Can an Ego Defense Mechanism Model Help Explain Dysfunctional IS Security Behavior?

Completed Research

Abhijit Chaudhury  
Bryant University  
achaudhu@bryant.edu

Debasish Mallick  
University of St. Thomas  
dnmallick@stthomas.edu

Abstract

IS security behavior studies are becoming popular. To date, much of the research has been based on theories such as the Theory of Planned Behavior, Technology Adoption Model, Rational Choice theory and Theory of Reasoned Action. They view users as rational individuals making conscious utilitarian decisions when there is increasing evidence that security breaches are the result of human behavior such as carelessness, malicious intent, bad habits, and hostility. We propose the ego defense mechanism model, taken from the psychoanalytical world. This model makes no assumption of rationality and has been developed to help understand the roots of dysfunctional behavior such as fear, phobias, anger, forgetfulness, indifference and hostility. Our model shows that security threats trigger anxiety among users and the ego react by both functional and dysfunctional behavior. This could be the earliest if not the first paper to explore user behavior in IS security situations using this framework.

Keywords

Ego defense mechanism, IS Security.

Introduction

IS security behavior studies are becoming increasingly popular as business losses due to security breaches mount. The PricewaterhouseCoopers report of 2015 and Symantec’s 2017 report highlight information system vulnerability due to users’ lack of awareness and interest. According to Balozian and Leidner (2016), non-opportunistic but non-malicious behavior such as carelessness accounts for a significant number of breaches. Symantec’s report of 2017 points out that sophisticated attacks are becoming rarer, while simple attack modes such as spear phishing via emails are proving to be more effective as users get regularly seduced into opening risky virus-laden attachments exhibiting carelessness and denial of seriousness of IS threats.

To date, much of the research in the IS security behavior field has been based on basic theories such as the Theory of Planned Behavior (Ajzen 1991), Technology Adoption Model (TAM; Davis 1986), and Theory of Reasoned Action (Fisbein and Ajzen 1975). Almost all IS security research uses elements from these models, which view users as rational individuals making conscious utilitarian decisions (Zafar et al. 2017). However, there is increasing evidence in trade journals that security breaches are the result of human errors due to carelessness, malicious intent, bad habits, indifference, and hostility (Boss et al. 2015).

In contrast, the psychoanalytical world makes no assumption of rationality and theories there have developed to help understand the roots of dysfunctional behavior such as unreasonableness, fear, phobias, anger, and hostility. The psychoanalytical world is placed well to address the weaknesses in current IS theories to address the rich spectrum of unproductive behavior that users exhibit. The basic and fundamental model of psychoanalytical world was proposed by Anna Freud (1936) and was called the “Ego Defense Mechanism (EDM).” At this stage of research, we are using this basic model. According to
this model, individuals have an ego which in the face of threats develops anxiety and which leads to defensive actions such as denials, hostility, repression, resistance and others in order to obtain some relief from anxiety. This could be the earliest if not the first paper to explore user behavior in IS security situations using this framework of EDM. Our survey-based model shows that threats in the environment measured through dimensions such as likelihood and severity of damage triggers anxiety in individuals. This anxiety is measured along dimensions such as cognitive, affective aspect such as fear, and physiological aspects and escapism. The anxiety in turn leads to both diminishment of dysfunctional behavior such as denial of threats and resistance to policies and enhancement of productive behavior such as commitment to policies and exploration of solutions.

**Literature Survey**

<table>
<thead>
<tr>
<th>Theory/Independent factors</th>
<th>Mediating factors</th>
<th>Explained behavior</th>
<th>Philosophical roots</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection Motivation Theory (PMT)</td>
<td>Security policy attitude</td>
<td>Compliance intention</td>
<td>Rational, conscious, and cognitive</td>
<td>Tejaswi and Rao 2009</td>
</tr>
<tr>
<td>Technology Threats and Avoidance Theory</td>
<td>Avoidance motivation</td>
<td>Avoidance behavior</td>
<td>Rational, conscious, and cognitive</td>
<td>Lang and Xue 2010</td>
</tr>
<tr>
<td>Theory of Planned Behavior and Rational Choice Theory</td>
<td>Beliefs about consequences</td>
<td>Intention to comply</td>
<td>Rational, conscious, and cognitive</td>
<td>Balogun et al. 2010</td>
</tr>
<tr>
<td>PMT with Habit</td>
<td>Cognitive mediating process</td>
<td>Compliance intention</td>
<td>Rational and cognitive with unconscious habit</td>
<td>Vance and Babul 2012</td>
</tr>
<tr>
<td>Control Reactive Compliance Model (CRCM)</td>
<td>Reaction to new ISP</td>
<td>Compliance intention</td>
<td>Rational, conscious, and cognitive</td>
<td>Lowry and Moody IS 2014</td>
</tr>
<tr>
<td>Selective Organizational Information Privacy and Security Violation Model (SOIPVM)</td>
<td>Risk perception</td>
<td>Compliance intention</td>
<td>Rational, conscious, and cognitive</td>
<td>Walker and Lowry 2016</td>
</tr>
<tr>
<td>Fear Appeals Theory</td>
<td>Response efficacy, fear appeals</td>
<td>Intent</td>
<td>Rational based on PMT, but also recognizes role of affective states such as fear</td>
<td>Johnston and Warburton 2010; Johnston et al. 2015; Wall and Busche, 2017</td>
</tr>
<tr>
<td>Rational Choice Theory with Affective Drivers</td>
<td>Attitude toward compliance</td>
<td>Compliance behavior</td>
<td>Rational, cognitive, conscious individuals with affective factors</td>
<td>D’Arcy and Lowry 2017</td>
</tr>
<tr>
<td>Martin Model of Consumer Behavior</td>
<td>Reinforcing feedback in repeating behavior</td>
<td>Security behavior</td>
<td>Unconscious habits and affective behavior</td>
<td>Martin and Randolph 2017</td>
</tr>
</tbody>
</table>

**Table 1: Theories of IS Security Behavior: Literature Survey**

Early research (see Table 1) began with technology adoption models (TAM), the Theory of Reasoned Action (TRA), Theory of Planned Behavior (TPB), and Rational Choice Theory (RCT; Levin and Milgrom 2004). In turn, theories that used elements of TAM, TRA, and TPB, such as Protection Motivation Theory (Tejaswi and Rao 2009), Technology Threats and Avoidance (Lang and Xue 2010), and the Control Reactive
Compliance Model (Lowry and Moody 2012), became popular. One of the most cited papers, Bugurcu et al. (2010), is based on RCT and TPB.

While the rational and cognitive approach to decision making by IS users is the dominant approach, over time scholars have realized that this is a severely limited approach, in that it does not take into account emotional and affective factors in human behavior (D’Arcy and Lowry 2017). Over time, affective factors such as fear came to be proposed by Wall and Busche (2017), and fear appeal papers by Johnston and Warkentin (2010) and Johnston et al. (2015) appeared. Martin and Randolph (2017) highlighted that most of the choices we make in our daily working lives in the context of IS security are made out of habit. Table 1 demonstrates that the focus of IS researchers has been moving away from strict rational and cognitive approaches to hybrid approaches that include affect and habits.

Some of the deficiencies of the rational and cognitive approach that have been highlighted are: (1) Emotions drive decisions related to ISP compliance as much as rational considerations do (D’Arcy and Lowry 2017); (2) Most decisions in the context of IS security are habit-driven and made unconsciously (Martin and Randolph 2017); (3) TPB, TAM, and other models have shown strong correspondence between intention and subsequent behavior when there is a short time gap between intention and actually performing (D’Arcy and Lowry 2017). However, where there is a large gap, such as between buying a gym membership after the New Year and then going regularly through the year, the event and the process have historically been of low correlation. The behavioral roots of buying a gym membership and visiting regularly are different. The situation is similar to intending to comply with ISP and then going through all the frustrations involved in compliance during our daily work; (4) Compliance and noncompliance with ISP are taken as two ends of a single continuum, when the actual situation is that ISP has many elements; an individual may comply with some and not to others, and equally may comply today and not tomorrow. Questions that only address our intention to comply with ISP do not capture the mixture of functional and dysfunctional behavior we exhibit in our working lives.

In the real world, users fail to comply for a wide variety of reasons that include indifference, boredom, hostility, tiredness, exasperation, and so on. There is therefore a need for an approach that acknowledges users’ less than rational behavior and investigates its causes and consequences. Our research is based on the psychoanalytical model of ego defense mechanisms, which focuses exclusively on the most unreasonable spectrum of behaviors and immature reactions such as denial, fantasy, dissociation, disinterestedness, acting out, projection, and passive aggression. Defense mechanisms operate at the unconscious level and are involuntary in nature.

There are many examples in the IS security context where considering EDM brings up a very different perspective. A user might frequently fail to pay for and update their antivirus protection on machines they use at home for office work. The EDM approach would view such behavior as a mixture of denial that IS threats are consequential and repression of thoughts relating to bad consequences resulting from getting hacked. Similarly, an IT administrator who professes virtues of ISP compliance but is himself lackadaisical in observing rules could be viewed as practicing deception as a result of some hidden hostility toward the employer. Using EDM terminology, this would also be an instance of displacement where the aggressive impulse is redirected away from management toward the firm’s policies. Denial, repression, deception, and displacement are characterized as defense mechanisms.

**Research Question**

The paper focuses on the question “Can the ego defense mechanism model help explain both dysfunctional and functional behavior in the context of IS security, and can it be empirically established?” The rest of the paper is organized as follows: The next section sets out our theoretical framework, then the research model, followed by data analysis and finally the conclusion.
Theoretical Framework: Ego Defense Mechanism

Anna Freud (1936) was first to define ego defense mechanisms in detail, in her book The Ego and the Mechanisms of Defense. The latest clinical model employing EDM includes several constructs: first, a Self, which is the totality of one's personal being, the physical and psychological aspects, both conscious and unconscious. Ego is part of the Self. In psychoanalytical theory, "ego encompasses the adaptive and executive aspects of the human brain: the ability of the mind to integrate, master, and make sense of the inner and outer reality" (Vaillant 1993). Then we have stress or threats, which disturb the ego, generating anxiety (Beresford 2012). The ego reacts to this anxiety by employing defense mechanisms that relieve us of discomfort (figure 1 and 2).

figure 1: Ego Defense Mechanism

These defense mechanisms are psychological strategies brought into play by the ego to manipulate, deny, or distort reality in order to defend against feelings of anxiety. There are many processes that make up our defense mechanisms. Some of them are denial, which is denying reality, the threat and the source of anxiety; repression, or the burying of a painful feeling or thought from one's awareness; identification, incorporating an object or thought into oneself; displacement, shifting impulses from an unacceptable target to a more acceptable or less threatening target; and rationalization, the justification of one's behavior and motivations by substituting "good" acceptable reasons for the actual motivations.

Ego defense mechanisms work like the body's immune system, by recognizing a threat and the anxiety it is causing and constructing a defense to relieve that anxiety. They are unconscious psychological mechanisms that reduce anxiety arising from unacceptable or potentially harmful stimuli. The list of DMs is extensive and no theoretical classification has ever been agreed upon. Working within a psychoanalytic framework, Vaillant (1993) proposed a developmental hierarchy of defense levels, ranging from pathological mechanisms (e.g., denial and distortion), which allow the individual to alter current external experiences to remove any need to deal with reality, to mature mechanisms such as sublimation, humor, and altruism.

One resource used to evaluate these mechanisms is the Defense Style Questionnaire (DSQ-40), which is used in this paper. Andrews et al (1993) proposed a three-level arrangement of the DSQ-40—mature, neurotic, and immature—which was also adopted by Beresford (2012).

Research Model and Hypothesis

Increasing threats and anxiety: Our model is based on the ego defense mechanism model (Beresford 2012). It is a very general model applied to many situations where individuals are apt to exhibit neurotic behavior (Beresford 2012). Waqas, et al. (2015) using ego defense model show how stressors in the environment lead to anxiety on the part of medical students. Similarly, using the same model, Eum and Rice (2011) establish anxiety related to test environments and in a more general setting Araujo, et al. (1998) show how stress elements in adolescent lives lead to enhanced anxiety. In our model, anxiety consists of multiple elements, such as fear as an affect, cognitive dimensions of fear, physiological response to fear, and escapism. In the context of IS security, Wall and Busche (2017) propose a spare version of our model, where threat consists of severity and its likelihood, and propose that combination of elements provokes fear. As our general model has been used in many psychoanalytic situations over the last 50 years, we propose that:

H1: Increasing threats lead to increased anxiety
Anxiety and Dysfunctional behavior: Waqas, et al. (2015) using ego defense model show how anxiety on the part of medical students leads to dysfunctional behavior such as denial, suppression, displacement and others. Similarly, using the same model, Eum and Rice (2011) establish that cognitive anxiety related to test environments lead to avoidance orientation and poor academic performance. Araujo, et al. (1998) show how anxious adolescent show denial, regression and passive aggression. In our model, anxiety consists of multiple elements, such as fear as an affect, cognitive dimensions of fear, physiological response to fear, and escapism. In the context of IS security, Wall and Busche (2017) propose a spare version of our model only threat is considered and propose that threat leads to negligent behavior. Hence we posit:

H2: Anxiety is negatively correlated to dysfunctional behavior

Anxiety and Functional behavior: Waqas, et al. (2015) using ego defense model show how anxiety on the part of medical students leads to functional behavior such as sublimation and humor. Similarly, using the same model, Eum and Rice (2011) establish that cognitive anxiety leads to urge towards mastery. Araujo, et al. (1998) show how anxious adolescent can also exhibit mature behavior. In our model, anxiety consists of multiple elements, such as fear as an affect, cognitive dimensions of fear, physiological response to fear, and escapism. In the context of IS security, Wall and Busche (2017) propose a spare version of our model only threat is considered and propose that threat leads to protective behavior. Hence we posit:

H3: Anxiety is correlated positively to functional behavior

Methodology

Research Method
We have chosen to test our theoretically derived research model with survey data collected from undergraduate students in business schools in New England and the Midwest. The demographic characteristics are shown in Table 2

We developed instruments by adopting and adapting existing measures from previous research (see Table 7 for details).

Dependent Variables—Functional and dysfunctional behavior: In general, dysfunctional behavior is one that inhibits company’s goals and functional behavior is one promotes it. In particular, in this research, dysfunctional behavior is characterized by denial of IS threats and resistance to IS policies. Functional behavior is characterized by commitment to IS policies and exploration for better solutions.
The items were obtained from the Defense Style Questionnaire (DSQ-40) (Andrews et al. 1999), used in measuring unproductive behavior. Four items of our dependent behavior taken from DSQ were similar to behavior exhibited during organizational change: denial, resistance, exploration, and commitment, as described and measured in Neiva, Ross, et al. (2005). Items from management literature was thus mapped onto DSQ-40 used in psychoanalytical literature.

**Independent Variables**—**Threats, as a formative construct made up of risk severity, risk threats, domain understanding, and powerlessness.** The first three elements of the formative construct were obtained from the IS security research of Ng et al. (2009) and Herath & Rao (2009). Powerlessness is an item obtained from political science literature (Rousseau, et al. 2007).

**Mediating Variables**—**Anxiety, which is a formative construct made up of items from the Pain Anxiety Symptoms Scale (PASS 20).** Cognitive, escape, fear, and physiological anxiety were the four subscales considered by McCracken and Dhingra (2002) and they make up Anxiety factor.

**Data Collection**

The unit of data collection in our research is a single student. Undergraduate students from two business schools in New England and Midwest were surveyed. Seven sections were involved, and they were all sections smaller than 30 students each. Over 150 responses were received, out of which about 25 were rejected.

**TABLE 2: SAMPLE DEMOGRAPHICS**

<table>
<thead>
<tr>
<th>Respondents</th>
<th>% respondents</th>
<th>Respondents</th>
<th>% respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Male</td>
<td>63</td>
<td>Freshman and Sophomore</td>
<td>57%</td>
</tr>
<tr>
<td>Female</td>
<td>37</td>
<td>Junior &amp; Senior</td>
<td>43%</td>
</tr>
<tr>
<td>Age below 20 years</td>
<td>31%</td>
<td>Age equal to or above 20 years</td>
<td>69%</td>
</tr>
</tbody>
</table>

**Results**

**Assessment of Measurement & Structural Models**

Reflective Constructs: We tested for reliability and convergent and discriminant validity. Table 3 shows the means for the indicators of both formative and reflective constructs. Formative constructs are treated differently from reflective constructs. We assessed the reliability of reflective constructs with Cronbach’s alpha coefficient, composite reliability, and significance of item loading (see Tables 3 and 4). The reflective construct of top relational capital achieved a score above the recommended value of 0.7 for Cronbach’s alpha and composite reliability (Nunally and Bernstein 1994), “but values should not be lower than 0.6” and that is what we have achieved in this exploratory study (see Table 4). The cross loadings for non-formative constructs are shown in Table 5. The values ensure the scale reliability and the internal consistency of the construct in our research model. For convergent validity of the reflective construct, we examined the factor loadings of the individual measure and the average variance extracted (AVE) (see Table 4). The AVE values for the reflective constructs were above the minimum recommended value of 0.50 (Fornell and Larcker 1981). For discriminant validity, we have Table 4, which shows that the AVEs for the reflective construct relational capital are much greater than their highest squared correlation with any other latent variable, thus ensuring discriminant validity.

Formative Constructs: The formative measurement model is assessed differently. The validity of formative constructs is assessed at two levels: the indicator level and the construct level. The indicator validity is assessed by indicator weights being significant at the 0.05 level (Chin, 1998) and also by the variance inflation factors (VIF) being below 10 (Gujarati, 2003). All items met these requirements of indicator significance and VIF values. Validity at the construct level in terms of inter-construct correlations is assessed by having the correlations be less than 0.7, which is the case (Table 4) (Henseler et al. 2009). At the construct level, nomological validity is ensured by having a relationship among formative constructs as justified in terms of prior literature, which is also the case here (Henseler et al. 2009).
The structural model was analyzed in three steps. First, the R-square of each of the endogenous latent variables was determined along with the most essential criteria. The path coefficients needed to be significant at the 0.05 level and the path weights to be more than 0.10 (Urbach and Ahlemann 1975). PLIS structural model results are shown in Figure 4 and summarized in Table 6. The model accounts for 33.8 percent of variance in Functional behavior, 3.38 percent of the variance in Dysfunctional behavior, and 16.6 percent of variance in Anxiety.

In the basic model of Threats, Anxiety, Functional and Dysfunctional behavior, all elements were significant. As shown in Figure 3, the effect of Threat on Anxiety was significant and positive ($\beta = 0.48, p < 0.05$), supporting Hypothesis 1. The effect of Anxiety on Dysfunctional behavior was significant and negative ($\beta = 0.581, p < 0.001$), supporting Hypothesis 2. The effect of Anxiety on Functional behavior was significant and positive ($\beta = 0.185, p < 0.05$), supporting Hypothesis 3.
Conclusion

In this research, we wanted to move beyond the single and unitary dimension of compliance as a dependent variable that dominates IS security literature. We wanted to address the rich spectrum of both productive and unproductive behavior exhibited by users in the context of security. Our goal was to validate the psychoanalytic ego defense model in the context of IS security. The important findings of the research are that threat perception in the IS security world is related to both productive and dysfunctional behavior and that anxiety plays an important role in that relationship. All the three basic relationships in the model were validated. This includes the threat–anxiety relationship, similar to the threat–fear relationship suggested by Wall and Busche (2017). The relationship between anxiety and dysfunctional behavior is also validated in that increasing anxiety leads to lower dysfunctional behavior. Also increasing anxiety leads to more functional behavior. This is in line with results obtained from fear appeal models (Johnston and Warkentin 2010; Johnston et al. 2015; Wall and Busche 2017), where threats were found to lead to more compliance. A survey was conducted among university students. Using students as survey population is common in ego defense studies such as Waqas, et al. (2015) and Eum and Rice (2011). Our model makes a major contribution in moving away from a purely rational & cognitive model to including affective elements such as fear, and its cognitive and physiological aspects as an intermediate variable between threats and compliance. Similarly, as dependent variables, we introduce both functional and dysfunctional behaviors with their own dimensions of deny, commit, resist, and explore. In future research, the model will be specialized to separate IS security scenarios. Each scenario is expected to bring along its suite of stressors, and types of functional and dysfunctional behavior. That will allow a deeper understanding of the roots of compliance behavior in different settings.

REFERENCES


---

**Table 7: Indicator Sources and Definitions**

<table>
<thead>
<tr>
<th>ANXIETY: Cognitive, Physiological, Fear and Escape (Formative)</th>
<th>COGNIT</th>
<th>FACED with hacking, I will find it hard to concentrate on a solution</th>
<th>McCracken and Dhingra 2002</th>
</tr>
</thead>
<tbody>
<tr>
<td>PHYSIO</td>
<td>Thinking about IT security issues makes me feel sick and nervous</td>
<td>McCracken and Dhingra 2002</td>
<td></td>
</tr>
<tr>
<td>FEAR</td>
<td>Issues about IT security are terrifying to me</td>
<td>McCracken and Dhingra 2002</td>
<td></td>
</tr>
<tr>
<td>ESCPE</td>
<td>It is difficult to protect one’s system against hacking</td>
<td>McCracken and Dhingra 2002</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FUNCTIONAL: Commit, Exploration (Formative)</th>
<th>COMMIT</th>
<th>If hacked I will work out my anxiety through doing constructive acts like implementing IS security steps</th>
<th>Andres et al. 1993 (DSQ-5); Bovey and Hede 2001</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXPLOR</td>
<td>If I were in a security crisis I would seek out another person who had the same problem</td>
<td>Andres et al. 1993 (DSQ2); Bovey and Hede 2001</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DYSFUNCTIONAL: Denial and Resistance (Formative)</th>
<th>DENIAL</th>
<th>I do not feel getting hacked</th>
<th>Andres et al. 1993 (DSQ4); Bovey and Hede 2001</th>
</tr>
</thead>
<tbody>
<tr>
<td>RESIST</td>
<td>I can keep a security-related problem out of my mind till I have time to deal with it</td>
<td>Andres et al. 1993 (DSQ3); Bovey and Hede 2001</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LIKELIHOOD (Reflective)</th>
<th>LIKL1</th>
<th>There is a likelihood that my system will get hacked and cause extreme damage</th>
<th>DSS 2009</th>
</tr>
</thead>
<tbody>
<tr>
<td>LIKL2</td>
<td>Damage due to virus and malware attack is uncertain??</td>
<td>DSS 2009</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>POWER (Reflective)</th>
<th>POWER1</th>
<th>Hackers are more knowledgeable than us</th>
<th>Rousseau and Garcia-Retamero 2007</th>
</tr>
</thead>
<tbody>
<tr>
<td>POWER2</td>
<td>The hackers have more resources than we have</td>
<td>Rousseau and Garcia-Retamero 2007</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SEVERITY (Reflective)</th>
<th>SEVER1</th>
<th>Hacking would jeopardize the work that I do with my colleagues</th>
<th>Ng et al. 2009</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEVER2</td>
<td>Having my computer hacked would be a serious problem for me</td>
<td>Ng et al. 2009</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>UNDERSTANDING (Reflective)</th>
<th>UND1</th>
<th>I am familiar with computer security practices</th>
<th>Ng et al. 2009</th>
</tr>
</thead>
<tbody>
<tr>
<td>UND2</td>
<td>I am familiar with IS security technologies</td>
<td>Ng et al. 2009</td>
<td></td>
</tr>
</tbody>
</table>