A Composite Framework for Behavioral Compliance with Information Security Policies

Salvatore Aurigemma
University of Hawaii at Manoa
sa8@hawaii.edu

Raymond Panko
University of Hawaii at Manoa
panko@hawaii.edu

Abstract
To combat potential security threats, organizations rely upon information security policies to guide employee actions. Unfortunately, employee violations of such policies are common and costly enough that users are often considered the weakest link in information security. This paper presents a composite theoretical framework for understanding employee behavioral compliance with organizational information security policies. Building off of the theory of planned benefits, a composite model is presented that incorporates the strengths of previous studies while minimizing theoretical gaps present in other behavioral compliance models. In building the framework, related operational constructs are examined and normalized to allow better comparison of past studies and help focus future research efforts.

1. Introduction
There are numerous threats (viruses, malware, corporate espionage, etc) to the confidentiality, integrity, and availability of organizational information and information systems. While there are many security mechanisms designed to mitigate the information security risks from relevant threats, it is often incumbent upon users to utilize the technologies for them to be effective; information security depends on the effective behavior of humans [39] [42] [43] [44] [52] [55].

To assist users in ensuring information security during the use of information technologies and resources, organizations provide employees information security policies (ISPs) [30] [54]. An ISP describes employee roles and responsibilities, addressing specific security issues, in protecting the information resources of their organization [11].

Unfortunately, employees seldom comply with the guidance provided in their ISPs [44], resulting in billions of dollars annually in losses to their organizations [12]. It is for this reason that employees are often considered the weakest link in information security [26] [53] [59].

Given the importance of the employee in information security, it is essential to identify and better understand the determinants of security behavior. Behavioral compliance research findings can help focus organizational efforts toward improving employee compliance with ISPs. The challenge for organizations is to know how to transform users from the biggest information security vulnerability to the first line of ISP compliance defense [28].

Anderson and Argwal [6] present an excellent summary of behavioral information security literature over the past 20 years. Significant effort has been expended, especially in the past five years, towards obtaining a better understanding of the antecedents of employee behavioral compliance. A review of the literature shows some commonalities in the supporting theories used in related research. However, the varied conceptual implementations of these theories have resulted in a confusing array of behavioral compliance models and operational constructs that make comparison of results challenging.

This paper specifically examines empirically evaluated ISP behavioral compliance models and presents a composite framework with normalized first and second order operational constructs.

2. Theoretical foundation – theory of planned benefits
The theory of planned benefits (TPB) extends the theory of reasoned action [5] [16] and is considered one of the most influential frameworks for the study of human action [2] [59]. According to the TPB, human behavioral intention to perform an action is guided by subjective norms, attitude towards the behavior, and perceived behavioral control [1] [3]. Subjective norms are beliefs about the normative expectations of other people that result in perceived social pressure [3]. An employee’s attitude towards a behavior is determined by their belief that performing (or not performing) the behavior will lead to certain consequences [11]. Perceived behavioral control refers to people's perceptions about the presence of factors that may
facilitate or impede the performance of a behavior [3] [23].

Given some actual control over the behavior in question, people are expected to follow their intentions when confronted with an appropriate impetus. Thus, behavioral intention is assumed to be the immediate antecedent of actual behavior [3].

In the context of ISP behavioral compliance, the TPB model states that the more favorable an employee’s attitude and normative beliefs towards following ISP-related actions, and the greater the feeling of behavioral control over those actions, the stronger the intention to comply with the ISP [59]. Figure 1 depicts the generic TPB model.

![Figure 1. Theory of planned benefits model.](image)

The use of the TPB in ISP behavioral compliance literature is well established. As shown in table 1, The TPB is used explicitly in four of the eight studies that inform the framework presented in this paper. In the remaining four studies, core constructs of the TPB are employed, allowing comparison with TPB-based studies. For example, in Johnston and Warkentin [21], the primary theory used to derive their model is protection motivation theory (PMT), with a focus on attitude’s impact on behavioral intent. However, Johnston and Warkentin also add the normative beliefs and self-efficacy constructs to their model, effectively emulating the TPB model shown in figure 1. The studies evaluated in this paper were chosen by conducting a comprehensive literature review for empirical studies resulting in theoretical models describing ISP behavioral compliance in organizations.

The TPB has been used successfully in other information security contexts, such as insider security contravention [55] and computer abuse [23]. Lee and Lee [23], using the TPB model, posited criminology-based theories to better illuminate the constructs of normative beliefs, attitude and perceived behavioral control. Lee and Lee’s [23] focus on purposeful computer abuse is different than the focus of this paper (understanding general ISP behavioral compliance), but the approach they take in expanding the knowledge of individual TPB constructs with promising theories is consistent with ISP-related literature.

### Table 1. Empirical organizational ISP behavioral compliance studies.

<table>
<thead>
<tr>
<th>Authors</th>
<th>Theories applied</th>
<th>Normalized related constructs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bulgurcu et al (2010)</td>
<td>TPB &amp; RCT</td>
<td>BINT, NORM, SEFF, ATT, ORSEC, CBA, CASS, BOUT</td>
</tr>
<tr>
<td>Johnston &amp; Warkentin (10)</td>
<td>PMT</td>
<td>BINT, NORM, SEFF, PVUL, TSEV, REFF</td>
</tr>
<tr>
<td>Herath &amp; Rao (09)</td>
<td>Decomposed TPB, PMT, GDT</td>
<td>BINT, NORM, SEFF, REFF, SANCT, SSEV, SPROB, PVUL, TSEV, ORSEC</td>
</tr>
<tr>
<td>Ng et al (09)</td>
<td>PMT</td>
<td>BINT, SEFF, REFF, PVUL, TSEV</td>
</tr>
<tr>
<td>Zhang et al (09)</td>
<td>TPB</td>
<td>BINT, NORM, PBC, ATT, REFF</td>
</tr>
<tr>
<td>D’Arcy et al (09)</td>
<td>GDT</td>
<td>BINT, SANCT, SSEV, SPROB</td>
</tr>
<tr>
<td>Workman et al (08)</td>
<td>PMT, SCT</td>
<td>BINT, SEFF, CONT, PVUL, TSEV, REFF, CBA</td>
</tr>
<tr>
<td>Pahnila et al (07)</td>
<td>TRA, GDT, PMT, SCT</td>
<td>BINT, NORM, SEFF, CONT, ATT, SANCT, PVUL, TSEV</td>
</tr>
</tbody>
</table>


Construct legend: BINT = Behavioral Intent; NORM = Subjective Norms; SEFF = Self-efficacy; CONT = Perceived Controllability; ATT = Attitude; ORSEC = Organizational Security Commitment; CBA = Cost Benefit Analysis; PVUL = Perceived Vulnerability; PSEV = Perceived Severity; TSEV = Threat Severity; REFF = Response Efficacy; SANCT = Sanction Effects; PBC = Perceived Behavioral Control; SSEV = Sanction Severity; SPROB = Probability of Sanction Imposition; CASS = Consequence Assessment; BOUT = Belief Outcomes.

### 3. Composite framework

There is a growing base of quality ISP behavioral compliance research being published. However, without a common theoretical framework and use of consistently operationalized constructs, comparison of past studies is hindered and focus for future research is obscured. By evaluating the theoretical foundations of a number of recent studies in the field, a common core of constructs (described below) has emerged and is summarized in table 2. The selection criteria for which constructs and theoretical extensions were used in the framework is as follows. First, only empirical studies that were published in high-quality, peer-reviewed journals and conferences were used to develop the composite framework. Five of the eight studies used (shown in table 1) were published in MIS Quarterly [11] [21], Information Systems Research [14], Decision Support Systems [28], and the European
Journal of Information Systems [20]. The remaining three studies are topically relevant and cited extensively in the aforementioned research. Additionally, only those constructs that were empirically evaluated in at least a third of the foundational papers, and found to be significant in a majority of those, were included in the final model. Table 1 provides a synopsis of each study used to inform the composite framework; the table includes the theories applied in the base studies and normalized constructs used (described in greater detail in table 2). In using the TPB as the core theoretical lens for modeling behavioral intention, a composite framework for ISP behavioral compliance is possible and shown in figure 2.

The composite framework for ISP behavioral compliance states that employee behavioral intention to follow security guidelines is impacted by subjective norms, their attitudes toward compliance, perceived behavioral control over the behavior, and the strength of their involvement and identification with their organization’s commitment to information security. Employee attitude, a powerful predictor of behavioral intent, is influenced by three core variables. First, attitude can be guided by the perceived impacts (based upon sanction severity and certainty of punishment imposition) of threatened penalties for disobeying the ISP. Second, attitude can be shaped by the perception of the overall danger a security threat poses based upon the magnitude of the threat, susceptibility to the threat, and effectiveness of available security countermeasures. Finally, attitude can be impacted by the affective and cognitive assessment of a particular security behavior in terms of a cost-benefit analysis. The cost-benefit analysis is driven by the employee’s beliefs about the overall assessment of consequences (perceived benefit of compliance and perceived costs of compliance and non-compliance), which is shaped by various intrinsic and extrinsic belief motivators. A detailed description of the components of the composite framework follows.

3.1 Subjective norms

Employees’ perceived social pressure to follow ISPs reflects their beliefs about how important referents (peers, supervisors, subordinates) would like them to perform their security-related responsibilities [3] [59]. If an employee believes that relevant others expect ISP compliance from them, they are more likely to undertake appropriate security actions [20]. Subjective norms is used in five of eight (62%) of the supporting models of the composite framework.
Other names used for subjective norms includes normative beliefs [11] [29] and social influence [21]. While the extent information technology and security literature has used a variety of labels for the construct, each of the above contain the notion that an employee’s behavioral intent is influenced by what relevant others expect to be done [20]. For sake of consistency with the TPB, the term subjective norms is used for the remainder of this paper.

While the subjective norms construct is well represented in the ISP-compliance literature, there is at least one instance in which its explanatory power was not significant, in discordance with the TPB. In Zhang et al’s [59] study of the impact of perceived technical protection on security behaviors, the authors found no significant relationship between subjective norms and behavioral intent. An examination of the sample data by the authors provided a possible explanation for the incongruity with the TPB. Zhang et al [59] noted that the majority of their respondents were employees with at least six years of experience at their organizations. This experience may indicate the presence of habits to comply or not comply with ISPs. As noted in other information system studies [51], the effect of subjective norms can erode with increasing experience.

There is extensive literature on the impact of habit on the TPB, including some that provide evidence of habits significantly adding to the prediction of intention over and above the effect of attitude and subjective norm and to the prediction of behavior from intention alone [10] [38]. It has been posited that in the TPB model, habit may be best considered as a control variable [32]. In the ISP-compliance literature, the only study that specifically addressed the impact of habits on behavioral intentions was Pahnila et al [29]. Based upon the findings of Limayem and Hirt [24], Pahnila et al [29] posited that habits (defined as unconscious or automatic behaviors) can trump subjective norms over time, directly influencing actual behavior and reducing the impact of behavioral intentions to comply with ISPs. Both habits and subjective norms were found to have a positive significant relationship with behavioral intent in the Pahnila et al [29] study. Although habit may explain more variance when applied to the TPB model, it does not aid understanding of what underlies peoples behavior [25], thus it is included in the composite ISP compliance model as a possible control variable of subjective norms.

3.2 Perceived behavioral control

The concept of perceived behavioral control (PBC) was introduced to the TPB to address non-volitional aspects potentially inherent in all behaviors [3]. Seven (88%) of the evaluated ISP compliance models include PBC in some form (as described below). Prior to PBC, similar ideas appeared in the health belief model [22], and Triandis’ model of interpersonal behavior [50]. According to Ajzen [3], the PBC construct owes its greatest debt to Bandura’s work on self-efficacy.

A central tenet of social cognitive theory [8], perceived self-efficacy was introduced to deal with coping behavior in the context of behavior modification [7]. Perceived self-efficacy refers to peoples beliefs about their own capabilities to carry out a task [8]. The concepts of PBC and self-efficacy are quite similar as both are concerned with a person’s perceived ability to perform a behavior [3]. In the context of ISP behavior compliance, self-efficacy refers to an employee’s self confidence in their skills or ability to comply with the actions called for in the ISP [28]. People with a high level of self-efficacy have a stronger form of self conviction about their ability to mobilize motivation and cognitive resources needed to successfully execute the guidance of the ISP [33].

A second component of PBC is known as perceived controllability, a very similar concept to Rotter’s [36] locus of control with some nuanced differences. Perceived controllability considers the extent of which an employee’s behavior is considered proactive or reactive [3]. Locus of control is defined in a similar fashion, but is further described as having internal and external components [57]. Internal locus of control is a belief that people control their own actions while external locus of control refers to the belief that forces (other people, fate, environmental factors, etc) determine outcomes [36]. Perceived controllability does not draw as clear a distinction between internal and external components; perceived control over an outcome is independent of the internal or external locus of factors responsible for it [3]. Thus, while perceived controllability is focused on a person’s belief of whether an event is controllable, self-efficacy focuses on a person’s beliefs of their capabilities (skills and abilities) in performing a particular behavior.

Of the ISP behavioral compliance models examined in this study, six ([11] [20] [21] [28] [29] [57]) use self-efficacy instead of PBC. For example, Bulgurcu et al [11] use self-efficacy as they state it measures the same latent construct as PBC [15] and is consistent with recent behavioral literature [17] [18] [19] [58]. Ajzen [3] acknowledges that in some cases, only one of the components (self-efficacy or perceived controllability) may be sufficient to calculate the effect of PBC. Only Zhang et al [59] explicitly uses the PBC construct, with both of its component variables. As discussed above, Workman et al [57] use both self-efficacy and locus of control constructs. Pahnila et al [29] uses both self-efficacy and facilitating conditions.
Table 2. ISP behavioral compliance constructs

<table>
<thead>
<tr>
<th>Construct</th>
<th>Definition</th>
<th>Other names</th>
<th>Used in</th>
<th>Supporting theories</th>
</tr>
</thead>
<tbody>
<tr>
<td>Behavioral intent (BINT)</td>
<td>An individual’s intention to perform a particular ISP-related behavior</td>
<td></td>
<td>[11],[14],[20],[21],[28],[29],[57],[59]</td>
<td>Theory of planned benefits (TPB)</td>
</tr>
<tr>
<td>Subjective norms (NORM)</td>
<td>An individual’s beliefs about the normative expectations of other people that result in perceived social pressure to comply with accepted security behaviors</td>
<td>Social pressures[20]</td>
<td>[11],[20],[21],[28],[29]</td>
<td>TBP</td>
</tr>
<tr>
<td>Habit</td>
<td>Unconscious or automatic behaviors</td>
<td></td>
<td>[29],[59]</td>
<td>TBP, Social Cognitive Theory (SCT)</td>
</tr>
<tr>
<td>Perceived behavioral controls (PBC)</td>
<td>Refers to people’s perceptions about the presence of factors that may facilitate or impede the performance of an ISP-related behavior</td>
<td></td>
<td>[11],[21],[28],[29],[57],[59]</td>
<td></td>
</tr>
<tr>
<td>Self-efficacy (SEFF)</td>
<td>Refers to peoples beliefs about their own capabilities to carry out information security tasks</td>
<td></td>
<td>[11],[21],[28],[29],[57]</td>
<td></td>
</tr>
<tr>
<td>Perceived controllability (CONT)</td>
<td>Considers the extent of which an employee's ISP-related behavior is considered proactive or reactive</td>
<td>Locus of control[57]</td>
<td>[11],[21],[28],[29],[57]</td>
<td></td>
</tr>
<tr>
<td>Attitude toward compliance (ATT)</td>
<td>Belief that performing (or not performing) a particular security behavior will lead to certain consequences</td>
<td></td>
<td>[11],[21],[28],[29],[57]</td>
<td></td>
</tr>
<tr>
<td>Sanction effects (SANCT)</td>
<td>Perceived impact of threatened penalties for disobeying the ISP</td>
<td></td>
<td>[11],[14],[20],[29]</td>
<td>General deterrence theory (GDF)</td>
</tr>
<tr>
<td>Perceived sanction severity (SSSEV)</td>
<td>Perceived harshness of the penalty associated with a specific ISP disobedience</td>
<td></td>
<td>[11],[14],[20]</td>
<td></td>
</tr>
<tr>
<td>Perceived probability of sanction imposition (SPIRB)</td>
<td>Perceived probability that an ISP disobedience will be punished if detected</td>
<td></td>
<td>[11],[14],[20]</td>
<td></td>
</tr>
<tr>
<td>Threat assessment (THREAT)</td>
<td>Perception of the overall danger of a security threat based upon the magnitude of the threat, susceptibility to the threat, and effectiveness of available countermeasures</td>
<td>Security breach concern[20]</td>
<td>[20],[29],[57]</td>
<td>Protection motivation theory (PMT)</td>
</tr>
<tr>
<td>Perceived vulnerability (PVUL)</td>
<td>Relates to how likely an employee feels that they will encounter a particular security threat</td>
<td>Threat appraisal[20]</td>
<td>[20],[29],[57]</td>
<td></td>
</tr>
<tr>
<td>Perceived threat severity (TSEV)</td>
<td>Perceived potential damage posed by a security threat</td>
<td>Perceived susceptibility[21],[28]</td>
<td>[20],[21],[28],[57]</td>
<td></td>
</tr>
<tr>
<td>Response efficacy (REFP)</td>
<td>Refers to an employee’s perceived effectiveness of a particular recommended security threat response from the ISP</td>
<td>Perceived effectiveness[20]</td>
<td>[20],[21],[28],[57]</td>
<td></td>
</tr>
<tr>
<td>Cost-benefit analysis (CBA)</td>
<td>The affective and cognitive assessment of a behavior acquired through personal experience</td>
<td>Perceived security protection[59]</td>
<td>[20],[21],[28],[57]</td>
<td></td>
</tr>
<tr>
<td>Consequence assessment (CASS)</td>
<td>An individual’s beliefs about the overall assessment of consequences from taking an ISP-related security action</td>
<td></td>
<td>[11],[20],[59]</td>
<td>Rational choice theory (RCT)</td>
</tr>
<tr>
<td>Perceived benefit of compliance (PBIEN)</td>
<td>The overall expected favorable consequences to an employee for complying with the ISP</td>
<td></td>
<td>[11]</td>
<td></td>
</tr>
<tr>
<td>Perceived cost of compliance (PCOMP)</td>
<td>The overall expected unfavorable consequences to an employee for complying with the ISP</td>
<td></td>
<td>[11]</td>
<td></td>
</tr>
<tr>
<td>Perceived cost of non-compliance (PNCOMP)</td>
<td>The overall expected unfavorable consequences to an employee for non-compliance with the ISP</td>
<td></td>
<td>[11]</td>
<td></td>
</tr>
<tr>
<td>Beliefs about outcomes (BOOUT)</td>
<td>Describes an employee’s intrinsic and extrinsic motivations that form their beliefs about overall assessment of consequences</td>
<td></td>
<td>[11]</td>
<td></td>
</tr>
<tr>
<td>Organizational Security Commitment (ORSEC)</td>
<td>Overall strength of an individual’s involvement and identification with their organization’s commitment to information security</td>
<td>Awareness of security countermeasures[14]</td>
<td>[11],[14],[20]</td>
<td></td>
</tr>
<tr>
<td>Perceived security protection (PCOMP)</td>
<td>The overall expected unfavorable consequences to an employee for complying with the ISP</td>
<td></td>
<td>[11],[14],[20]</td>
<td></td>
</tr>
<tr>
<td>Perceived cost of non-compliance (PNCOMP)</td>
<td>The overall expected unfavorable consequences to an employee for non-compliance with the ISP</td>
<td></td>
<td>[11],[14],[20]</td>
<td></td>
</tr>
</tbody>
</table>

a very similar construct to locus of control and perceived controllability originating with Triandis [50]. Finally, only the D’Arcy et al [14] study ignores the concept of PBC altogether.

Of the seven ISP behavioral compliance models evaluated that used PBC/self-efficacy, only Pahnila et al [29] found self-efficacy to be an insignificant contributor to behavioral intent. However, in the Pahnila et al [29] study, self-efficacy was measured as one of three components of a higher-order construct called coping appraisal. A closer examination of how coping appraisal was measured would need to be conducted to determine if self-efficacy alone would have had a significant effect on behavioral intent in their study.

Due to the similarity in construct definitions and measurement items described in Ajzen [3] and Workman et al [57], and in keeping with the basic framework of the TPB, the composite ISP behavioral compliance model presented in this paper uses the construct PBC with supporting variables of self-efficacy and perceived controllability. Additionally, discussion of comparisons between the health belief model (a precursor theory to PMT) and the TPB in
section 3.3.2 below support the use of the TPB PBC constructs in the composite model.

3.3 Attitude toward compliance

The third main construct that guides an employee’s behavioral intent to comply with ISPs is their attitude toward compliance. In the context of this paper, satisfying of the attitude element means that the consequences of executing the ISP are believed to be desirable [41]. All eight (100%) of the contributing models to the framework address attitude.

Numerous TPB-related studies ([9] [25] [27] [37]) have shown that attitude can be the strongest predictor of behavioral intent, which makes research in this component of the TPB extremely valuable. In fact, the majority of literature in the information systems field on behavioral intent has focused most on investigating attitude and its antecedents [11]. The ISP behavioral compliance literature presented in this paper has focused on three main themes in decomposing the attitudinal construct: sanction effects, threat assessment, and cost-benefit analysis.

3.3.1 Sanction effects

Sanction effects are based upon general deterrence theory (GDT), which can be traced back to Bentham (1748-1832) and Beccaria (1738-1794) [40]. The main hypothesis of the GDT is that people weigh costs and benefits when deciding whether to commit a crime (or in the context of this study, intend to violate some portion of the ISP). Specifically, the GDT focuses on sanctions against committing an unwanted act and their effectiveness as a deterrent [48]. The effectiveness of sanctions is based upon the perceived severity of the sanction and the perceived probability of sanction imposition [47]. The GDT is well established in the information security field ([45] [46] [47]) and represented in three of the ISP compliance models reviewed in this paper ([14] [20] [29]).

The rationale for applying sanction effects to the attitudinal component of the TPB is that security mechanisms can be deployed by organizations to increase the perceptions of certainty and severity of punishment for ISP violations, thereby strengthening the behavioral intent to comply. Despite the theoretical base provided by the GDT, deterrence-based research in information security has been inconclusive [14]. Research on computer abuse behavior has focused on sanction effect mechanisms (policy, systems, awareness programs) meant to increase the perceived cost of abusive behaviors [23]. However, these mechanisms appear mostly ineffective even though they are deployed in over 80 percent of U.S. organizations [23].

Of the four ISP behavioral compliance models examined in this paper, three ([11] [14] [20]) found sanction effects to be a significant contributor to behavioral intent while the other [29] did not. Sanction effects is incorporated into the composite model of ISP behavioral compliance as it addresses a potentially important component of a person’s attitude that is not addressed in other supporting constructs.

3.3.2 Threat Assessment

The protection motivation theory [34] [35] is an extension of the health belief model [22] and elucidates the processes involved in coping with a threat [21]. The PMT consists of two main processes: threat assessment and coping appraisal. The appraisal of the threat and coping responses result in the intention to perform (or not perform) a particular action associated with a fear appeal related to that action. Coping appraisal is comprised of locus of control and self-efficacy [57], described earlier, and is normalized in this study under the label of perceived behavioral control.

Threat assessments, according to the PMT, are comprised of three variables: perceived severity, perceived vulnerability, and perceived response efficacy. The perception of threat is defined as the anticipation of a violation (physical, psychological, or social) to oneself or others [57]. When a threat is perceived, behavior is adjusted to account for an acceptable amount of risk. Perceived severity of a threat will lead a person to behave more cautiously if their perception of the damage from the threat is greater. Thus, if a person feels that a specific security threat, such as the threat of spreading viruses from opening email attachments, is very high, they will tend to limit or eliminate that practice.

Perceived vulnerability, also called perceived susceptibility [21] [28], relates to how likely an employee feels that they will encounter a particular threat [21] [57]. However, individuals vary widely in their perceptions of vulnerability. Given the same information about the probability of an information security threat, one person may feel the likelihood of occurrence is very small and thus they are less vulnerable, while another feels quite opposite [28]. Workman et al [57] refers to some people’s “illusion of invulnerability” that allows them to ignore threats existing in the world so that they may continue to view the world as safe and orderly. Bad things happen to other people, not oneself. In the ISP compliance context, employees that operate with a sense of invulnerability are less likely to comply with the
actions directed in the ISP. However, when an employee is given a reason to believe they are vulnerable to a specific threat, they will be more likely to comply with the ISP.

People often hold different views about the effectiveness of a directed behavior in the face of a threat [57]. A person’s beliefs about the availability and effectiveness of a threat mitigation action determines their behavior, not the objective facts about the recommended response [28]. Response efficacy refers to an employee’s perceived effectiveness of a recommended threat response [34]. According to PMT, moderate to high levels of response efficacy are associated with positive beliefs about the threat mitigation of a particular recommended response [21]. The term perceived benefits [28] is also used in the ISP compliance literature but is defined synonymously with response efficacy. One significant difference between the PMT and TPB view of response efficacy is PMT’s conceptualization of the construct as a coping appraisal mechanism along with self-efficacy [57]. In keeping with the TPB model, the composite framework presented in this paper presents response efficacy as a component of attitudinal threat assessment in that it is specifically concerned with an individual’s belief about the effectiveness of a particular action against a threat of some perceived severity and susceptibility.

As mentioned earlier, the PMT is an extension of the health belief model (HBM). The HBM suggests that an individual’s behavior is determined by a threat assessment and beliefs about the efficacy of the behavior to resolve the threat [28]. As the TPB extended the theory of reasoned action by including the perceived behavioral control construct, PMT extended the HBM by including self-efficacy and locus of control (see section 4 discussion above). Numerous empirical studies have been conducted comparing the HBM and the TPB ([9] [27] [37]), all of which conclude that the TPB is a better measure of behavioral intent and also reaffirm the importance of the attitudinal component of the TPB. The main contribution of the PMT to the composite model of ISP behavioral compliance is the addition of the threat assessment construct and associated variables.

### 3.3.3 Cost-benefit analysis

The TPB posits that behavior-related consequences manifest in one’s attitude toward behavioral intent [2]. In the context of obedience to ISPs, an employee’s attitude is formed when the compliance-related consequences that will be personally experienced if they comply or do not comply are considered [11]. Thus, when an employee considers executing a behavior, they conduct a cost-benefit analysis. An employee’s **cost-benefit analysis** can be described as the affective and cognitive assessment of a behavior acquired through personal experience; the overall assessment may be either favorable or unfavorable [3]. Three ISP compliance studies ([11] [20] [57]) have explored to some extent the cost-benefit analysis component of the attitude construct; all found cost-benefit analysis to be a significant contributor to attitude. Herath and Rao’s [20] evaluation of cost-benefit analysis is cursory. They use a variable, response cost, to estimate an employee’s beliefs about how costly performing an ISP-related action will be.

Workman et al [57] proffer that an employee’s intention to follow ISP-directed behaviors may be influenced by whether they perceive that the effort required to protect an information resource is worth the cost of the protection effort. It is noted, however, that cost-benefit attitudes vary among individuals when comparing such things as business value or threat severity to their own self-interests [57]. Thus, if an ISP action is considered to address an extremely important resource, but it is very difficult or exceedingly time consuming to conduct, an employee may perceive the cost as outweighing the benefit [49]. Conversely, if an ISP action provides only a minimal benefit, but the associated effort is also minimal, it may be adopted [31]. Workman et al [57] measure cost-benefit analysis by assessing the inconvenience, cost, and impact to an employee’s work from implementing the ISP.

Bulgurcu et al [11] took a more robust approach to exploring the antecedents of an employee’s cost-benefit analysis through the application of rational choice theory (RCT). The RCT, with roots in economic theory, argues that behavior is determined by balancing the costs and benefits of different options. Determinants of an employee’s attitude originate in their beliefs about complying (or not complying) with the ISP and the consequences of their actions [11]. Their cost-benefit analysis methodology posits two main constructs: beliefs about overall assessment of consequences and beliefs about outcomes.

**Beliefs about overall assessment of consequences** has three distinct beliefs: perceived benefit of compliance, perceived cost of compliance, and perceived cost of non-compliance [11]. **Perceived benefit of compliance** is the overall expected favorable consequences to an employee for complying with the ISP. **Perceived cost of compliance** is the overall expected unfavorable consequences for complying with the ISP. **Perceived cost of non-compliance** is the overall expected unfavorable consequences for non-compliance.

Bulgurcu et al [11] further go on to define their second component of cost-benefit analysis, beliefs
about outcomes. **Beliefs about outcomes** describes how an employee forms their beliefs about overall assessment of consequences. Addressing both intrinsic and extrinsic motivations, Bulgurcu et al [11] posit seven outcome beliefs that provide for the foundation for beliefs about consequences. The authors readily admit that they did not address all of the factors and outcome beliefs possible, such as those factors included in the sanction effects and threat assessment constructs. For sake of parsimony, only the distinct beliefs about the overall assessment of consequences construct is included in the composite ISP behavioral compliance framework.

### 3.4 Organizational security commitment

Beyond the three main TPB constructs of subjective norms, PBC, and attitude, recent ISP compliance research identified another possible antecedent to behavioral intent – **organizational security commitment** [11] [14] [20]. This construct is used in three (38%) of the supporting models used in developing the framework and was found to be a significant contributor to behavioral intent in all of these studies. Herath and Rao [20] introduced the concept of organizational security commitment to the context of ISP compliance research. Organizational security commitment is defined as the overall strength of an individual’s involvement and identification with their organization and captures the perceived relationship between the organization and the employee [56]. In the information security context, employees are less likely to enact poor security behaviors and put their organization at risk if their organizational security commitment is high [20].

D’arcy et al [14] decompose a similar concept that addresses user awareness of organizational security countermeasures. Their definition of security countermeasures consists of an organization’s ISP, security monitoring technologies, and security education, training, and awareness (SETA) programs. By implementing (or not implementing) such countermeasures, an organization helps define its commitment to security, but it is the employee’s awareness and identification with such commitments that proffer to impact behavioral intent.

Bulgurcu et al [14] developed a comparable variable, called information security awareness, which has a direct effect on both behavioral intent and an indirect effect via an employee’s cost-benefit analysis. Information security awareness is defined as an employee’s general knowledge about information security and specific knowledge of the ISP of their organization [11].

Including other variables, such as organizational security commitment, with the TPB is considered an acceptable practice. While the TPB’s behavioral intent has been consistently measured based upon subjective norms, attitude, and PBC, any number of factors may directly or indirectly influence behavioral intentions based upon the context applied to the behavior of interest [4] [13] [15]. The inclusion of organizational security commitment to the composite ISP compliance model makes logical sense and is empirically validated ([11] [14] [20]).

### 4. Framework value

The value of the composite framework for behavioral compliance with information security policies is twofold. First, the framework synthesizes the results of related recent research to produce a more complete, yet still parsimonious, model based largely upon the theory of planned benefits. The framework adds a core theoretical extension of organizational security commitment and decomposes the attitudinal component of the TPB, in the context of ISP compliance. Such a composite framework is useful in examining which specific aspects of ISP compliance have been evaluated in past studies and which areas need to be addressed in future research. And, by having a more complete model, practitioners can better focus their security education and training efforts and technology to maximize ISP compliance.

Second, the normalized constructs supporting the framework allow researchers to explore commonalities, as well as disjoints, in previous empirical research on this topic. For research that supports specific components of the model, consensus grows and allows focus to shift to other areas where there is insufficient empirical research or, perhaps, conflicting results. For example, future studies that wish to explore sanction effects on ISP compliance are better able to use common construct definitions and instruments defined in related studies. Likewise, the results of future studies can be more readily compared to past ISP compliance study results for component and overall model goodness of fit.

### 4.1 Weaknesses

The composite framework, as well as the eight supporting ISP compliance models, primarily focuses on the antecedents of behavioral intent to comply, not actual compliance. It is often difficult to gain access to measure organizational ISP compliance, hence the reliance upon theories, such as the TPB, to bridge the gap between intent and actual behavior. There is a
paucity of ISP research that actively explores this gap. Only one of the eight studies contributing to this framework attempted as such. In the Workman et al [57] study, the authors measured actual behavioral compliance by observing three components of the subject organization’s ISP and found their ISP compliance model supported both behavioral intent and actual behavior; this result supports not only the core TPB, but also the components of the composite framework present in the Workman et al [57] model. However, one study in a single organization is insufficient to properly validate the composite framework’s predictability of actual behavior in the ISP context.

Additionally, a detailed examination of the models presented in the studies of table 1 show that, while there are significant commonalities on construct definition and measurement, there are many model implementation discrepancies that need to be addressed in the evolution of the composite framework. For example, regarding the studies that evaluated organizational security commitment, all found that the variable directly impacted behavioral intention, but also had indirect effects from different attitudinal components (cost-benefit analysis [11], response efficacy [20], and sanction effects [14]). The composite framework in this paper does not address such issues.

5. Future Research

Although there have been a number of high-quality, robust empirical studies of ISP behavioral compliance in recent years, much work is left to be done to expand the understanding of the core constructs in the framework. As addressed above, a significant focus of future research should be on addressing the empirical gap between measured behavioral intent and actual behavior in a variety of workplace contexts and ISP threat vectors.

Additionally, there is an opportunity to evaluate and expand the cost-benefit analysis component of attitude. As noted in their study, Bulgurcu et al [11] did not examine the component of the composite framework identified as threat assessment and their treatment of sanction effects was very limited. There is great potential in expanding the cost-benefit analysis variable by incorporating both threat assessment and sanction effects, thereby providing a more parsimonious composite ISP behavioral compliance model with greater explanatory value.

6. References


