Legitimacy and Personal Values: The Mediating Role of Legitimacy Perceptions in Information Security Policy Compliance

Completed paper

Carlos I. Torres
Baylor University
carlos_torres@baylor.edu

Robert E. Crossler
Washington State University
rob.crossler@wsu.edu

Richard D. Johnson
Washington State University
richard.d.johnson@wsu.edu

ABSTRACT

This paper extends Protection Motivation Theory (PMT) based on Legitimacy and Personal Values theories. We postulate that legitimacy is a more comprehensive antecedent to compliance with security policies than the traditional fear element introduced in fear appeals research. Furthermore, we argue that personal values have an effect on policy legitimacy perceptions as well as compliance with the policy. We tested our model using a sample of 259 respondents from an online survey. Our results confirm that legitimacy as a whole is a strong influencer of compliance with the security policy and moderates the effect of the threat appraisal (threat vulnerability and severity) in the intention to comply with the policy.

Our mediation analysis also shows that not only higher-order personal values (conservation and self-transcendence) are significant influencers in legitimacy perceptions, but also all PMT traditional constructs are significant antecedents to legitimacy perceptions, providing support to legitimacy judgments and evaluations made before a policy or rule is considered legitimate thus leading to compliance.

Our findings shed light on motivators to policy compliance other than fear, such as legitimacy perceptions that should be considered in security policy promotion in organizations' individually tailored security policies and the various interventions that can motivate compliance with security policies.

Keywords

PMT, legitimacy judgments, legitimacy theory, information security, information security policy compliance, personal values

INTRODUCTION

Cybersecurity threats present issues to organizations worldwide. These threats are expected to increase in the foreseeable future.   Cybersecurity has been the CIO's top concern in the SIM IT Issues and Trends study from 2018 to 2021 (Kappelman et al., 2021; Kappelman et al., 2019; Pearlson et al., 2020). In 2020, cybercrime cost estimates were estimated at around 1 Trillion USD, representing over a 60% increase in two years from the 600 billion USD estimate (Malekos-Smith & Lostri, 2020) in 2018 and more than double the 2014 estimate of 400 billion USD (CSIS, 2018).

Despite extant theorization efforts in information security (InfoSec) policy compliance, organizations struggle to enforce secure behaviors. In 2018, 60% of the almost 1,200 C-level IT executives and infosec managers worldwide surveyed by Ernst & Young expressed that employees' careless practices are the leading infosec culprit (EY, 2018). As a result, employees' lack of knowledge or negligent behavior has become the primary risk they believe they face, being at the highest level of concern compared to the last five years by the time of the study (EY, 2018).

IS scholars have theorized about the potential reasons for the lack of compliance with infosec policies in an attempt to explain and prevent cybercrime (e.g., Bulgurcu et al., 2010; Johnston & Warkentin, 2010b; Siponen & Vance, 2010). Prior studies in infosec policy compliance focus on fear (e.g., Boss et al., 2015; Johnston et al., 2015; Moody et al., 2018) as the main driver for compliance with the security policy.

Even though the theories mentioned above confirm the use of fear to promote acceptance of infosec policies as a good strategy, organizations still struggle with enforcing security policies (Kappelman et al., 2021; Pearlson et al., 2020). This makes studying new and different alternatives to eliciting security behaviors a relevant research topic, as suggested by Wall and Buche (2017).

In this project, we argue that users' lack of legitimacy perceptions regarding the implemented policies can be a potential reason for the apparent lack of compliance with information security policies. Legitimacy is a psychological property of a social arrangement such as a group or organization, which leads people to believe that the decisions or rules proposed by an organization are worth being followed voluntarily rather than out of fear or anticipation of punishment or rewards (Tyler, 2006a). Legitimacy is an internal state related to a perception of obligation and responsibility to others (Tyler, 2006a) and, similar to personal values, is an internal motivation for behavior. Values and legitimacy work together. In the context of everyday laws, people follow the laws because they consider they ought to obey legitimate authorities and rules and because they perceive the law as legitimate since the conduct prohibited by the law is wrong according to their values (Tyler, 1990, 1997, 2006a)

Personal values are an intrinsic part of the individual, generally defined as a broad set of desirable goals motivating people's actions through active participation as guiding principles in their lives (Sagiv & Schwartz, 2021). Personal values have constantly received attention from practitioners and are the subject of constant discussions, particularly in the context of work and education, among others. The study of personal values started in the 1990s with the initial theory of personal value types (Schwartz, 1992), deepening understanding of the personal values system construct and its effects on people's perceptions, cognitions, and behaviors (Sagiv & Schwartz, 2021). In addition, personal values have previously been posited as important influencers of compliance with security policies (Torres & Crossler, 2019).

This paper argues that personal values have a significant role in forming legitimacy perceptions, acting together with legitimacy to motivate security behaviors. Considering that systematic investigation regarding the legitimacy of InfoSec policies from the user perspective has been mainly absent in the central and rich infosec policy compliance literature (few exemptions, e.g., Hsu et al., 2015; Kam et al., 2013; Son, 2011). This opens a research opportunity encompassed in our research question:

How do legitimacy perceptions of an InfoSec policy affect compliance with the policy?

The phenomenon under study requires an understanding of potential elements that can increase legitimacy perceptions. Considering that personal values have been found to be significant predictors of perceptions in the workplace (Sagiv & Schwartz, 2021; Sagiv et al., 2011), we try to answer the following research question:

How do personal values influence legitimacy perceptions of an InfoSec policy?

By drawing on organizational theories of legitimacy judgments (Deephouse et al., 2017; Suchman, 1995; Tost, 2011; Tyler, 1997) and the theory of personal value types (Schwartz, 1992), we incorporate a legitimacy construct and modify previous fear-based protection motivation theory (Boss et al., 2015) characterizing research in this field of knowledge. Our study also includes personal values as an antecedent to policy compliance (Torres and Crossler 2019) and as a means to affect different legitimacy perceptions to foster intention to comply with the policy.

The first section of this paper discusses the theoretical background on legitimacy and values and the concepts of fear in the infosec policy compliance literature. The second part describes our proposed research model, research method, data analysis, and a summary of findings. Finally, the third part discusses the results, limitations, implications for practice, and suggestions for future research.

THEORETICAL BACKGROUND

Protection Motivation Theory (PMT) in InfoSec Research

One of the most common theories used in Infosec research is protection motivation theory (PMT) (Maddux & Rogers, 1983; Rogers, 1975, 1983). Multiple research projects have used PMT as the base theoretical framework to explain how employees abide by security policies (e.g., Boss et al., 2015; Crossler et al., 2014; Herath & Rao, 2009; Johnston & Warkentin, 2010b; Johnston et al., 2015; Warkentin et al., 2016).

PMT relies on threat appraisal and coping appraisal, which in turn include four essential elements: vulnerability to the threat, threat severity, the efficacy of the recommended response, and the person's self-efficacy to perform such a response (Herath & Rao, 2009; Maddux & Rogers, 1983; Rogers, 1975, 1983).

PMT posits that people process and appraise security threats. Researchers use perceptions of threat severity and vulnerability/susceptibility as constructs to represent the threat appraisal policies (e.g., Boss et al., 2015; Crossler et al., 2014; Herath & Rao, 2009; Johnston & Warkentin, 2010b; Johnston et al., 2015; Warkentin et al., 2016). Threat severity is the perception of how much damage a threat can cause if it materializes. Threat vulnerability is the likelihood of the person being affected by it (Wall & Buche, 2017).

In addition, PMT research uses fear appeals to elicit secure behaviors. Fear appeals are persuasive messages based on fear intended to generate a behavioral change in response to an imminent threat (Johnston & Warkentin, 2010b; Johnston et al., 2015). PMT posits that a successful fear appeal includes a coping alternative to counter the security threat. Wall and Buche (2017) summarize the coping appraisal as follows:

> A coping mechanisms refer to security actions or technologies that organizations ask insiders to use to limit the danger that threats pose. Coping appraisals refer to individuals' beliefs regarding the coping mechanism and the use of it (Rogers, 1983). Fear appeals may seek to alter insiders' appraisals of coping mechanisms to ensure that insiders' appraisals favor the coping mechanism (Johnston & Warkentin, 2010). Research often represents coping appraisals as response efficacy, response costs, and self-efficacy perceptions (Boss et al., 2015). Response efficacy is an individual's belief that a coping mechanism will reduce a threat. Response costs are perceptions of the personal effort, time, and resources required to respond to the threat by employing the coping mechanism. Self-efficacy refers to the extent to which an individual feels capable of using the coping mechanism to mitigate the threat (Wall & Buche, 2017, p. 279).

Despite strong support and evidence for PMT and fear appeals' role in InfoSec policy compliance, academic controversy over the argument that fear appeals may not be sufficient to induce behavioral change has emerged (Renaud & Dupuis, 2019; Wall & Buche, 2017). This argument supports the idea of introducing more intrinsic elements of evaluation to policy compliance, as suggested in the literature (Lawson et al., 2016; Marett et al., 2019; Wall & Buche, 2017). We are using PMT as a very mature theory with a parsimonious theoretical framework that we can modify to introduce other elements that induce compliance with security policies in organizations.

In general, governments, legal authorities, and organizations strive to produce norms (laws) to be followed by the public, promoting public compliance with the norm (Tyler, 2006b). Furthermore, the key to effective government is that people view compliance with the law as appropriate out of internal motivation to voluntary adoption, assuming the obligation to follow legal rules and personal commitment through personal morality and legitimacy (Tyler, 2006b). Personal morality is to obey because the person believes it is right according to their own values, and legitimacy is to obey out of a feeling that the authority has the right to dictate behavior (Tyler, 2006b). We thus intend to introduce legitimacy and personal values into the PMT framework as the drivers of voluntary compliance with InfoSec policies.

Legitimacy

Legitimacy is a commonly used construct in organizational research. Kelley and Thibaut (1959) claim that in order to have compliance with regulations and policies, the power structure must be legitimate. They explain that only in the presence of legitimacy will a person conform to the norm or rule rather than to their personal interest.

Organizations possess a control system with different mechanisms, such as rewards and sanctions, to achieve their goals. Even though they are necessary, those mechanisms are not enough to guarantee compliance (Tyler, 2006b; Tyler & Blader, 2005). Individuals are better motivated to perform and achieve such goals and comply with norms, regulations, and superior orders based on internal motivators such as legitimacy (Tyler & Blader, 2005). Furthermore, it is accepted that alignment with organizational requirements is only possible if power/authority structures are solidified and legitimate in organizations (Cooren & Robichaud, 2013).

From a behavioral perspective, social psychology defines legitimacy as the belief that a set of social arrangements are appropriate, proper, and just leading to feeling obligated to defer to and comply with the rules set by the group (Tyler, 1990, 2006a). Social psychologists take an individual-based view on legitimacy since people within an organized group have individual and personal feelings about the obligation to obey group rules and the decisions of group authorities (Tyler, 1997). When individuals believe that authorities and rules are legitimate, rules are entitled to be obeyed and followed (Tyler, 1990, 1997, 2006a). Furthermore, because of this perception of legitimacy, obedience and submission to the rules are voluntary (Tyler, 1990, 1997, 2006a). However, Tyler (1997) posits that even though the psychology of legitimacy involves instrumental and relational elements, the legitimacy construct has been mainly conceptualized and operationalized as a unidimensional construct that is effective in facilitating the maintenance of established order and set of rules within the social organization (Tyler, 1997).

Legitimacy has another epistemological and ontological perspective commonly used in management research (Suddaby et al., 2017). Institutional theorists posit that legitimacy is an attribute at the organizational level that provides stable and engrained support for institutions, going beyond the person's self-interest, and shaping their reactions to institutional policies (Tyler, 2006a; Weatherford, 1992). Institutionalists define legitimacy as "a generalized perception or assumption that the actions of an entity are desirable, proper or appropriate within some socially constructed system of norms, values, beliefs, and definitions" (Suchman, 1995, p. 574).

Institutional theorists have conceptualized legitimacy within an underlying assumption that the construct can be categorized based on its defining and constituting properties (Suddaby et al., 2017). Even though a considerable amount of research compares and creates various types of legitimacy, there has been an over proliferation of legitimacy types (Suddaby et al., 2017) that, in the end, become mere conceptual definitions, not entirely separable as empirical phenomena due to overlapping between them (Deephouse et al., 2017).

Some of the aforementioned concepts have been used in IS research, particularly IT governance research. Barrett et al. (2013) introduced legitimacy in the diffusion of managerial practices. Constantinides and Barrett (2014) considered legitimacy as the route organizations take to gain control of a particular IT deployment. Kam et al. (2013) used legitimacy from the government and other authorities as motivators of university implementations of different security policies. Simultaneously with IS scholars analyzing legitimacy and its relationship with IT diffusion, Son (2011) introduced legitimacy to infosec policy compliance, explaining that intrinsic motivators are better predictors of compliance than traditional extrinsic motivators.

Understanding the differences between the institutional view of legitimacy as a property and the psychological view of legitimacy as a perception (Suddaby et al., 2017), Tost (2011) bridges the discrepancies between the institutional and behavioral views by formulating a theoretical framework of legitimacy judgments. In order to form a judgment of generalized legitimacy, the person makes instrumental, moral, and relational evaluations (Tost, 2011).

Immediately after a legitimacy judgment takes place, this legitimacy judgment leads to the intention to comply or react to it. Moreover, it is argued that legitimacy judgments lead to a general perception of legitimacy, thereby influencing behaviors (Tost, 2011). Furthermore, the effectiveness of interventions to induce legitimacy by managers depends on congruence between organizational and personal values because personal values affect the legitimacy perception and govern individual behavioral choices (Tyler, 1997).

Personal Values

Schwartz conceives values as a universal system of cognitive representations of the individual motivations. Schwartz places importance on the concept that people differ only in the relative weight each individual has on each of the value types. Since each of them represents one motivation, it is possible to give high priority to different values simultaneously. Schwartz initially defines ten types of values, later extending his theory by dividing some of those ten value types to account for 19 types of values which form the circular motivational continuum (Schwartz et al. 2012).

Rohan clarifies that all humans have a value system, and this value system is comprised of a specific number of value types. Still, each person places a different relative priority on each of the value types (Rohan 2000, p. 262). We want to highlight that, according to Rohan, the value types defined by Schwartz are unique and apply to all humanity regardless of whether they are being studied in the context of personal or social value systems. However, on a personal level, there will be only one personal value system, while people tend to have more than one social value system. She also points out that the personal and social value systems are comprised of exactly the same value types and are in constant conflict when a person needs to adhere to social norms. (Rohan 2000, p. 267).

Schwartz (1992) diagramed the value types making emphasis on those priorities of adjacent value types will be similar while in opposite values, there will always be conflicting and large differences in priorities. The literature identifies the values construct as a multidimensional and summarizable in terms of a two-dimensional structure (Bardi and Schwartz 2003; Rohan 2000; Schwartz 1992; Schwartz 1999; Schwartz et al. 2001). Even with many values being part of any of the value types (56 values tested by Schwartz), the value construct can be parsimoniously defined as comprised of "four higher-order value types that form two basic, bipolar, conceptual dimensions" (Schwartz 1992, p. 43).

The two bipolar dimensions are openness to change versus conservation and self-enhancement versus self-transcendence. Openness to change orders the values in a way that motivates the person to follow his/her own interest (no matter if it is economical, intellectual, or emotional interest), sometimes in directions riskier than other people would do. Conservation considers the values that look to maintain the status quo and are averse to change and prompt to keep traditions and maintain long-time relationships (Schwartz 1992).

Self-enhancement orders values that motivate people to highlight their own personal interests (even at the expense of others). Self-transcendence promotes values that encourage people to be unselfish and look to benefits to be generally distributed between relatives, others, and society in general (Schwartz 1992).

RESEARCH MODEL

Figure 1 is a diagram of our research model, created to align infosec policy compliance with legitimacy and personal values theories. We aim to modify the full PMT nomology (Boss et al., 2015) by including legitimacy concepts to complement one of the current leading theories in InfoSec policy compliance research.

We posit that legitimacy can be included in the current PMT nomological representation (Boss et al., 2015), and we can replace fear with legitimacy. Furthermore, we argue that threat appraisals are essential in creating legitimacy judgments even though they don’t include all the evaluation elements required to be salient for an individual to form generalized legitimacy (Tost, 2011) and then decide to comply with the security policy.

A legitimacy perspective in voluntary compliance to norms requires exploring and understanding people's values as motivators to perceive the rule as legitimate as well as acceptable moral behavior (Tyler, 1990, 1997). So we introduce Schwartz (1992) 's theory of value types as another important factor contributing to the model and hypotheses development. Personal values can spark relational, moral, and instrumental evaluations leading to generalized legitimacy judgments in the individual (Tost, 2011). Those judgments are the mental evaluations through which the person analyzes and forms the generalized legitimacy perception of the policy (Finch et al., 2015). Furthermore, personal values directly affect behavior (Sagiv & Roccas, 2021; Sagiv & Schwartz, 2021), and it has been demonstrated in different studies about motivators or inhibitors to rule-breaking (Feldman et al., 2015).

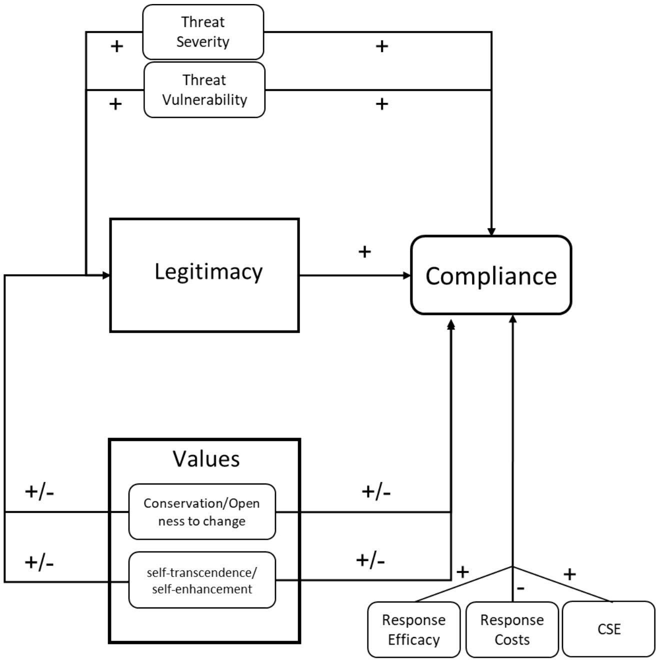

Figure 1: Research Model

Tyler and Blader (2005) based their understanding of compliance with organizational regulations by building on top of the obeying the law literature that emphasizes the need for society to motivate and enforce compliance with the law (Tyler, 1990, 2006b). Tyler and Blader (2005) say that "organizational rules and policies stipulate desired employee behavior, and organizations benefit when those policies are followed" (p. 1145). Compliance is the act of rule-following involving conformity to organizational policies (Tyler & Blader, 2005). Compliance involves actions that align behavior in the workplace with organizational policies (Tyler & Blader, 2005), and organizations can gain voluntary compliance with their rules if authorities and regulations are consistent with what people consider right or wrong (Tyler, 2006b).

The obeying the law literature identifies two important types of an internalized sense of obligation to comply with the law (Tyler, 2006b). First, "citizens may comply with the law because they view the legal authority ... as having a *legitimate* right to dictate their behavior" (Tyler, 2006b, p. 25). This represents people's need to bring their behavior into line with the rule out of the perceived legitimacy of such a norm (Tyler, 2006b). An intrinsic assumption that legitimacy enhances compliance with the law is commonly accepted by lawyers and scholars (Tyler, 2006b). In their view, a legitimacy perception becomes an obligation to comply with the requirements of an authority irrespective of rewards or sanctions (Tyler, 2006b). In his seminal work on obedience to the law, Tyler (1990) analyzed overall levels of legitimacy and its relation to adherence to the law and found that those who view the norm as legitimate were more likely to comply with the law (Tyler, 2006b). Similarly, Tyler (2006b) reviewed 16 studies on protests suggesting that perceived illegitimacy of the norms prompted protest and noncompliance with the law. Furthermore, in the context of organizational policies, it has been demonstrated that a generalized legitimacy perception produces the final result of compliance with the policy (Tyler & Blader, 2005).

In the case of InfoSec policies, organizations seek compliance with security norms and regulations to protect information assets while facilitating coordination and ensuring a secure environment to conduct regular activities smoothly (Kappelman et al., 2021). The extant InfoSec literature highlights the importance of compliance with InfoSec policies to protect organizations from security threats (e.g., Cram et al., 2019; Cram et al., 2021; Moody et al., 2018). Thus, we hypothesize that similar to general organizational policies (Tyler & Blader, 2005), a high legitimacy perception of the proposed policy will lead to higher compliance with it.

H1.A perceived legitimacy will positively influence compliance with the InfoSec policy.

The second type of internalized sense of obligation to comply with the law identified in the literature on obeying the law derives from "the person's desire to behave in a way that accords with his or her own sense of personal morality" (Tyler, 2006b, p. 25). Personal morality is the individual's feeling of an obligation to do what is right according to the person's values system (Tyler, 2006b). Furthermore, Tyler and Blader (2005) demonstrated that the person's values judgments encourage voluntary rule-following (compliance) via self-regulatory mechanisms.

Feldman et al. (2015) studied motivators and inhibitors of breaking the rules. Their study was motivated by reactions to ethical scandals in business that associated the unethical behavior with "falling moral standards caused by lack of values" (Feldman et al., 2015, p. 69). Based on the theory of personal values (Schwartz, 1992), they explained how personal values are associated with rule-breaking behavior and how some second-order construct values are better predictors of rule-breaking behavior than others. We introduced the construct in our model and hypotheses based on existing IS compliance research, integrating the values construct theory by considering the complete second-dimensional order and its bipolar definition (Torres & Crossler, 2019).

Openness to change orders the values in a way that motivates the person to follow their own interest (no matter if it is economical, intellectual, or emotional interest) sometimes in directions riskier than other people would do. Conservation considers the values that look to maintain the status quo and are averse to change and prompt to keep traditions and maintain long-time relationships (Schwartz 1992). In that sense, we propose openness to change will negatively impact the intentions to comply with the policy. At the same time, conservation will be more positively related with intentions to comply with InfoSec policies.

H2a: Conservation is related with intention to comply with InfoSec policy, such that individuals who prioritize this value are more likely to comply with InfoSec policies

H2b: Openness to change is related with intention to comply with InfoSec policy, such that individuals who prioritize openness to change are less likely to comply with InfoSec policies.

Self-enhancement orders values that motivate people to highlight their own personal interests (even at the expense of others). Self-transcendence promotes values that motivate people to be unselfish and look to benefits to be generally distributed between relatives, others, and society in general (Schwartz 1992). As with openness to change, we postulate a negative impact from self-enhancement on intentions to comply with security policy. Thus, we propose self-transcendence to be positively related with the intention to comply with information security policies.

H3a: Self-transcendence is related with intention to comply with InfoSec policy, such that individuals who prioritize this value are more likely to comply with InfoSec policies

H3b: Self-enhancement is related with intention to comply with InfoSec policy, such that individuals who prioritize openness to change are less likely to comply with InfoSec policies.

"Legitimacy shapes the motivations that are engaged when people are involved in understanding the social world" (Tyler, 2006a, p. 386). If a group status is considered legitimate, people are motivated to interpret the rules and norms in ways that justify them because they support their existing social arrangement (Tyler, 2006a). According to "Why People Obey the Law" (Tyler, 1990, 2006b), people focus not only on the personal gain/loss within a particular situation, but they make different evaluations of results of potential behaviors to make an assessment of whether a reaction to the law is appropriate (Tyler, 1990, 2006b). The evaluations previous to the legitimation of a law or regulation have been formulated in a framework of legitimacy judgments (Tost, 2011). In order to form a general perception of legitimacy about a rule, norm, institution, and authority, the person makes instrumental, moral, and relational evaluations (Tost, 2011). Moral evaluations of a law or rule are interpretations of how well the norm adapts to the person's beliefs or values system and how much it supports the person's existing social/ethical arrangements (Sagiv & Roccas, 2021; Tost, 2011).

Personal values have been posited to affect not only behaviors but also people's perceptions and cognition over time and across situations (Sagiv & Schwartz, 2021). Furthermore, the relationship between values and behavior has been proposed to present three organizing principles: accessibility, interpretation, and control (Sagiv & Roccas, 2021). Each principle has a mechanism through which values and behavior are connected, and cognition is translated into action (Sagiv & Roccas, 2021). The interpretation mechanism aligns with the evaluations made by the social system members. In interpreting, an individual compares the legitimacy perception to a reference point to decide if the action from authority is legitimate or not (Finch et al., 2015). We consider that in the case of InfoSec policy compliance, the relationship between evaluation and interpretation as a mechanism to translate values into behavior is consistent with the aforementioned theorization of moral evaluations in legitimacy judgments (Finch et al., 2015; Tost, 2011)

For instance, in a series of experiments where people were presented with a social dilemma (contribution vs. competition), the participants' interpretation (perception) of the dilemma was found to be dependent on their values (Sagiv et al., 2011). When a situation was framed as a form of cooperation, the perception of a boss's just request correlated positively with universalism and benevolence values that reflect concern for others and negatively with power, achievement, and hedonism values that promote self-interests (Sagiv et al., 2011). Similar to the previous example in which values that reflected a concern for others elicited a perception of justness over a request from a boss, the perception of legitimacy is attached to the values and the perceptions of personal vs. group benefits (Tyler, 2006a).

The personal values theory (Schwartz, 1992) posits that self-transcendence values and most of the conservation values (except for security personal), as represented in figure 2, have a social focus in which concerns for others, their family, group, or organizations affect the interpretation and analysis of a possible behavior (Sagiv, 2011; Sagiv & Schwartz, 2021; Sagiv et al., 2011; Schwartz & Sagiv, 1995).

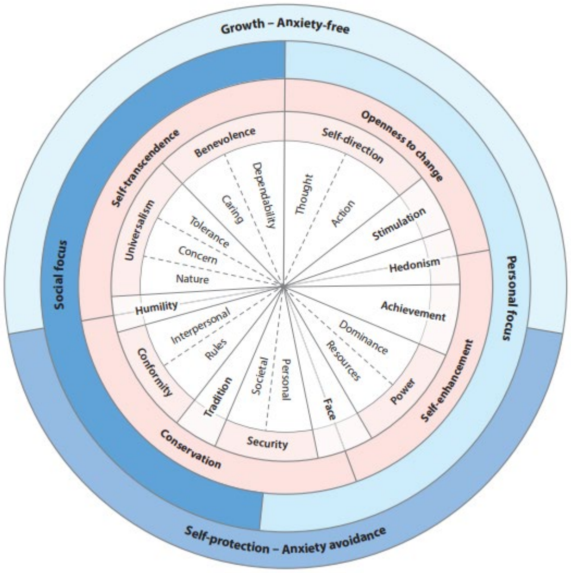

Figure 2. Value types with a social focus

Note. Reprinted from Sagiv, L., and Schwartz, S. H. 2021. "Personal Values across Cultures," Annual Review of Psychology (73), p. 2022

People who value conservation, particularly societal security, refer to maintaining social order, and at the national level, they expect government stability (Sagiv & Schwartz, 2021; Schwartz et al., 2017). Furthermore, tradition and conformity values also tend to make interpretations with a focus on their group or organization and maintain a high standard of moral evaluation (Sagiv, 2011; Sagiv & Roccas, 2021; Sagiv & Schwartz, 2022). Therefore, in the case of InfoSec, in which security becomes an ethical evaluation affecting groups and organizations, we hypothesize that values reflecting security and concern for the group, such as conservation, will positively impact the legitimacy perception of the InfoSec policy. Moreover, following the required tradeoff between opposite values included in the bipolar second-order conceptualization (Bardi & Schwartz, 2003; Feldman et al., 2015; Sagiv, 2011; Schwartz, 2013; Schwartz, 1992; Schwartz et al., 2017;

Schwartz et al., 2001), we propose that self-enhancement will negatively affect the legitimacy perception of the InfoSec policy.

H4a: Conservation positively influences legitimacy perceptions of InfoSec policies.

H4b: Openness to change negatively influences legitimacy perceptions of InfoSec policies.

People who value self-transcendence highly tend to perceive actions from an altruistic perspective, and they also tend to choose occupations that benefit others (Sagiv & Schwartz, 2021). Therefore, in the case of InfoSec policies, in which secure behaviors are promoted for the general organizational benefit over the individual benefit as part of work ethics, we hypothesize that values reflecting concern for others, such as self -transcendence, will positively affect the legitimacy perception of the InfoSec policy. Moreover, following the required tradeoff between opposite values included in the bipolar second-order conceptualization (Bardi & Schwartz, 2003; Feldman et al., 2015; Sagiv, 2011; Schwartz, 2013; Schwartz, 1992; Schwartz et al., 2017; Schwartz et al., 2001), we propose that values that promote self-interest, such as self-enhancement, will negatively affect the legitimacy perception of the InfoSec policy.

H5a: Self-transcendence positively influences legitimacy perceptions of InfoSec policies.

H5b: Self-enhancement negatively influences legitimacy perceptions of InfoSec policies.

PMT consists of two appraisal processes: threat appraisal and coping appraisal. A threat appraisal consists of both vulnerability, which is how the threat applies to their specific circumstances and will effectively occur (Maddux & Rogers, 1983), and severity, which is how harmful or the extent of damage the threat can cause (Wall & Buche, 2017).

We continue drawing from legitimacy theory, proposing that individuals judge the legitimacy of rule, norm, or policy, by using instrumental, moral, and relational criteria (Finch et al., 2015; Tost, 2011). We claim that perceived vulnerability and susceptibility are instrumental and relational evaluations of the policy in order to determine its legitimacy. Furthermore, extant research has demonstrated that both severity and vulnerability are partially mediated by fear, thus directly affecting fear (Boss et al., 2015). Considering that we posit in this research project that legitimacy perceptions replace fear in the PMT nomological network and that threat appraisal can be considered as one of the types of evaluations required to form legitimacy perceptions of an InfoSec policy, the threat appraisal – legitimacy relationship will be positively correlated as described in the following hypotheses:

H6a. An increase in perceived vulnerability to the threat increases the legitimacy of the InfoSec policy.

H6b. An increase in the perceived severity of the threat increases the legitimacy of the InfoSec policy.

PMT has extensively hypothesized the relationship between threat appraisal and compliance with InfoSec policies. An increase in the perceived severity of a threat and perceived threat vulnerability increases compliance with the InfoSec policies due to policies being the mechanism designed for protection commonly described in the InfoSec compliance literature (Boss et al., 2015; Crossler et al., 2014; Herath & Rao, 2009; Johnston & Warkentin, 2010b; Johnston et al., 2015; Mou et al., 2022; Wall & Warkentin, 2019).

H7a. An increase in perceived vulnerability to the threat increases compliance with InfoSec policy.

H7b. An increase in perceived severity of the threat increases compliance with InfoSec policy.

The PMT posits that if the person feels capable of coping with the threat, the threat appraisal process fails, and it is not considered because the threat is unnoticed (Boss et al., 2015; Floyd et al., 2000). The coping appraisal process considers three constructs: self-efficacy, response efficacy, and response costs (Maddux & Rogers, 1983). Response efficacy is how much a person believes that they have an effective response to the threat (Maddux & Rogers, 1983). Self-efficacy is understood as the individual's perception of their ability to accomplish what is required (Compeau & Higgins, 1995) in this case, to avert danger. "Response costs are any perceived direct personal costs (e.g., effort, time, money, or trouble) incurred by the individual by taking protective steps" (Boss et al., 2015, p. 831). As previously posited in PMT research coping appraisal response requires that people believe the response is adequate, perform the response, and the cost will not be high (Aurigemma et al., 2019; Boss et al., 2015; Johnston & Warkentin, 2010b; Johnston et al., 2015; Rogers, 1975; Tsai et al., 2016; Wall & Warkentin, 2019; Warkentin et al., 2016). This leads to the following hypothesis from fear appeals and PMT research that we include in our model:

H8a. An increase in response efficacy increases InfoSec policy compliance

H8b. An increase in self-efficacy increases InfoSec policy compliance

H8c. An increase in response costs decreases InfoSec policy compliance

The model is grounded in the theory of personal values (Schwartz, 1992; Schwartz et al., 2017), the social psychology model of legitimacy and law obedience (Tost, 2011; Tyler, 1990, 2006b; Tyler & Blader, 2005). Additionally, our model comprises general relationships based on the extant PMT and fear appeals security research (Boss et al., 2015). Our research model, incorporating all the above-explained hypotheses, is summarized in figure 3.

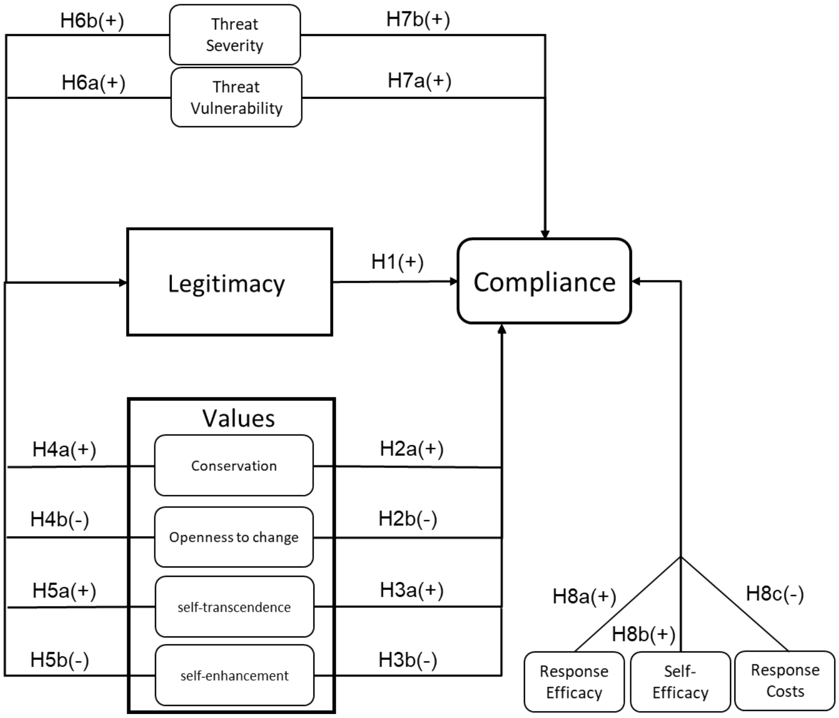

Figure 3. Detailed Research Model

RESEARCH METHODOLOGY

We used an anonymous self-reported survey using Qualtrics and recruited participants from a human subjects pool consisting of students over the age of 18 and enrolled in business classes at a pacific northwest university. Compeau et al. (2012) analyzed multiple studies using student samples to conclude that using students as research subjects is appropriate if the context and theory allow for the generalization of the findings. All constructs were adapted to the InfoSec context by ensuring similar meanings across contexts (Crossler et al., 2018; Hong et al., 2014).

Context

It has been argued that due to rapidly changing technological environments, and when adapting theories from other disciplines, studies need to be properly contextualized. By doing so, we expect to impact the way IS research develops and tests theories, so their predictive power and practical applicability are enhanced (Niederman & March, 2015).

To contextualize this study, we followed the guidelines of Whetten (2009), Hong et al. (2014), and Crossler et al. (2018). Each of these papers addresses the challenges of adapting theory from one context to another. All identify the importance of ensuring similar meaning across contexts as critical to developing context-sensitive explanations of phenomena. Such context-sensitivity does not require surface-level similarity of constructs and items – what Locke (1986) called ecological validity – but rather similarity in the essential features to produce similar underlying meanings for participants. Furthermore, context is an important factor to consider when defining the generalizability goals for our studies (Compeau et al., 2012).

This study's main contextualizing challenge was the global COVID -19 pandemic in 2020-2021. The lockdowns suffered in 2020 and part of 2021 forced people to work and study from home, usually using their mobile devices. The FBI warned the public about criminals exploiting virtual and remote work environments by government agencies and private organizations due to the extent of people working and studying virtually[1].

Our study adopted measures and offered a scenario that capitalized on the critical element of working and studying virtually by using a mobile device. We sought to recreate a scenario where the university suggested voluntary adoption of new work/studying from home InfoSec application targeting mobile devices. We sought a sample frame of individuals experimenting with new policies due to being at home. Adapting the original measures to the business student taking online

[1] https://www.ic3.gov/Media/Y2020/PSA200401

synchronous classes from the home context provided an opportunity to understand the impact of new InfoSec policies. Furthermore, it caters to the information security policymaking area, in which developing work from home policies has become a new challenge. In terms of generalizability and following Compeau et al. (2012) guidelines for research using student subjects, we state that our results from business students can be generalizable to current and future workers. The sample frame also provides a key distinction in participant age, which may help extend understanding of generational differences in InfoSec policy compliance.

Measures

The measures used in the study, found in appendix 1, are specified below. The changes in items reflect differences in the context of InfoSec policies while preserving original meanings and purposes.

For the values construct, we used the Portrait Values Questionnaire (PVQ) measure used in previous research and developed by Schwartz et al. (2017) to extend the values construct's cross-cultural validity. In addition, we adapted the measures from the existing literature: legitimacy and policy compliance were adjusted from the management literature (Tyler & Blader, 2005). For threat appraisal and coping appraisal, we adapted previous items from the PMT literature (Boss et al., 2015; Milne et al., 2000; Woon et al., 2005).

We conducted a preliminary analysis of the management literature for the legitimacy construct and found a widely cited measure that we decided to use in this project (Tyler & Blader, 2005). As a result, the wording of the legitimacy and compliance items was modified to target InfoSec policies and the information security organization specifically, as previously adapted in the IS literature (Son, 2011). In addition, we added two more items to the scale, accounting for other possible types of legitimacy. All the adaptations were made as our contextualization process suggested (Crossler et al., 2018; Hong et al., 2013), and the changes were made to the instrument before collecting data from students.

Procedures

The survey was conducted through an online platform, and students were offered the opportunity to receive extra credit for their voluntary participation in the study. Invitations were anonymously sent to all students registered to participate in online studies during the time campus was closed, and all students took their classes online. The students were told their participation was voluntary and were offered extra credit for participating in the study. The data was anonymous; identifiers were collected on a separate platform by the lab in charge of running the surveys to provide extra credit for their involvement.

Students were given a URL for the survey. When participants clicked on the survey invitation, they saw a welcome screen outlining the research and asking for their consent to participate. If participants agreed to participate, they could proceed to complete the survey. The survey properties were set to allow participants to leave any items blank, read ahead in the questionnaire before completing items and return to prior questions. An additional procedural step was the inclusion of two attention checks as a primary instrument validation principle (Boudreau et al., 2001)

Results

Analysis

We collected a total of 500 responses. After removing incomplete data and careless respondents, there were 259 usable responses, as presented in table 1. We followed Schwartz et al. (2017) recommendations of dropping respondents who used the same answer for more than 49 items (of a total of 57 items in the PVQ) or that missed more than 28 answers; in our table, they are called values outliers.

Total Responses	500
Responses Removed	
Did not consent	4
Incomplete responses	52
Failed attention checks	96
Duplicate IDs	71
Speeders/Slow answers (less than 4 minutes, more than 50 mins)	11
Values outliers	7
Usable Responses	259
% Usable responses	51.8 %
Average Duration (usable responses)	15.24 mins

Table 1. Responses

We attribute the relatively high number of students who failed the attention checks to how extra credit was assigned. Students received extra credit for participating in the study, regardless of whether they failed the attention checks. This undoubtedly led some students, whose only motivation for participating was to earn extra credit, to respond without carefully attending to the questions. Including the three attention check questions gives us confidence that these responses have been filtered out. Similarly, the duplicate IDs could also be due to how the extra credit was assigned. The students had access to many studies over the semester, and in order to receive extra credit, they needed to participate in at least two surveys. When the survey was made available to students, it was the only available survey on the platform. Students who needed two surveys to obtain extra credit could have tried to fulfill the requirement by taking the same survey twice.

Table 2 shows the demographic details of the sample. The sample has more women (59.8%). The sample is mostly white (69.9%). The average age is 22 years old, and most students (85.6%) are in their third or fourth year of higher education.

AGE			**Ethnicity**			**Gender**			**Year in School**		
	N	**%**		**N**	**%**		**N**	**%**		**N**	**%**
18	11	4.2	White	181	69.9	Male	104	40.2	First	18	6.9
19	24	9.3	Black	10	3.9	Female	155	59.8	Second	16	6.2
20	70	27.0	Indian	3	1.2				Third	131	50.6
21	82	31.7	Asian	36	13.9				Fourth	91	35.1
22	39	15.1	Hawaii	3	1.2				Other	1	0.4
23	3	1.2	Hispanic	26	10				Missing	2	0.8
>23	27	10.4									
Missing	3	1.2									

Table 2. Participant Age, Gender and Year in School

Table 3 provides the breakdown of the sample in terms of major. 85% of the sample are business majors, with the highest percentages in marketing, accounting, and general business.

Major	**N**	**Percent**
Marketing	63	24.3%
Non-business majors	38	14.7%
Accounting	37	14.3%
General Business	30	11.6%
Other Business Majors	30	11.6%
Finance	24	9.3%
MIS	15	5.8%
Management	12	4.6%
International Bussiness	10	3.9%

Table 3. Participant Majors

Table 4 reports means (based on unweighted averages of the scale items), standard deviations, and ranges for each of the constructs in our model. We note that for all constructs except the values constructs, the responses cover nearly the full range of possible scores, thus providing adequate variability for our modeling.

Construct	Mean	Std Dev	Range
Compliance	3.66	0.99	1-5
Legitimacy	3.54	0.58	1.2-4.9
Threat Severity	3.50	0.69	1-5
Threat Vulnerability	2.69	0.95	1-5
Response Efficacy	3.56	0.70	1-5
Response Cost	3.24	0.71	1.25-5
CSE	3.10	0.98	1-5
Conservation	4.35	0.67	2.4-5.87
Openness to Change	4.95	0.61	3.25-6
Self-Transcendence	4.93	0.57	3.27-6
Self Enhancement	4.06	0.77	2-5.89

Table 4. Construct Means and Distributions

Assessment of the Measurement Model

We used SmartPLS 3 (Ringle et al., 2015) to analyze the measurement and structural models. To assess the measurement model, we tested the reliability, convergent validity, and discriminant validity of the measures (Lowry & Gaskin, 2014) as well as additional tests recommended for SmartPLS (Hair et al., 2016). To assess the structural model, we used bootstrapping with 5000 samples.

The values construct was derived by calculating the mean score for each of the 19 first-order values as the mean of the raw ratings given to the items collected for the value. According to Schwartz and Butenko (2014), it is necessary to correct for individual differences in the use of the response scale before performing analyses. Scale use differences can produce results that can be misleading and inaccurate conclusions due to values always functioning as a system (Schwartz, 2013; Seligman & Katz, 1996). With the right scores per value, we inserted those items as reflecting the second-order values constructs used in our hypothesis formulation. Humility and face are recommended to be treated as separate values when it comes to second-order constructs since trying to include them as part of the already defined second-order constructs have shown inconsistent results (Cieciuch et al., 2014; Schwartz & Butenko, 2014; Schwartz et al., 2012;

Schwartz et al., 2017). In our theorization process, we included only the second-order constructs. Thus, face and humility were not considered as part of any of the constructs under analysis.

The first assessment of the measurement model indicated potential problems with a few constructs. In total, for all items collected in the survey, fifteen items had loadings below 0.70. Hair et al. (2016) argue that “indicators with outer loadings between 0.40 and 0.70 should be considered for removal from the scale only when deleting the indicator leads to an increase in the composite reliability … or average variance extracted … above the suggested threshold value” (pp.112-113).

We reviewed each of the items that loaded below 0.70 and removed the items with very low loadings (below 0.40) and/or where a robust conceptual argument could be made. If an item loaded between 0.5 and 0.7 and the overall construct metrics met their required thresholds, we did not remove the item. In our analysis, to increase the reliability of the constructs, we dropped two items from the legitimacy measure (2 and 7), two items from the CSE measure (3 and 7), one item from threat severity (2), one item from the response costs measure (1). With these items removed, we re-ran the model. The loadings for the retained items were satisfactory. The composite reliabilities were all above 0.70, and the average variances extracted were all above 0.50 except for self-transcendence (0.49) (Table 6).

For discriminant validity, we examined the individual item cross-loadings, which were all less than the constructs’ loadings. We also compared the shared variance between constructs in comparison to the shared variance between each construct and its own measures (Fornell & Larcker, 1981). We identified high correlations between the values construct. This is a consistent finding that values literature has found common among adjacent values since the value types are linearly dependent (Schwartz et al., 2017). Noting that high correlations between the values included in the model will likely be present and that the constructs should still be considered individually for the sake of data analysis

All the constructs meet the conditions for discriminant validity as well. We examined the individual item cross-loadings for discriminant validity, which were lower than the constructs' loadings. We also compared the shared variance between constructs in relation to the shared variance between each construct and its own measures (Fornell & Larcker, 1981). In this case, all constructs meet the conditions for discriminant validity (Table 6). For discriminant validity, the Heterotrait-Monotrait Ratio (HTMT) can be used as well, and none of the values should exceed the 0.85 threshold (Henseler et al., 2015). For this model, the highest HTMT value was 0.78 (Vulnerability and Severity), which is natural since both are related as they are considered the threat appraisal. Also, you can see high correlations between the values construct, which is expected due to the nature of the values construct as a system, including all the values.

		ICR	**Cronbach Alpha**
1	Compliance	0.928	0.88
2	Legitimacy	0.893	0.86
3	Threat Appraisal Severity	0.835	0.69
4	Threat Appraisal Vulnerability	0.928	0.89
5	Response Costs	0.845	0.75
6	Response Efficacy	0.840	0.80
7	CSE	0.907	0.88
8	Openness to change	0.837	0.76
9	Conservation	0.799	0.68
10	Self-enhancement	0.787	0.55
11	Self-transcendence	0.824	0.74

Table 5. Composite Reliability, Cronbach Alpha and AVE

		1	2	3	4	5	6	7	8	9	10	11
1	Compliance	0.90										
2	Legitimacy	0.47	0.72									
3	Threat Severity	0.28	0.32	0.80								
4	Threat Vulnerability	0.24	0.28	0.63	0.90							
5	Response Costs	-0.07	-0.19	-0.12	-0.11	0.81						
6	Response Efficacy	0.33	0.53	0.38	0.44	-0.15	0.76					
7	CSE	0.14	0.20	0.07	0.03	-0.13	0.18	0.74				
8	Openness to change	0.11	0.02	0.01	0.03	0.02	0.05	0.12	0.80			
9	Conservation	0.30	0.24	0.24	0.21	0.02	0.25	0.09	0.35	0.71		
10	Self-enhancement	0.10	0.11	0.11	0.15	0.00	0.19	0.10	0.47	0.38	0.81	
11	Self-transcendence	0.20	0.15	0.11	0.06	-0.04	0.12	0.17	0.55	0.46	0.43	0.70

Note: Diagonal elements (shaded) are the square root of the average variance extracted (AVE). Off-diagonal elements are the correlations among constructs. For discriminant validity, diagonal elements should be larger than off-diagonal elements.

Table 6. Discriminant Validity

Overall, the reliability scores and the fit of the corresponding measurement model were acceptable. The SRMS saturated was .071, which presents an acceptable model fit (< 0.8) (Brown, 2015; Hair et al., 2016).

Assessment of the Structural Model

We found mixed results for the hypotheses in the research model presented in Figure 5. First, legitimacy was a very strong predictor of compliance with the security policy. From the values system, only conservation had a significant effect on compliance as well as on legitimacy. Finally, the threat appraisal constructs (vulnerability and severity) had substantial significant effects on legitimacy, even though the path threat vulnerability - legitimacy was significant only at the .1 level (Beta = .102; *p* = .069).

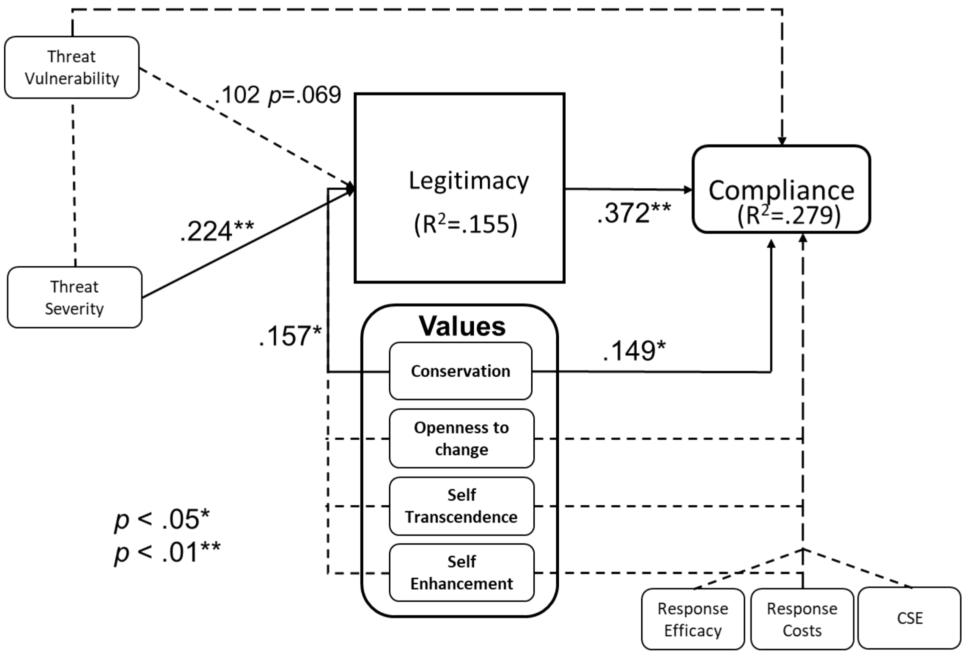

Figure 4: Results

Two things were surprising from our results. First, the threat appraisal (vulnerability and severity) constructs did not directly influence compliance with the security policy. We ran a mediation analysis as Hair et al. (2016) recommended, finding that legitimacy fully mediated the relationship between the threat appraisal constructs and compliance with the security policy. Furthermore, the coping appraisal constructs didn't significantly influence compliance with the security policy as usually supported in InfoSec research using PMT as the theoretical framework.

Our mediation analysis considered that threat appraisal and coping appraisal go through a legitimacy judgment evaluation process. The evaluations previous to legitimizing a law or regulation have been formulated in a framework of legitimacy judgments (Tost, 2011). In order to form a general perception of legitimacy about a rule, norm, institution, and authority, the person makes instrumental, moral, and relational evaluations (Tost, 2011). We include moral evaluations of a law or rule as interpretations of how well the norm adapts to the person's beliefs or values system and how much it supports the person's existing social/ethical arrangements (Sagiv & Roccas, 2021; Tost, 2011). Also. Tost (2011) posits that in order to form a judgment of generalized legitimacy, the person makes other instrumental and relational evaluations (Tost, 2011). PMT considers the coping appraisal a mechanism through which evaluations of the personal cost, the efficacy of the proposed solution, and the capability to administer the remedy on its own are connected to the expected behavior (Warkentin et al., 2012). This mechanism aligns with the evaluations made in legitimacy judgments. In interpreting, an individual compares the legitimacy perception to a reference point to decide if the action from authority is legitimate or not (Finch et al., 2015; Tost, 2011). In the case of InfoSec policy compliance, the relationship between evaluation and legitimacy as a mechanism to translate the coping appraisal into behavior is consistent with the aforementioned theorization of instrumental and relational evaluations in legitimacy judgments (Tost, 2011)

Immediately after a legitimacy judgment takes place, this legitimacy judgment leads to the intention to comply or react to it. Moreover, it is argued that legitimacy judgments lead to a general perception of legitimacy, thereby influencing behaviors (Tost, 2011). We continue drawing from legitimacy theory, proposing that individuals judge the legitimacy of rule, norm, or policy, by using instrumental, moral, and relational criteria (Finch et al., 2015; Tost, 2011). Let's consider that the threat and coping appraisal are instrumental and relational evaluations of the policy. The evaluations need to be made before the person determines the legitimacy of the proposed policy. The results from our mediation analysis are summarized in figure 5.

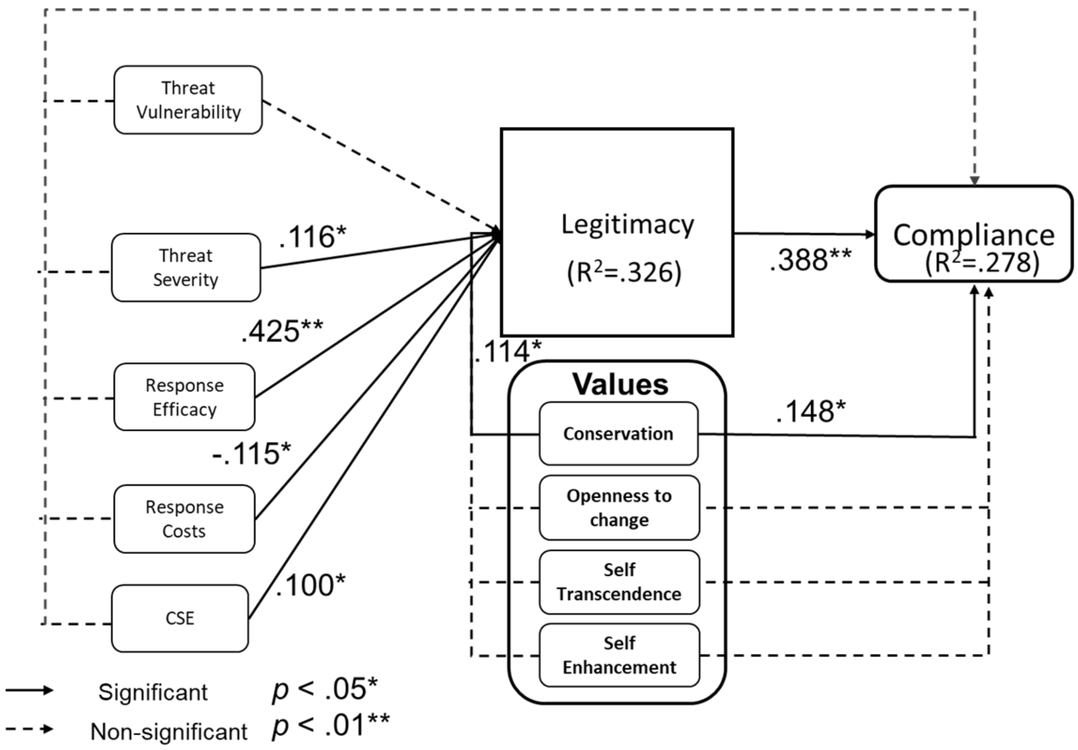

Figure 5: Mediation Analysis Results

Our full mediation analysis suggests that threat severity significantly influences legitimacy, while all the coping appraisal constructs (CSE, Response Costs, and Response Efficacy) significantly influence a legitimacy perception. Regarding the values construct, the results were surprising since the only value that had a significant influence on compliance was conservation. All other values (openness to change, self-enhancement, self-transcendence) were not significant towards compliance with the security policy. Regarding the expected influence of values in the formation of legitimacy perceptions, again, conservation was the only value with a significant influence on legitimacy. The mediation test (Hair et al., 2016) indicates that legitimacy perceptions partially mediated the relationship between conservation and compliance. Finally, similar to the values–compliance relationship, all other values (openness to change, self-enhancement, self-transcendence) were not significant towards legitimacy perceptions.

Common Method Bias

Because our data were collected in a single survey, it is essential to rule out CMB as a threat to validity. We followed the approach of Simmering et al. (2015) as implemented by Chin et al. (2013) for PLS, using blue attitude (Miller & Chiodo, 2008) as a marker variable. The results produced very similar results, thus supporting the claim that common method bias is not present in our study.

DISCUSSION

Our study yields important implications for theory. Expanding upon our findings of the importance of legitimacy perceptions in compliance with InfoSec policies, this section provides a detailed reflection on our results in relation to our model and hypothesis.

The most important implication is similar to what has been found in general law (Tyler, 1990, 1997) and organizational policies (Tyler & Blader, 2005). Legitimacy perceptions of a suggested security request or policy from the information security department heavily influence compliance with such policy. In an information security context, compliance involves actions that align behavior in the workplace with security policies (Tyler & Blader, 2005), and organizations try to gain voluntary compliance with their rules which is only possible if employees consider the particular policy legitimate (Tyler, 2006b)

Introducing legitimacy perceptions as the primary motivator to compliance in the PMT nomological network is a substantial contribution to the InfoSec policy compliance literature discussing the effectiveness of fear appeals in producing sustainable and permanent secure behaviors in employees and IT users (Renaud & Dupuis, 2019).

The PMT literature shows inconsistent and sometimes inconclusive results about the relationships between the five main independent variables (threat severity, threat susceptibility, response costs, response efficacy, and self-efficacy) and intention to comply (Mou et al., 2022). Furthermore, in Mou et al.'s metanalysis, only three of PMT's five determinants of security intention are supported. Similar to our results, they found inconsistent support for perceived vulnerability and no evidence for response cost (Mou et al., 2022). Our results indicate that in the presence of legitimacy, none of PMT" s predictors influence intention to comply with the security policy.

In the PMT literature, multiple studies do not include fear as an intermediary step between threat appraisal and compliance or behavioral intention (Mou et al., 2022) (e.g., Johnston & Warkentin, 2010a; Johnston et al., 2015; Wall & Warkentin, 2019). Furthermore, when fear is included in the model, the relationship between threat appraisal and behavioral intention is partially mediated by fear. The threat appraisal constructs directly influence behavioral intention (Boss et al., 2015; Mou et al., 2022). The fact that in our results, legitimacy fully mediated the relationship between threat and coping appraisal with compliance is fascinating. It indicates that legitimacy perceptions are based on instrumental, relational, and moral evaluations (Tost, 2011) that the person makes before committing to obey or accept a new rule.

Furthermore, our mediation analysis of our data suggests that all coping appraisal constructs (response efficacy, self-efficacy, and response costs) exert a significant influence on legitimacy perceptions. This analysis provides empirical support to Tost (2011) legitimacy judgments conceptualization, indicating that instrumental, relational, and moral evaluations precede and lead to a general perception of legitimacy that ultimately influences our behaviors (Tost, 2011).

The relationship between the values construct and legitimacy was not according to the expectation and was somehow disappointing. Tyler (1990), in his seminal work "why people obey the law," mentions that the individual makes a relational evaluation between the authority and the self. Based on how similar they are, or in other words, how much of the values are shared, the person forms a legitimate perception of the law. However, even if the person believes the law is legitimate, whenever there is a discrepancy between the personal values system and the authority values system, obedience to the law will be diminished due to the conflict of values. We speculate that, in our context, students perceive the IT security organization as a holder of conservation values. If that is the case, only students holding the same value type (conservation) would be motivated to accept the suggestion from the IT department based on values similarity.

Moreover, the evaluation of similar values can be what drives the influence of conservation in legitimacy perceptions. Because the person identifies with the organization's values, the new rule or suggested behavior is perceived as legitimate based on a relational evaluation of the organization's values structure compared to the personal values system.

Our study yields important recommendations for practice as well. Compliance with security policies requires that the organization develops a series of actions intending to align behavior in the workplace with organizational policies (Tyler & Blader, 2005). The best way organizations can gain voluntary compliance with their rules is by inducing a perception of such a rule being legitimate and consistent with what people consider brings benefits to both the employee and the organization.

This study helps identify which values to watch for and how the importance of reinforcing security values in the workforce to promote the proper and long-term implementation of security policies. This study highlights the importance of workers with conservation type of values when aiming to present InfoSec policy compliance as an element of personal gain rather than a tool to keep them safe and secure. When workers driven by these values understand that the policy will keep them safe and does not require substantial changes according to their traditions, they will be more likely to comply with security policies, even more, when they perceive the rule to be according to their personal value system.

Limitations and Future Research

The findings of our study must be considered in light of our study's limitations. Covid 19 drastically changed the context in which the study was developed. Our efforts to contextualize the online class environment limit our ability to conclude whether our findings can be fully generalized (Cram et al., 2019). COVID -19 forced our base to go through a contextual change regarding compliance with security policies that could have potentially modified their legitimacy perceptions when it comes to abiding by rules proposed by the IT department. Replications in a different context and hopefully under normal conditions could shed light on the personal values – legitimacy, and the personal values – compliance relations. Further research can explain the lack of significant results for most of the value types. Currently, there are studies in progress identifying possible value changes due to the COVID -19 pandemic (Sagiv & Schwartz, 2021)

Finally, we measured self-reported compliance with the security policy rather than behavioral intention. We aimed to study the actual security behavior as suggested in the InfoSec literature (Crossler et al., 2013; Lowry et al., 2017). We agree with scholars arguing that in a research design measuring actual behavior, the results may be different, and we could potentially provide stronger evidence for the values system influencing and motivating secure behaviors (Sagiv & Schwartz, 2021).

Future research seeking to identify the interventions needed to modify the individual's legitimacy perceptions and their values scale is warranted in order to alter and improve compliance with

InfoSec policies. Values have been proposed to be changed through a series of processes: "identification; adaptation; priming; consistency maintenance; and direct persuasion" (Sagiv & Schwartz, 2021, p. 28.13), and legitimacy perceptions through the communication style used by the organization (Barrett et al., 2013).

REFERENCES

Aurigemma, S., Mattson, T., & Leonard, L. (2019). Evaluating the Core and Full Protection Motivation Theory Nomologies for the Voluntary Adoption of Password Manager Applications. *AIS Transactions on Replication Research*, *5*, 1-21. https://doi.org/10.17705/1atrr.00035

Bardi, A., & Schwartz, S. H. (2003). Values and Behavior: Strength and Structure of Relations. *Personality and Social Psychology Bulletin*, *29*(10), 1207-1220.

Barrett, M., Heracleous, L., & Walsham, G. (2013). A Rhetorical Approach to IT Diffusion: Reconceptualizing the Ideology-Framing Relationship in Computerization Movements. *MIS Quarterly*, *37*(1), 201-220.

Boss, S., Galletta, D., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors. *MIS Quarterly*, *39*(4), 837-864.

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

Brown, T. A. (2015). *Confirmatory Factor Analysis for Applied Research*. Guilford publications.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly*, *34*(3), 523-548.

Chin, W. W., Thatcher, J. B., Wright, R. T., & Steel, D. (2013). Controlling for common method variance in PLS analysis: the measured latent marker variable approach. In *New perspectives in partial least squares and related methods* (pp. 231-239). Springer.

Cieciuch, J., Davidov, E., Vecchione, M., Beierlein, C., & Schwartz, S. H. (2014). The Cross-National Invariance Properties of a New Scale to Measure 19 Basic Human Values: A Test Across Eight Countries. *Journal of cross-cultural psychology*, *45*(5), 764-776.

Compeau, D., & Higgins, C. (1995). Computer Self-Efficacy: Development of a Measure and Initial Test. *MIS Quarterly*, 189-211.

Compeau, D., Marcolin, B., Kelley, H., & Higgins, C. (2012). Research Commentary—Generalizability of Information Systems Research Using Student Subjects—A Reflection on our Practices and Recommendations for Future Research. *Information Systems Research*, *23*(4), 1093-1109.

Constantinides, P., & Barrett, M. (2014). Information Infrastructure Development and Governance as Collective Action. *Information Systems Research*, *26*(1), 40-56.

Cooren, F., & Robichaud, D. (2013). *Organization and Organizing*. https://doi.org/10.4324/9780203094471

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

Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2021). When Enough is Enough: Investigating the Antecedents and Consequences of Information Security Fatigue. *Information systems journal*.

Crossler, R. E., Di Gangi, P. M., Johnston, A. C., Bélanger, F., & Warkentin, M. (2018). Providing Theoretical Foundations: Developing an Integrated Set of Guidelines for Theory Adaptation. *Communications of the Association for Information Systems*, *43*(1), 31.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future Directions for Behavioral Information Security Research. *Computers & Security*, *32*, 90-101.

Crossler, R. E., Long, J. H., Loraas, T. M., & Trinkle, B. S. (2014). Understanding Compliance with Bring Your Own Device Policies Utilizing Protection Motivation Theory: Bridging the Intention-Behavior Gap. *Journal of Information Systems*, *28*(1), 209-226.

CSIS, M. (2018). *Economic Impact of Cybercrime- No Slowing Down*. Retrieved October from https://www.mcafee.com/enterprise/en-us/solutions/lp/economics-cybercrime.html

Deephouse, D. L., Bundy, J., Tost, L. P., & Suchman, M. C. (2017). Organizational Legitimacy: Six Key Questions. *The SAGE handbook of organizational institutionalism*, 27-54.

EY. (2018). *Cybersecurity regained: preparing to face cyber attacks. 20th Global Information Security Survey 2017–18*. Retrieved November from https://www.ey.com/Publication/vwLUAssets/GISS_report_2017/$FILE/REPORT%20-%20EY%20GISS%20Survey%202017-18.pdf

Feldman, G., Chao, M. M., Farh, J.-L., & Bardi, A. (2015). The Motivation and Inhibition of Breaking the Rules: Personal Values Structures Predict Unethicality. *Journal of Research in Personality*, *59*, 69-80.

Finch, D., Deephouse, D., & Varella, P. (2015). Examining an Individual's Legitimacy Judgment Using the Value–Attitude System: The Role of Environmental and Economic Values and Source Credibility. *Journal of Business Ethics*, *127*(2), 265-281.

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A Meta-Analysis of Research on Protection Motivation Theory. *Journal of applied social psychology*, *30*(2), 407-429.

Fornell, C., & Larcker, D. F. (1981). Structural Equation Models with Unobservable Variables and Measurement Error: Algebra and Statistics. In: SAGE Publications Sage CA: Los Angeles, CA.

Hair, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2016). *A primer on partial least squares structural equation modeling (PLS-SEM)*. Sage publications.

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new Criterion for Assessing Discriminant Validity in Variance-Based Structural Equation Modeling. *Journal of the academy of marketing science*, *43*(1), 115-135.

Herath, T., & Rao, H. R. (2009). Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations. *European Journal of Information Systems*, *18*(2), 106-125.

Hong, W., Chan, F. K., Thong, J. Y., Chasalow, L. C., & Dhillon, G. (2013). A Framework and Guidelines for Context-Specific Theorizing in Information Systems Research. *Information Systems Research*, *25*(1), 111-136.

Hong, W., Chan, F. K., Thong, J. Y., Chasalow, L. C., & Dhillon, G. (2014). A framework and guidelines for context-specific theorizing in information systems research. *Information systems research*, *25*(1), 111-136.

Hsu, C., Lin, Y.-T., & Wang, T. (2015). A Legitimacy Challenge of a Cross-Cultural Interorganizational Information System. *European Journal of Information Systems*, *24*(3), 278-294.

Johnston, A. C., & Warkentin, M. (2010a). Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly*, 549-566.

Johnston, A. C., & Warkentin, M. (2010b). Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly*, *34*(3), 549-566.

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset through Sanctioning Rhetoric. *MIS Quarterly*, *39*(1), 113-134.

Kam, H.-J., Katerattanakul, P., Gogolin, G., & Hong, S. (2013). Information Security Policy Compliance in Higher Education: A Neo-Institutional Perspective. PACIS,

Kappelman, L., Maurer, C., McLean, E., Kim, K., Johnson, V., Snyder, M., & Torres, R. (2021). The 2020 SIM IT Issues and Trends Study. *MIS Quarterly Executive*, *20*(1), Article 8.

Kappelman, L., Torres, R., McLean, E., Maurer, C., Johnson, V., & Kim, K. (2019). The 2018 SIM IT Issues and Trends Study. *MIS Quarterly Executive*, *18*(1), 7.

Kelley, H. H., & Thibaut, J. W. (1959). *The Social Psychology of Groups*. New York, Wiley.

Kish-Gephart, J. J., Harrison, D. A., & Treviño, L. K. (2010). Bad Apples, Bad Cases, and Bad Barrels: Meta-Analytic Evidence About Sources of Unethical Decisions at Work. *Journal of Applied Psychology*, *95*(1), 1.

Lawson, S. T., Yeo, S. K., Yu, H., & Greene, E. (2016). The Cyber-Doom Effect: The Impact of Fear Appeals in the US Cyber Security Debate. 2016 8th International Conference on Cyber Conflict (CyCon),

Locke, E. A. (1986). Generalizing from laboratory to field settings: Research findings from industrial–organizational psychology, organizational behavior, and human resource management. *Industrial-Organizational Psychologist*, *33*(2), 57-64.

Lowry, P. B., Dinev, T., & Willison, R. (2017). Why Security and Privacy Research Lies at the Centre of the Information Systems (IS) Artefact: Proposing a Bold Research Agenda. *European Journal of Information Systems*, *26*(6), 546-563.

Lowry, P. B., & Gaskin, J. (2014). Partial Least Squares (PLS) Structural Equation Modeling (SEM) for Building and Testing Behavioral Causal Theory: When to Choose It and How to Use It. *IEEE transactions on professional communication*, *57*(2), 123-146.

Maddux, J. E., & Rogers, R. W. (1983). Protection Motivation and Self-Efficacy: A Revised Theory of Fear Appeals and Attitude Change. *Journal of experimental social psychology*, *19*(5), 469-479.

Malekos-Smith, Z., & Lostri, E. (2020). *The Hidden Costs of Cybercrime*. https://www.mcafee.com/enterprise/en-us/solutions/lp/economics-cybercrime.html

Marett, K., Vedadi, A., & Durcikova, A. (2019). A Quantitative Textual Analysis of Three Types of Threat Communication and Subsequent Maladaptive Responses. *Computers & Security*, *80*, 25-35.

Miller, B., & Chiodo, B. (2008). Academic entitlement: Adapting the equity preference questionnaire for a university setting. Southern Management Association meeting, St. Pete Beach, FL,

Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and Intervention in Health-Related Behavior: A Meta-Analytic Review of Protection Motivation Theory. *Journal of applied social psychology*, *30*(1), 106-143.

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

Mou, J., Cohen, J. F., Bhattacherjee, A., & Kim, J. (2022). A Test of Protection Motivation Theory in the Information Security Literature: A Meta-Analytic Structural Equation Modeling Approach. *Journal of the Association for Information Systems*, *23*(1), 196-236.

Niederman, F., & March, S. (2015). Reflections on Replications. *AIS Transactions on Replication Research*, *1*, 1-16.

Pearlson, K., Gerth, T., Mauer, C., Sumner, M., & Jain, R. (2020). The 2019 SIM IT Issues and Trends Study: Emerging Research. *MIS Quarterly Executive*.

Renaud, K., & Dupuis, M. (2019). Cyber Security Fear Appeals: Unexpectedly Complicated. Proceedings of the New Security Paradigms Workshop,

Ringle, C., Wende, S., & Becker, J. S. (2015). 3 (Version 3.2. 3). *SmartPLS GmbH: Boenningstedt, Germany*.

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. *The journal of psychology*, *91*(1), 93-114.

Rogers, R. W. (1983). Cognitive and Psychological Processes in Fear Appeals and AttitudeCchange: A Revised Theory of Protection Motivation. *Social psychophysiology: A sourcebook*, 153-176.

Rohan, M. J. (2000). A Rose by any Name? The Values Construct. *Personality and social psychology review*, *4*(3), 255-277.

Sagiv, L. (2011). Personal Values, National Culture and Organizations: Insights Applying the Schwartz Value Framework. *The handbook of organizational culture and climate*, *2*, 515-537.

Sagiv, L., & Roccas, S. (2021). How do Values Affect Behavior? Let me Count the Ways. *Personality and social psychology review*, *25*(4), 295-316.

Sagiv, L., & Schwartz, S. H. (2021). Personal Values Across Cultures. *Annual review of psychology*, *73*, 2022.

Sagiv, L., & Schwartz, S. H. (2022). Personal Values Across Cultures. *Annual review of psychology*, *73*, 517-546.

Sagiv, L., Sverdlik, N., & Schwarz, N. (2011). To Compete or to Cooperate? Values' Impact on Perception and Action in Social Dilemma Games. *European Journal of Social Psychology*, *41*(1), 64-77.

Schwartz, S. (2013). Value Priorities and Behavior: Applying. The Psychology of Values: The Ontario Symposium,

Schwartz, S. H. (1992). Universals in the Content and Structure of Values: Theoretical Advances and Empirical Tests in 20 Countries. In *Advances in experimental social psychology* (Vol. 25, pp. 1-65). Elsevier.

Schwartz, S. H. (1999). A Theory of Cultural Values and Some Implications for Work. *Applied psychology*, *48*(1), 23-47.

Schwartz, S. H., & Bardi, A. (1997). Influences of Adaptation to Communist Rule on Values Priorities in Eastern Europe. *Political psychology*, *18*(2), 385-410.

Schwartz, S. H., & Butenko, T. (2014). Values and Behavior: Validating the Refined Value Theory in Russia. *European Journal of Social Psychology*, *44*(7), 799-813.

Schwartz, S. H., Cieciuch, J., Vecchione, M., Davidov, E., Fischer, R., Beierlein, C., Ramos, A., Verkasalo, M., Lönnqvist, J.-E., & Demirutku, K. (2012). Refining the Theory of Basic Individual Values. *Journal of personality and social psychology*, *103*(4), 663-688.

Schwartz, S. H., Cieciuch, J., Vecchione, M., Torres, C., Dirilem-Gumus, O., & Butenko, T. (2017). Value Tradeoffs and Behavior in Five Countries: Validating 19 Refined Values. *European Journal of Social Psychology*, *47*, 241-258.

Schwartz, S. H., Melech, G., Lehmann, A., Burgess, S., Harris, M., & Owens, V. (2001). Extending the Cross-Cultural Validity of the Theory of Basic Human Values with a Different Method of Measurement. *Journal of cross-cultural psychology*, *32*(5), 519-542.

Schwartz, S. H., & Sagiv, L. (1995). Identifying Culture-Specifics in the Content and Structure of Values. *Journal of cross-cultural psychology*, *26*(1), 92-116.

Seligman, C., & Katz, A. N. (1996). The Dynamics of Value Systems. The Psychology of Values: The Ontario Symposium,

Simmering, M. J., Fuller, C. M., Richardson, H. A., Ocal, Y., & Atinc, G. M. (2015). Marker variable choice, reporting, and interpretation in the detection of common method variance: A review and demonstration. *Organizational Research Methods*, *18*(3), 473-511.

Siponen, M., & Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly*, *34*(3), 487-502.

Son, J.-Y. (2011). Out of Fear or Desire? Toward a Better Understanding of Employees' Motivation to Follow IS Security Policies. *Information & Management*, *48*(7), 296-302.

Suchman, M. C. (1995). Managing Legitimacy: Strategic and Institutional Approaches. *Academy of management Review*, *20*(3), 571-610. https://doi.org/10.2307/258788

Suddaby, R., Bitektine, A., & Haack, P. (2017). Legitimacy. *Academy of Management Annals*, *11*(1), 451-478.

Torres, C. I., & Crossler, R. E. (2019). Information Security Compliance: A Complete Values View. *AMCIS 2019 Proceedings*. https://aisel.aisnet.org/amcis2019/adv_info_systems_research/adv_info_systems_research/3/

Tost, L. P. (2011). An Integrative Model of Legitimacy Judgments. *Academy of management Review*, *36*(4), 686-710.

Tsai, H.-y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding Online Safety Behaviors: A Protection Motivation Theory Perspective. *Computers & Security*, *59*, 138-150.

Tyler, T. R. (1990). *Why People Obey the Law*. Yale University Press.

Tyler, T. R. (1997). The Psychology of Legitimacy: A Relational Perspective on Voluntary Deference to Authorities. *Personality and social psychology review*, *1*(4), 323-345.

Tyler, T. R. (2006a). Psychological Perspectives on Legitimacy and Legitimation. *Annual review of psychology*, *57*, 375-400.

Tyler, T. R. (2006b). *Why People Obey the Law*. Princeton University Press.

Tyler, T. R., & Blader, S. L. (2005). Can Businesses Effectively Regulate Employee Conduct? The Antecedents of Rule Following in Work Settings. *Academy of Management Journal*, *48*(6), 1143-1158.

Wall, J. D., & Buche, M. W. (2017). To Fear or Not to Fear? A Critical Review and Analysis of Fear Appeals in the Information Security Context. *Communications of the Association for Information Systems*, *41*, 13.

Wall, J. D., & Warkentin, M. (2019). Perceived Argument Quality's Effect on Threat and Coping Appraisals in Fear Appeals: An Experiment and Exploration of Realism Check Heuristics. *Information & Management*.

Warkentin, M., Johnston, A. C., Walden, E., & Straub, D. W. (2016). Neural correlates of protection motivation for secure IT behaviors: An fMRI examination. *Journal of the Association for Information Systems*, *17*(3), 194.

Warkentin, M., Malimage, N., & Malimage, K. (2012). Impact of Protection Motivation and Deterrence on IS Security Policy Compliance: A Multi-Cultural View. Proceedings of the Pre-ICIS Workshop on Information Security and Privacy, Orlando, Paper,

Weatherford, M. S. (1992). Measuring Political Legitimacy. *American political science review*, *86*(1), 149-166.

Whetten, D. A. (2009). An examination of the interface between context and theory applied to the study of Chinese organizations. *Management and organization review*, *5*(1), 29-56.

Woon, I., Tan, G.-W., & Low, R. (2005). A Protection Motivation Theory Approach to Home Wireless Security. *ICIS 2005 proceedings*, 31.