Proceedings of the 52nd Hawaii International Conference on System Sciences | 2019

The Compromise of One's Personal Information: Trait Affect as an Antecedent in Explaining the Behavior of Individuals

Marc J. Dupuis
University of Washington
marcjd@uw.edu

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

Abstract

This research examined the role trait affect, a lifelong and generally stable type of affect, has on the information security behavior of individuals. We examined this in the context of how one responds to the threat of one's personal information becoming compromised. This was done by extending Protection Motivation Theory (PMT) by incorporating the two higher order dimensions of affect, positive affect and negative affect, as antecedents to self-efficacy, perceived threat severity, and perceived threat vulnerability. A survey was used to explore this further. Seven of the 11 hypotheses were supported, including three of the six related to affect. This research makes two primary contributions. First, trait affect may play an indirect role in understanding how individuals evaluate, respond to, and cope with a threat. Second, this research extended the application of PMT, which has been the primary theory used to understand the information security behavior of individuals.

1. Introduction

Computers provide people with a wide range of benefits, such as connecting with friends, shopping for items, and sending emails. In addition to the many benefits computers provide to people, there are inherent risks. These risks exist in many different forms; the compromise of one's personal information arguably being the most significant, which can occur through something as simple as a post on a social networking site [1]. This is particularly important given the general lack of knowledge individual users have with respect to technical and non-technical controls related to privacy and security [2].

In an organizational setting, compliance with security policies is mandatory. Organizations have paid a considerable amount of time, money, and attention to information security with positive outcomes. This includes investment in security education, training, and awareness (SETA) programs [3]. However, individual users are not a homogeneous group and most do not have any organized means of participating in a SETA program. Policies do not exist for individual users, nor are they required to engage in safe security behavior.

Several factors have already been empirically associated with the security behaviors of individual users, including perceived threat severity, perceived threat vulnerability, self-efficacy, response efficacy, response costs, locus of control, and social influences. However, there is one factor that has been included less in comparison in research on individual users' information security behaviors—affect. Fortunately, there has been greater recognition of the important role affect may play in information security research [4].

Research in the decision-making domain has shown that affect influences individuals' risk perceptions [5] and their self-efficacy [6]. Risk perceptions and self-efficacy have both been associated with individual users' information security behaviors, suggesting that affect may provide some additional and important insights in this area.

This research helps to close the gap in existing research by examining the role of trait affect on the information security behavior of individual users. While organizations may care little about the information security behavior of individual users outside the confines of the organization, all users within the organization are also individual users. Thus, their behavior, habits, and perceptions of information security risk, and their ability to counter significant threats should be of great interest to organizations. Likewise, by examining the behavior of individual users outside of the organization we were able to test our hypotheses 'policy free' and thus control for the influence and inconsistency of policies across organizations.

Overall, this research makes two primary contributions. First, trait affect may play an indirect role in understanding how individuals respond to and cope with a threat. Second, this research extended the application of Protection Motivation Theory, which has been the primary underlying theory used to understand the information security behavior of individual users.

URI: https://hdl.handle.net/10125/59922
ISBN: 978-0-9981331-2-6

2. Literature Review

2.1. Protection Motivation Theory

PMT was developed in 1975 by Rogers as an extension of expectancy-value theory to provide a more complete understanding of the effects of fear appeals on attitude change [7]. A fear appeal is a communication regarding a threat to an individual that provides information regarding one's well-being [8]. In PMT, two independent appraisal processes occur as a result of a fear appeal: threat appraisal and coping appraisal. Six components of a fear appeal have been articulated, three for each of the appraisal processes [8]. Threat appraisal consists of: 1) the severity of the perceived threat, based on prior research showing that the manipulation of fear will affect the perceived severity of the threat; 2) the vulnerability to the perceived threat, noted in prior research to increase as fear-appeals go from low-fear to high-fear; and 3) rewards, both intrinsic and extrinsic, such as personal satisfaction or fulfillment and social acceptance by peers.

In contrast to threat appraisal that is believed to inhibit maladaptive responses, coping appraisal is concerned with the factors that determine whether an individual will cope with and avert a specific threat [8]. Coping appraisal consists of: 1) the perceived effectiveness of a counter-response (perceived response efficacy), reported to increase compliance with recommendations as the perceived effectiveness of the recommendations increased [8]; 2) perceived response costs, considering the cost (time, effort, financial, etc.) of the adaptive response; and 3) belief that the individual can effectively perform the counter-response (self-efficacy), with prior research showing a positive correlation between self-efficacy expectancy and changes in behavior (assumed causal relationship) [8].

2.2. Trait Affect

Affect influences or alters how individuals perceive things. These altered perceptions have an effect on the decisions people make [5]. This may occur through affect's influence on how people perceive risk, as well as how people formulate their self-efficacy expectations related to a specific situation [9]. Earlier, we discussed the important role that constructs related to threat appraisal and coping appraisal have had in understanding the information security behavior of individual users. Understanding the antecedents of these constructs is an important step in developing a more complete understanding of the behavior of individual users with respect to information security.

Although research with affect has been conducted in IS research, there has been a significant lack of consistency in what is meant by affect and how it should be measured [10]. A few of the ways it has been conceptualized within this research includes microcomputer playfulness [11], perceived enjoyment [12], computer anxiety [13], etc.

There have been several different theoretical approaches used within IS research that have employed an affect type construct. For example, the Theory of Reasoned Action (TRA), the Theory of Planned Behavior (TPB), and the Technology Acceptance Model (TAM) all include a construct that assesses an individual's attitude towards a behavior [14]. Attitudes consist of the beliefs about a specific behavior and are weighted by evaluations of these beliefs. These attitudes may consist of some affective descriptors (e.g., happy), but generally speaking they are far removed from what would be typically termed affect.

While some research has examined the role of affect on behavior in the IS domain in general, less has focused on information security behavior in particular. An exception to this is a study that examined social networking sites and the role affect has on the implementation of security safeguards. Drawing on Social Capital Theory, Wu, Ryan, and Windsor [15] employed three social capital constructs – structural capital, relational capital, and cognitive capital – as antecedents of affect towards social networking sites. Affect in their study was operationalized in the same manner as by Compeau and Higgins [16] – as a positive attitude toward a technology. This study provides support for the underlying argument of the current study, namely, that affect may help to explain the information security behavior of individuals. Other exceptions focused on social networking [17] and computer abuse within an organization [18].

2.2.1. Affect, Mood, and Emotion. Affect has come to mean several different things in existing literature and has often been used interchangeably with mood and emotion [19]. While this is understandable in one respect since they are all interrelated concepts, it also poses significant difficulties for the study of affect as it makes it inherently difficult to compare studies, let alone validate existing ones.

For the purposes of this research, emotion can be characterized as a generally short-lived and intense reaction to an event or stimulus, whereas mood is longer-lasting and milder in degree [20]. Both of the terms represent a type of affect and can be classified as affective states [21]. Affective states include: fear, sadness, guilt, hostility, shyness, fatigue, surprise, joviality, self-assurance, attentiveness, and serenity [22]. However, they only represent a portion of the broader concept of affect. Mood and emotion fluctuate over time and vary in intensity. In contrast, trait affect changes little over one's life and is generally stable over time. In many respects, trait affect is similar to personality in this regard [23].

Exploring the role of trait affect on the risk perceptions of individuals in the information security domain has several advantages over that of state affect. First, it is a broader perspective that can help inform research on state affect. Second, trait affect is generally stable over time and context free [22]. Third, trait affect is not dependent on single affect-eliciting events (e.g., having ice cream may make someone happy in the moment). Thus, trait affect is a logical starting point for work examining the role of affect on the information security behavior of individual users.

The predominant approaches taken in conceptualizing affect have been valence-based. This includes affect as either positive or negative on a bipolar continuum [5], and positive affect and negative affect as two distinct dimensions [24]. The former approach has largely been replaced by the latter in recent years due to its higher degree of convergent and discriminant validity [25]. Positive affect is related to the frequency of pleasant events and satisfaction, whereas negative affect is related to stress and poor coping [24]. An individual with high positive affect does not necessarily have low negative affect and vice versa as they are largely independent dimensions. Thus, it is possible for an individual to have high positive affect and high negative affect, simultaneously.

2.3. Research Model

The research model that follows includes five constructs that act as determinants of the information security behavior of individual users. Two of these constructs account for an individual's risk perception—perceived threat severity and perceived threat vulnerability. The other three constructs account for coping appraisal in PMT—perceived response efficacy, perceived response costs, and self-efficacy.

While the model itself is based on PMT with the additional components of trait positive affect and trait negative affect, we did not measure behavioral intentions, which is a central component of PMT [7]. There are three primary reasons for this. First, the relationship between intention and behavior has generally been weaker than has often been assumed [26]. Second, the responses required to mitigate the threat of personal information compromise may have largely become habitual for most users, which has been problematic for the intention-behavior relationship [27]. Finally, we are concerned with the individual user's current behavior, not how it may change in response to an experimental manipulation.

2.4.1. Information Security Behavior. Self-efficacy has been shown to vary based on the task under investigation [28]. Self-efficacy needs to be context-specific [29]. In this research we examined the threat of one's personal information being compromised and the nine responses found to be required to effectively mitigate this threat [30]. The importance of privacy and preventing one's personal information from being compromised by malware and other sources has been examined in several studies on individual users in both a personal and professional context (e.g., [31]).

2.4.2. Determinants of Information Security Behavior. In PMT, threat appraisal occurs as a result of a fear appeal, which stems from environmental and intrapersonal information. Threat appraisal consists of perceived threat severity, perceived threat vulnerability, and rewards, both intrinsic and extrinsic [8]. Perceived threat severity is the level of noxiousness elicited from a fear appeal.

Threat appraisal is believed to inhibit maladaptive responses, such as avoiding the creation of strong passwords (i.e., avoidance) or convincing one's self that there is no risk associated with running a computer that does not have current anti-malware software installed (i.e., denial) [32, p. 83].

H1: Higher levels of perceived threat severity related to the compromise of one's personal information are associated with higher levels of performing the responses necessary to mitigate this threat.

H2: Higher levels of perceived threat vulnerability related to the compromise of one's personal information are associated with higher levels of performing the responses necessary to mitigate this theat.

Coping appraisal is believed to increase the likelihood of an individual engaging in an adaptive response (e.g., running back-ups of data) to mitigate a threat. It consists of perceived response efficacy, perceived response costs, and self-efficacy. Higher levels of perceived response efficacy and self-efficacy are believed to lead to greater levels of choosing an adaptive rather than a maladaptive response [8]. However, if the perceived costs associated with an adaptive response are high, then the individual is less likely to choose an adaptive response.

H3: Higher levels of perceived response efficacy related to the actions necessary to mitigate the threat of one's personal information being compromised are associated with higher levels of performing these responses.

H4: Higher levels of perceived costs related to the responses necessary to mitigate the threat of one's personal information being compromised are associated with lower levels of performing these responses.

H5: Higher levels of self-efficacy related to the responses necessary to mitigate the threat of personal information compromise are associated with higher levels of performing these responses.

2.4.3. Affect in Risk Judgments. One of the primary manners in which affect influences risk decisions is by the effect it has on how individuals perceive risk. This is important given the significant body of research that shows how people perceive risk, generally operationalized as perceived threat severity and perceived threat vulnerability, has been one of the major determinants of risk behavior in general [33], and in information security behavior in particular [34].

There are two primary mechanisms through which affect is said to influence our risk perceptions: optimistic bias and mood maintenance. Optimistic bias involves those with a greater positive affect (and/or lower negative affect) will make more optimistic judgments related to risk than those with a higher negative affect (and/or lower positive affect) [35]. This is explained in part by the priming mechanism of affect. In contrast, the concept of mood maintenance involves individuals behaving in such a way so as to maintain their current mood [9]. For example, individuals that are happy do not want to behave in such a way as to change that state.

These two mechanisms are contradictory to one another, but can be reconciled by understanding the context in which each one works. When the losses (i.e., risks) are hypothetical or small then the optimistic bias will generally take precedent. However, if the losses are large and not hypothetical in nature then the mood maintenance hypothesis has been shown to be more effective as an explanatory agent [9]. With respect to the compromise of one's personal information, the mood maintenance mechanism is more appropriate given the very real and large impact consequences such as identity theft, financial losses, embarrassment, and reputation damage can have on an individual.

Thus, individuals with higher levels of positive affect are more likely to see risky situations as something they would just assume avoid. As a result, they perceive something negative happening as more likely than those with lower levels of positive affect. Therefore, it is expected that higher levels of trait positive affect are associated with higher levels of perceived threat severity and perceived threat vulnerability.

H6: Higher levels of trait positive affect are associated with higher levels of perceived threat severity.

H7: Higher levels of trait positive affect are associated with higher levels of perceived threat vulnerability.

Likewise, individuals with higher levels of negative affect are less likely to view the world and situations in a pessimistic manner. As a result, these individuals believe that their risks are lower than what they may actually be based on objective evidence.

H8: Higher levels of trait negative affect are associated with lower levels of perceived threat severity.

H9: Higher levels of trait negative affect are associated with lower levels of perceived threat vulnerability.

2.4.4. Affect and Self-Efficacy. In addition to affect having an effect on how decisions are evaluated, it has also been shown to influence an individual's self-efficacy. Bryan and Bryan (1991) induced positive mood as part of an experimental manipulation and found that this resulted in higher self-efficacy for older children (junior to high school students), but not for those younger. Other results have also supposed affect's influence on self-efficacy [6]. This optimistic thinking leads to increased levels of self-efficacy compared to those with lower levels of positive affect.

H10: Higher levels of trait positive affect are associated with higher levels of self-efficacy related to performing the responses necessary to mitigate the threat of personal information compromise.

Likewise, those with higher levels of negative affect are more likely to make pessimistic evaluations in their ability to perform a task successfully. Therefore, it is expected that higher levels of trait negative affect are associated with lower levels of self-efficacy related to performing the responses necessary to mitigate the threat of personal information compromise.

H11: Higher levels of trait negative affect are associated with lower levels of information security self-efficacy related to performing the responses necessary to mitigate the threat of personal information compromise.

Based on hypotheses developed from the above discussion, the research model in Figure 1 (see section 4) was developed with the results noted therein.

3. Methods

This study explored the role trait affect has with the information security behavior of individual users in response to the threat of one's personal information being compromised. Previously developed and validated survey instruments for both the dependent and independent variables were used; the indicators for the PMT constructs were adapted from prior research.

The model that was tested included two constructs—trait positive affect and trait negative affect—hypothesized to act as antecedents to three independent variables—perceived threat severity, perceived threat vulnerability, and self-efficacy. These three constructs, along with perceived response efficacy and perceived response costs, are hypothesized to have a direct causal relationship with the information security behavior of individual users. Whereas trait positive affect and trait negative affect are hypothesized to have only an indirect effect on the dependent variable.

3.1. Research Procedures

Participants were recruited to complete the survey by using Amazon's Mechanical Turk. The use of Amazon's Mechanical Turk offers several advantages over other recruitment methods (e.g., students, word of mouth, flyers, and electronic postings) and can be as valid as these other approaches [36]. For example, turnaround time can be quick and the cost per participant low when compared to other methods, while quality remains comparable to other recruitment techniques [36].

The research itself consisted of a survey with a goal to obtain at least 310 usable responses based on a power analysis. This was done to help mitigate the chance of Type II errors, as well as ensure a large enough sample size for the number of paths in the model [37]. A meta-analysis of PMT indicates that the lowest effect size out of the five independent variables used in the current study to measure PMT is 0.21 for perceived threat vulnerability [33], which represents a low effect size [38]. Thus, using conservative estimates that included a one-tailed significance level of 0.05 (all hypotheses are directional), an effect size of 0.20, and a power of 0.80, the minimum sample size is 310 [38]. Therefore, the sample obtained of 556 participants met the minimum threshold of 310.

The primary measurement tool used to examine positive and negative affect has been the Positive and Negative Affect Schedule (PANAS) [24]. PANAS has been the primary measurement tool in large part due to the extensive reliability testing and validation of this instrument [39]. The PANAS consists of 20 items with 2 scales: positive affect (10 items) and negative affect (10 items) [24]. The instrument itself has been validated with several different time instructions, including an instruction for participants to indicate how "you generally feel this way, that is, how you feel on the average" [24, p. 1070]. This time instruction is designed to measure trait positive and negative affect.

3.2. Data Analysis Procedures

In addition to testing the structural model connecting various latent variables, it is also important to identify the measurement model, which links the indicators that can be measured to the unobservable latent variables [40]. The research model in this study included reflective, formative, and multidimensional constructs [41]. All indicators for the independent variables are reflective, but the measurement model also includes multidimensional aggregate constructs that are reflective first-order and formative second-order. Additionally, the dependent variable for the complete aggregated model is formative first-order and formative second-order. Therefore, the measurement model is considered formative. The following constructs are reflective: trait positive affect and trait negative affect [24], and perceived threat severity and perceived threat vulnerability [42]. In contrast, some of the constructs were multi-dimensional aggregate constructs consisting of reflective first-order, formative second-order: self-efficacy [43], perceived response costs [44], and perceived response efficacy [42]. A previously developed and validated survey instrument was used to assess the actions needed to protect one's self from the compromise of personal information and consisted of a formative first-order, formative second-order construct [30].

One thing that should be noted are the indicators used for perceived threat vulnerability have been modified for this study. In several studies, this construct has been problematic (e.g., significant but in the opposite direction [34] or not supported at all [43]). We opine that if individuals are already engaging in protective behaviors then they will believe they are less vulnerable to the threat. Thus, any correlation between the two constructs would be negative rather than positive. The problem likely stems from its adaptation from experimental research to survey research in which we are more interested in current behavior rather than people's perception of their vulnerability to a threat in the wake of a manipulation [42]. Therefore, in the current study we included two sets of indicators for this construct: one set was modified with a qualifier and the other set was left unchanged. An example of an indicator with the qualifier is: "If I do not take appropriate steps to protect myself, then I would be at risk for having my personal information compromised."

4. Analysis

4.1. Participants

Respondents from Amazon's Mechanical Turk provided pilot test data for this research. There were 109 responses to the survey with 12 being rejected for failing one or both of the attention check questions. This resulted in 97 respondents to pilot test the instrument. Statistical analysis included tests for reliability, including Cronbach's Alpha and composite reliability, as well as validity, including convergent and discriminant validity.

After making some minor wordsmithing changes based on data collected from the pilot study, we conducted the main study with a significantly larger sample size. The main change that was made involved one of the indicators for response costs that was worded opposite of the other indicators; this was changed for the main study to make it consistent. We received 607 responses with 51 being rejected for failing one or both of the attention check questions. This resulted in a final sample size of 556. This number was deemed sufficient as it was greater than the minimum threshold of 310 that was established through the power analysis discussed in the methods section. Participants were compensated $1.00 for participating in the survey.

We also collected certain demographic information from the participants. This included gender, highest education level attained, age, state of residence, and ethnicity. The state of residence information collected was converted into the four primary regions of the United States so that the participants from the main study could be easily compared with the United States population as a whole. Likewise, the age information collected was converted into fewer ranges to allow for easier comparisons. The gender of the participants consisted of a larger percentage of females than what is found in the U.S. population, but not by a large margin. Second, participants were generally more educated and younger than the average individual in the U.S. population. Finally, while the regional distribution of participants was quite similar to the U.S. population, there were a greater number of participants that identified themselves as white, Asian, or Pacific Islander than what is found in the U.S. To the extent the MTurk workers do not closely resemble the U.S. population, they do nonetheless provide good degree of diversity on key demographic indicators [36].

4.2. Data Analysis

4.2.1. Common Method Bias. The survey conducted in this research involved a single research method—surveys. This can give rise to common method bias in which the method itself accounts for a large amount of the variance. One test that screens for common method bias is the Harman’s single-factor test. Although this specific test does have shortcomings [45], it can be helpful in determining if there are any significant issues with respect to common method bias. Less than 21% of the total variance was explained by a single factor, which is below the maximum threshold of 50%.

In addition to testing for common method bias, it is also important to implement certain conditions *a priori* to minimize the likelihood of common method bias in the first place. In this research, the participants were anonymous to the research team and they were asked to simply answer honestly; both of these conditions help minimize the degree to which common method bias may impact results [45].

4.2.2. Reliability and Validity. The reliability is acceptable for all of the reflective constructs as demonstrated by both Cronbach’s Alpha and composite reliability values over the 0.700 minimum threshold [46]. Likewise, convergent validity is also acceptable with the composite reliability greater than the AVE for all of the constructs and more than the 0.500 minimum threshold [46]. Finally, the measures demonstrated discriminant validity with the AVE of the constructs greater than the square of the correlations with other constructs, as well as passing the cross-loading method of assessing discriminant validity [40]. All indicators loaded more highly on the construct they intended to measure than any other construct. Discriminant validity was also assessed and supported by using the Heterotrait-Monotrait Ratio (HTMT) method [47].

The approach used to measure and model the multiple dimensions involved in the research model, which consists of both a formative first-order, formative second-order construct (dependent variable) and reflective first-order, formative second-order constructs (three of the independent variables), consisted of the process outlined in [48], [49].

The results indicate that both trait positive affect and trait negative affect influence self-efficacy with the former also influencing perceived threat severity. Also, self-efficacy is an effective predictor of behavior, as noted in prior research [33]. Additionally, there is support for the hypotheses that perceived threat severity, perceived threat vulnerability, and perceived response costs influence the responses we engage in to mitigate the threat of having one’s personal information compromised. While perceived response efficacy was found to be significant at the 0.10 level, it did not meet our threshold of 0.05 that was established *a priori*. Therefore, seven of the 11 hypotheses were supported based on this research. Overall, the research model accounted for approximately 55.3% of the variance, which is quite high considering the exploratory nature of this research.

As noted earlier, we modified the wording of the indicators for perceived threat vulnerability. The construct with the modified indicators was statistically significant with the dependent variable. When the structural model was calculated using the perceived threat vulnerability construct with the non-modified indicators it remained statistically significant, but in the opposite direction of what was hypothesized. Thus, the modification of the indicators for this construct appears appropriate for survey research in which a manipulation does not occur.

Figure 1 includes the results for the research model. The structural model was calculated using Smart PLS, version 3.0 [50]. Complete statistical tables may be found at http://faculty.washington.edu/marcjd/hicss2019/

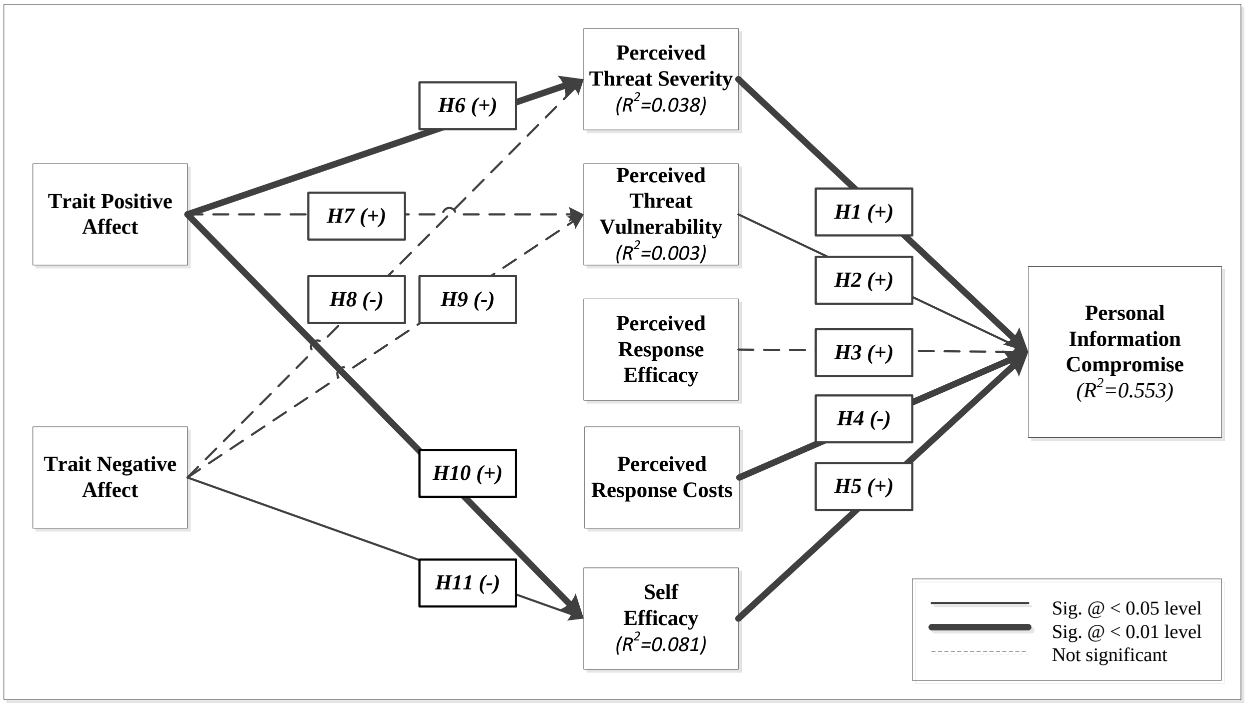

Figure 1. Trait Positive and Negative Affect and Personal Information Compromise

The complete results of our analysis are in Table 1.

Table 1. Research Model Results

Hypothesis	T Statistic	Sig.	Supported
H1: TS -> PIC	2.913	< 0.01	*Yes*
H2: TV -> PIC	2.090	< 0.05	*Yes*
H3: RE -> PIC	1.567	0.059	No
H4: RC -> PIC	2.812	< 0.01	*Yes*
H5: SE -> PIC	8.010	< 0.01	*Yes*
H6: TPA -> TS	4.185	< 0.01	*Yes*
H7: TPA -> TV	0.992	0.161	No
H8: TNA -> TS	0.312	0.378	No
H9: TNA -> TV	0.558	0.289	No
H10: TPA -> SE	5.037	< 0.01	*Yes*
H11: TNA -> SE	2.209	< 0.05	*Yes*
PIC: Personal Information Compromise **TS**: Threat Severity **|** **TV**: Threat Vulnerability **RE**: Response Efficacy **|** **RC**: Response Costs **SE**: Self-Efficacy **|** **TPA**: Trait Positive Affect **TNA**: Trait Negative Affect			

The previously developed instrument noted in the methods section was used to measure the dependent variable, while items adapted from Protection Motivation Theory and the PANAS [24] were used as the independent variables. Several tests were conducted to assess reliability and validity with minor changes made from the pilot study to the final study. All tests demonstrated acceptable levels of both reliability and validity. Likewise, the model explained a large amount of the variance—55.3 percent. Overall, seven of the 11 hypotheses were supported.

5. Discussion

5.1. Conclusions about the Research Problem and Hypotheses

The primary contribution this research makes is by incorporating trait affect into the research model. We did this by incorporating two constructs—one for trait positive affect and one for trait negative affect.

Both trait positive affect and trait negative affect appear to have a role in how individual users respond to information security threats. This includes primarily through their association with self-efficacy. Likewise, the degree to which individuals believe a threat is severe is associated with their level of trait positive affect. Individuals that are generally happier are more likely to view threats as severe, which is. This is consistent with the desire of individuals to maintain the status quo with respect to affect.

Prior research in the information systems domain that has examined the role of affect on the decisions we make has done this primarily by conceptualizing affect as how much an individual likes something, how much fun it is, and how interesting an activity may be [15], [51]. As discussed in the literature review section, the term affect has been operationalized in numerous ways. This has made the study of affect particularly problematic. Therefore, we spent considerable time discussing affect, how it was being operationalized in the current research, and why. Likewise, we used previously validated instruments from the psychology literature to measure affect. This process has led to the conclusion that trait affect, one of the many different types of affect, appears to be related to the information security behavior of individual users.

In addition to general conclusions that may be drawn about the research problem, we will discuss some of the issues related to the specific threat examined in this research.

5.2. Personal Information Compromise

Personal information compromise is a significant threat encountered by individual users. The current research suggests that those with higher levels of self-efficacy, a greater perception of the severity of the threat and more vulnerable to it, as well as lower levels of perceived costs related to the measures necessary to mitigate this threat, are more likely to engage in such measures.

Both of the antecedents examined here may lead to higher levels of self-efficacy as the level of trait positive affect increases and/or the level of trait negative affect decreases. Therefore, the relationship between these constructs and self-efficacy in this study is important and of great practical significance. At least for the threat of personal information compromise, individuals with higher levels of self-efficacy are more likely to perform the measures necessary to mitigate against this threat. Likewise, higher levels of trait positive affect are associated with higher levels of perceived threat severity.

5.3. Implications for Theory

With respect to Protection Motivation Theory, this research demonstrates the important role perceived threat severity, perceived threat vulnerability, perceived response costs, and self-efficacy may have in explaining human behavior.

In contrast to a single theory, such as Protection Motivation Theory, affect has been studied, conceptualized, and operationalized in numerous ways. There is no single definition of affect in the literature. As a result, we deconstructed affect based on the literature so that it could be reconstructed in the most logical manner possible. Developing a narrow focus of the type of affect under investigation in this research allowed us to demonstrate in a more definitive manner that trait affect in general, and both trait positive affect and trait negative affect in particular, may play a role in understanding the information security behavior of individual users.

The impact of trait affect on these two constructs is consistent with other research [15]. The primary implication for theory from this research is the need to conceptualize and operationalize affect in a very intentional and methodical manner for any study in which one wishes to measure it. It will be exceedingly difficult to compare different studies on affect if this is not done, let alone build upon our collective state of knowledge on the subject.

5.4. Implications for Practice

This research suggests that both trait positive affect and trait negative affect may act as antecedents to the information security behavior of individuals. While the focus has been on the individual user, employees of organizations are de facto individual users once outside of the organizational environment. Consequently, individuals with lower levels of trait positive affect and/or higher levels of trait negative affect may need additional encouragement and confidence building to improve their self-efficacy as it relates to performing information security tasks. This research is also consistent with other research on the connection between affect and self-efficacy [6]. Thus, organizations may view this connection in a more generic sense, even outside of the information security arena. Additionally, those with lower levels of trait positive affect may need additional messaging to convince them that they are vulnerable to the threat of having their personal information compromised.

5.5. Limitations

In this section, we discuss three possible limitations of this research. First, common method bias remains a possibility in any type of research in which a single method is used [45]. Although we did perform standard tests to check for it with no indications that it was a significant issue, common method bias cannot be ruled out completely.

Second, social desirability bias may have caused some participants to answer questions in a manner consistent with what they believe is the socially acceptable answer [52].

Third, the primary focus was on affect. There are several other types of affect that can and should be explored in future research in this area given the results found here, as well as countless other possible constructs that may provide additional insight into the information security behavior of individual users.

5.6. Further Research

With the above limitations in mind, we discuss two future research directions. First, trait affect in the current study was operationalized as two separate constructs—trait positive affect and trait negative affect. Although the hypotheses associated with the two constructs were supported in half of the cases, their efficacy may nonetheless vary based on the context of the study, such as the specific threat under examination. Therefore, it will be important to examine the issues raised here by looking at other threats.

Second, it may be prudent to consider other ways in which affect may be operationalized. This could include an examination of trait affect with a higher level of granularity than was done in this research, such as examining the lower dimensions of affect (e.g., joviality, self-assurance, hostility, sadness, and fear).

6. Conclusion

Seven of the 11 hypotheses examined here were supported, including three out of the six related to trait affect. Based on these results, this research makes two primary contributions.

First, we know that both trait positive affect and trait negative affect may play a role in the information security behavior of individual users, primarily through their impact on self-efficacy, but also through trait positive affect's impact on perceived threat severity.

Second, this research extended the application of Protection Motivation Theory (PMT), which has been the primary underlying theory used by researchers in understanding the behavior of individual users.

7. References

[1] M. Dupuis, S. Khadeer, and J. Huang, "'I Got the Job!': An Exploratory Study Examining the Psychological Factors Related to Status Updates on Facebook," *Comput. Hum. Behav.*, vol. 73, pp. 132–140, 2017.

[2] L. J. Camp, "Respecting people and respecting privacy," *Commun. ACM*, vol. 58, no. 7, pp. 27–28, 2015.

[3] R. Crossler and F. Bélanger, "The Effects of Security Education Training and Awareness Programs and Individual Characteristics on End User Security Tool Usage," *J. Inf. Syst. Secur.*, vol. 5, no. 3, pp. 3–22, 2009.

[4] T. Dinev, "Why would we care about privacy?," *Eur. J. Inf. Syst.*, vol. 23, no. 2, pp. 97–102, 2014.

[5] E. J. Johnson and A. Tversky, "Affect, generalization, and the perception of risk.," *J. Pers. Soc. Psychol.*, vol. 45, no. 1, pp. 20–31, 1983.

[6] E. J. Grindley, S. J. Zizzi, and A. M. Nasypany, "Use of Protection Motivation Theory, Affect, and Barriers to Understand and Predict Adherence to Outpatient Rehabilitation.," *Phys. Ther.*, vol. 88, no. 12, 2008.

[7] R. W. Rogers, "A Protection Motivation Theory of Fear Appeals and Attitude Change," *J. Psychol.*, vol. 91, no. 1, p. 93, 1975.

[8] R. W. Rogers, "Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation," in *Social psychophysiology : a sourcebook*, J. T. Cacioppo and R. E. Petty, Eds. New York: Guilford Press, 1983, pp. 153–176.

[9] A. M. Isen, T. E. Nygren, and F. G. Ashby, "Influence of positive affect on the subjective utility of gains and losses: It is just not worth the risk.," *J. Pers. Soc. Psychol.*, vol. 55, no. 5, pp. 710–717, 1988.

[10] P. Zhang, "The affective response model: a theoretical framework of affective concepts and their relationships in the ICT context," *MIS Q.*, vol. 37, no. 1, pp. 247–274, 2013.

[11] J. Webster and J. J. Martocchio, "Microcomputer Playfulness: Development of a Measure with Workplace Implications," *MIS Q.*, vol. 16, no. 2, pp. 201–226, Jun. 1992.

[12] F. D. Davis, R. P. Bagozzi, and P. R. Warshaw, "Extrinsic and Intrinsic Motivation to Use Computers in the Workplace.," *J. Appl. Soc. Psychol.*, vol. 22, no. 14, p. 1111, 1992.

[13] R. J. Coffin and P. D. MacIntyre, "Motivational influences on computer-related affective states," *Comput. Hum. Behav.*, vol. 15, no. 5, pp. 549–569, Sep. 1999.

[14] F. D. Davis, R. P. Bagozzi, and P. R. Warshaw, "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models," *Manag. Sci.*, vol. 35, no. 8, pp. 982–1003, 1989.

[15] Y. "Andy" Wu, Sherry Ryan, and John Windsor, "Influence of Social Context and Affect on Individuals' Implementation of Information Security Safeguards," in *ICIS 2009 Proceedings*, 2009, p. Paper 70.

[16] D. R. Compeau and C. A. Higgins, "Computer Self-Efficacy: Development of a Measure and Initial Test," *MIS Q.*, vol. 19, no. 2, pp. 189–211, 1995.

[17] R. Wakefield and K. Wakefield, "Social media network behavior: A study of user passion and affect," *J. Strateg. Inf. Syst.*, vol. 25, no. 2, pp. 140–156, Jul. 2016.

[18] J. (Jonathan) Kim, E. H. (Eunice) Park, and R. L. Baskerville, "A model of emotion and computer abuse," *Inf. Manage.*, vol. 53, no. 1, pp. 91–108, Jan. 2016.

[19] P. Ekman and R. J. Davidson, *The nature of emotion : fundamental questions*. New York: Oxford University Press, 1994.

[20] A. M. Isen, "Toward understanding the role of affect in cognition," in *Handbook of social cognition*, R. S. Wyer and T. K. Srull, Eds. Hillsdale, N.J.: L. Erlbaum Associates, 1984, pp. 179–236.

[21] D. Watson and A. Tellegen, "Toward a consensual structure of mood.," *Psychol. Bull.*, vol. 98, no. 2, pp. 219–35, 1985.

[22] D. Watson and L. A. Clark, “The PANAS-X: Manual for the Positive and Negative Affect Schedule - Expanded Form.” University of Iowa, 1994.

[23] M. Dupuis, “‘Wait, Do I Know You?’: A Look at Personality and Preventing One’s Personal Information from being Compromised,” in *Proceedings of the 5th Annual Conference on Research in Information Technology*, Boston, MA, USA, 2016, pp. 55–55.

[24] D. Watson, L. A. Clark, and A. Tellegen, “Development and Validation of Brief Measures of Positive and Negative Affect: The PANAS Scales,” *J. Pers. Soc. Psychol.*, vol. 54, no. 6, pp. 1063–1070, Jun. 1988.

[25] D. Watson and L. A. Clark, “Measurement and Mismeasurement of Mood: Recurrent and Emergent Issues.,” *J. Pers. Assess.*, vol. 68, no. 2, p. 267, Apr. 1997.

[26] T. L. Webb and P. Sheeran, “Does changing behavioral intentions engender behavior change? A meta-analysis of the experimental evidence,” *Psychol. Bull.*, vol. 132, no. 2, pp. 249–268, 2006.

[27] W. Wood, J. M. Quinn, and D. A. Kashy, “Habits in everyday life: Thought, emotion, and action,” *J. Pers. Soc. Psychol.*, vol. 83, no. 6, pp. 1281–1297, 2002.

[28] A. Bandura, “Guide for constructing self-efficacy scales,” *Self-Effic. Beliefs Adolesc.*, vol. 5, pp. 307–337, 2006.

[29] G. M. Marakas, R. D. Johnson, and P. F. Clay, “The Evolving Nature of the Computer Self-Efficacy Construct: An Empirical Investigation of Measurement Construction, Validity, Reliability and Stability Over Time.,” *J. Assoc. Inf. Syst.*, vol. 8, no. 1, pp. 15–46, Jan. 2007.

[30] M. Dupuis, R. Crossler, and B. Endicott-Popovsky, “Measuring the Human Factor in Information Security and Privacy,” in *The 49th Hawaii International Conference on System Sciences (HICSS)*, Kauai, Hawaii, 2016.

[31] M. Warkentin, A. C. Johnston, and J. Shropshire, “The influence of the informal social learning environment on information privacy policy compliance efficacy and intention,” *Eur. J. Inf. Syst.*, vol. 20, no. 3, pp. 267–284, Jan. 2011.

[32] P. Norman, H. Boer, and E. R. Seydel, “Protection motivation theory,” in *Predicting Health Behaviour: Research and Practice with Social Cognition Models*, M. Conner and P. Norman, Eds. Maidenhead: Open University Press, 2005, pp. 81–126.

[33] D. L. Floyd, S. Prentice-Dunn, and R. W. Rogers, “A Meta-Analysis of Research on Protection Motivation Theory,” *J. Appl. Soc. Psychol.*, vol. 30, no. 2, p. 407, 2000.

[34] R. Crossler, “Protection Motivation Theory: Understanding Determinants to Backing Up Personal Data,” in *The 43rd Hawaii International Conference on System Sciences (HICSS)*, Koloa, Kauai, Hawaii, 2010, p. 10.

[35] J. S. Lerner and D. Keltner, “Fear, anger, and risk.,” *J. Pers. Soc. Psychol.*, vol. 81, no. 1, pp. 146–159, 2001.

[36] Z. R. Steelman, B. I. Hammer, and M. Limayem, “Data Collection in the Digital Age: Innovative Alterantives to Student Samples.,” *MIS Q.*, vol. 38, no. 2, pp. 355–378, 2014.

[37] J. F. Hair, C. M. Ringle, and M. Sarstedt, “PLS-SEM: Indeed a Silver Bullet.,” *J. Mark. Theory Pract.*, vol. 19, no. 2, pp. 139–152, 2011.

[38] J. Cohen, *Statistical power analysis for the behavioral sciences*. Routledge Academic, 1988.

[39] E. A. Waters, “Feeling good, feeling bad, and feeling at-risk: a review of incidental affect’s influence on likelihood estimates of health hazards and life events,” *J. Risk Res.*, vol. 11, no. 5, pp. 569–595, Jul. 2008.

[40] W. W. Chin, “The partial least squares approach to structural equation modeling,” in *Modern methods for business research*, G. A. Marcoulides, Ed. Mahwah, N.J.: Lawrence Erlbaum, 1998, pp. 295–336.

[41] S. Petter, D. Straub, and A. Rai, “Specifying formative constructs in information systems research,” *MIS Q.*, vol. 31, no. 4, pp. 623–656, 2007.

[42] K. Witte, K. A. Cameron, J. K. McKeon, and J. M. Berkowitz, “Predicting risk behaviors: Development and validation of a diagnostic scale.,” *J. Health Commun.*, vol. 1, no. 4, pp. 317–341, 1996.

[43] A. C. Johnston and M. Warkentin, “Fear Appeals and Information Security Behaviors: An Empirical Study,” *MIS Q.*, vol. 34, no. 3, pp. 548–566, 2010.

[44] S. Milne, S. Orbell, and P. Sheeran, “Combining motivational and volitional interventions to promote exercise participation: Protection motivation theory and implementation intentions,” *Br. J. Health Psychol.*, vol. 7, no. 2, pp. 163–184, 2002.

[45] P. M. Podsakoff, S. B. MacKenzie, J.-Y. Lee, and N. P. Podsakoff, “Common method biases in behavioral research: a critical review of the literature and recommended remedies.,” *J. Appl. Psychol.*, vol. 88, no. 5, p. 879, 2003.

[46] J. Hair, W. Black, B. Babin, and R. Anderson, *Multivariate data analysis*, 7th ed. Upper Saddle River, NJ: Prentice Hall, 2010.

[47] J. Henseler, C. M. Ringle, and M. Sarstedt, “A new criterion for assessing discriminant validity in variance-based structural equation modeling,” *J. Acad. Mark. Sci.*, pp. 1–21, 2015.

[48] C. M. Ringle, M. Sarstedt, and D. W. Straub, “A critical look at the use of PLS-SEM in MIS quarterly,” *MIS Q*, vol. 36, no. 1, pp. iii–xiv, 2012.

[49] P. B. Lowry and J. Gaskin, “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 Trans. Prof. Commun.*, 2014.

[50] C. M. Ringle, S. Wende, and J.-M. Becker, “SmartPLS 3. Bönningstedt: SmartPLS,” 2015.

[51] D. Compeau, C. A. Higgins, and S. Huff, “Social Cognitive Theory and Individual Reactions to Computing Technology: A Longitudinal Study,” *MIS Q.*, vol. 23, no. 2, pp. 145–158, 1999.

[52] R. F. DeVellis, *Scale development: theory and applications*, 3rd ed. Thousand Oaks, Calif: SAGE, 2012.