant differences in our model for Finns compared with non-Finns. First, we added a control variable to our model that contained the value “1” if the respondent claimed Finland as his or her home country and “0” otherwise. We then modeled this binary variable to predict “intention to violate the security policy” as with our other control variables. Our results show that this variable had an insignificant effect on “intention” (β = .028, t = .783, p = .217).

Second, we performed a multigroup analysis using SmartPLS 3.2.7 with the two groups being those who stated Finland as their home country and those who did not. This process compared the difference between the two groups for every path in the model. We found no differences between the groups except for the effects for formal sanctions and gender. For example, whereas the effect of formal sanctions on intention to violate the ISP had a path coefficient of -.161 for Finns, it was .11 for non-Finns, a difference of .277 (t = 2.005, p = .045). Similarly, the coefficient for the effect of gender on intention

for Finns was -.049 compared with .089 for non-Finns, a difference of .137 (t = 2.157, p = .031).

However, when examining the model separately for each group, neither formal sanctions nor gender significantly affected intention. We conclude that although there was a slight difference for Finns and non-Finns for formal sanctions and gender, these differences were not significant enough to influence intention. Additionally, all other paths in the model showed no differences for Finns and non-Finns, providing an additional robustness check of our model.

Appendix C. Model Validation

To validate the discriminant and convergent validity of the reflective constructs in our model, we followed the partial least squares (PLS) validation guidelines described by Gefen and Straub (2005). Because one of the constructs in our model—neutralization—was formative, this construct was validated using techniques designed for formative constructs (Petter et al. 2007). The validation of the reflective constructs is discussed first.

Validation for Reflective Constructs

To test the convergent validity, we performed a bootstrap using SmartPLS using 600 resamples and then examined the t-values of the loadings of each item onto their intended constructs. The convergent validity is demonstrated when t-values of the item loadings are significant at the.05 α level. In this case, all items loaded significantly ($p < .001$), indicating a strong convergent validity. An additional test of convergent validity put forward by Fornell and Larcker (1981) is that the average variance extracted (AVE)—a measure of variance explained by a latent construct for the variance observed in its measurement items—should be at least.50 or higher. The AVE values are shown in Table B4. This test result also indicates a high degree of convergent validity.

Table C1. Item Loadings for Convergent Validity		
Construct	Item	Loading
Formal Sanctions	FormA	.92***
	FormC	.95***
Individualism/Collectivism	IC2	.82**
	IC4	.90***
Informal Sanctions	InformA	.92***
	InformC	.95***
Intention to Violate	Intention1	.96***
	Intention2	.97***
Moral Beliefs	MoralA	.90***
	MoralB	.93***
Power Distance	PD3	.87***
	PD4	.76***
Shame	ShameA	.92***
	ShameB	.95***
	ShameC	.93***
Uncertainty Avoidance	UA1	.92***
	UA2	.71***
N.B. *** p <.001		

Discriminant validity is commonly demonstrated using two tests performed in PLS (Gefen and Straub 2005). First, the cross loadings of the items on the latent variables of the model are examined to ensure that items load most highly on their intended latent variable by at least .10 more than other latent variables. In our test, all items met these criteria, as shown in Table B2, evidencing excellent discriminant validity.

A second test of discriminant validity compares correlations of constructs within the model to the square root of each construct's AVE score. In this comparison, a construct's square root of the AVE should be much larger than correlations with any other construct in the model and should be at least .50 (Fornell and Larcker 1981). In our test, each construct met both criteria, again denoting strong discriminant validity.

Table C2. Item Cross loadings									
Construct	Item	1	2	3	4	5	6	7	8
Formal Sanctions (1)	FormA	**.95**	.21	.76	-.21	-.33	.14	.68	.30
	FormC	**.95**	.21	.85	-.20	-.36	.15	.67	.34
Individualism/Collectivism (2)	IC2	.22	**.82**	.20	-.02	-.08	.13	.22	.28
	IC4	.17	**.90**	.20	-.03	-.16	.22	.20	.29
Informal Sanctions (3)	InformA	.77	.20	**.95**	-.22	-.38	.16	.71	.33
	InformC	.84	.24	**.95**	-.23	-.38	.15	.74	.35
Intention to Violate (4)	Intention1	-.21	-.05	-.23	**.96**	.54	-.07	-.32	-.14
	Intention2	-.21	-.01	-.22	**.97**	.55	-.06	-.31	-.11
Moral Beliefs (5)	MoralA	-.34	-.13	-.38	.48	**.90**	-.13	-.44	-.20
	MoralB	-.32	-.13	-.35	.55	**.93**	-.10	-.45	-.21
Power Distance (6)	PD3	.11	.20	.11	-.06	-.09	**.87**	.11	.15
	PD4	.15	.14	.17	-.05	-.12	**.76**	.12	.03
Shame (7)	ShameA	.63	.21	.67	-.30	-.47	.13	**.92**	.31
	ShameB	.70	.25	.73	-.31	-.47	.16	**.95**	.32
	ShameC	.68	.21	.72	-.31	-.43	.09	**.93**	.29
Uncertainty Avoidance (8)	UA1	.27	.29	.28	-.13	-.20	.09	.28	**.92**
	UA2	.31	.26	.33	-.07	-.16	.12	.27	**.71**

Table C3. Correlations, Average Variance Extracted, and Composite Reliability										
Construct	CR	AVE	1	2	3	4	5	6	7	8
Formal Sanctions (1)	.95	.90	**.95**							
Individualism/Collectivism (2)	.85	.74	.22	**.86**						
Informal Sanctions (3)	.95	.90	.85	.23	**.95**					
Intention to Violate (4)	.96	.93	-.22	-.03	-.23	**.97**				
Moral Beliefs (5)	.91	.84	-.36	-.14	-.40	.57	**.92**			
Power Distance (6)	.80	.67	.15	.21	.17	-.07	-.12	**.82**		
Shame (7)	.95	.87	.72	.24	.76	-.33	-.49	.14	**.93**	
Uncertainty Avoidance (8)	.80	.67	.34	.33	.35	-.13	-.22	.12	.33	**.82**
Note: CR = Composite reliability; AVE = Average variance extracted										

Finally, to test the reliability of the items in the analysis, SmartPLS was used to calculate the composite reliability score (Fornell and Larcker 1981), which was evaluated in the same way as Cronbach α. This score is a more accurate measurement of reliability than Cronbach α because it does not assume that the loadings or error terms of the items are equal (Chin et al. 2003). These scores are also reported in Table B3. All constructs exhibited a reliability score well over the .60 threshold needed for exploratory research (Nunnally 1967).

Validation for Formative Construct

Because formative constructs require different tests for their validation (Petter et al. 2007), we validated our models' formative construct—neutralization—separately from the reflective constructs. This was done in two ways. First, to evaluate construct validity, the weights of the items contributing to neutralization were examined for significance. Of the six neutralization items, three were not significant. Although Diamantopoulus and Winklhofer (2001) advocated for removing insignificant items in formative constructs, Bollen and Lenox (1991) cautioned that removing insignificant items from a formative construct may reduce the content validity of that construct. Because content validity is essential for formative constructs, Petter et al. (2007) advised retaining insignificant items when doing otherwise would reduce the construct's content validity. In the present case, the six neutralization techniques have long been recognized (Sykes and Matza 1957) and have received empirical support as formative constructs (Siponen and Vance 2010). For these reasons, we elected to retain the items to preserve the content validity of neutralization.

Next, we assessed the reliability of the neutralization construct by regressing intention on the six neutralization items and examining the variance inflation factor (VIF) statistic for each item. Because multicollinearity is a larger problem for formative constructs than reflective ones, Petter et al. (2007) recommended that all items have a VIF score of less than 3.3. In our test, no item had a VIF score above 2, indicating excellent reliability. Based on the results of these tests, we conclude that neutralization has sufficient construct validity and reliability.

Appendix D. Tests for Common Method Bias

Common method bias (CMB) is "variance that is attributable to the measurement method rather than to the constructs the measures represent" (Podsakoff et al. 2003, p. 879) and is a major contributor to systematic measurement error (Bagozzi and Yi 1991). Like all forms of measurement error, if CMB is sufficiently high, then incorrect conclusions may be drawn about the relationships between the constructs. Because we measured the dependent and independent variables in the same instrument, we tested for the influence of CMB.

First, to reduce the likelihood of CMB, the items were randomized within the instrument. This limits the ability of the participants to detect underlying construct patterns that could influence their answers (Cook and Campbell 1979; Straub et al. 2004). Second, we performed Harman's one-factor test (Podsakoff et al. 2012). In this test, all items are entered into an unrotated exploratory factor analysis to determine whether a single factor emerges or a single factor accounts for most of the variance. In our test, 48 factors emerged, the largest of which accounted for 27% of the variance. Both statistics indicated that CMB was not an issue.

However, because Harman's one-factor test is increasingly contested for its ability to detect CMB (Podsakoff et al. 2012), we also performed a test performed by Pavlou et al. (2007). In their test, the construct correlation matrix as calculated by PLS (reported in Table B3) is examined to determine whether any constructs correlate extremely highly (more than .90) with others in the model. In our case, none of the constructs were highly correlated. This finding likewise indicates that CMB was not a problem in the current study.

Finally, as a more rigorous test for CMB, we applied the full collinearity test established by Kock and Lynn (2012), which Kock (2015) demonstrated is also effective as a test for CMB. In this method, a new column in the data is created with random values, such as a random number between 0 and 1. Next, a model is created in which all latent variables and moderating variables point to a new dummy construct with the random variable as its only indicator. Finally,

the PLS algorithm is run, and the VIF scores are saved for each of the latent variables. Here, VIF scores greater than 3.3 are

> "an indication of pathological collinearity, and also as an indication that a model may be contaminated by common method bias. Therefore, if all VIFs resulting from a full collinearity test are equal to or lower than 3.3, the model can be considered free of common method bias" (Kock 2015, p. 7).

In the case of our model, we found that the VIF scores for all the latent and moderation variables ranged between 1.07 and 2.63. This result, along with those cited above, failed to indicate the presence of CMB.