IPRPD
International Journal of Business & Management Studies
ISSN 2694-1430 (Print), 2694-1449 (Online)
Volume 06; Issue no 06: June, 2025
DOI: 10.56734/ijbms.v6n6a15

A PSYCHOANALYTIC MODEL OF DENIAL AND REACTIVE BEHAVIOR OF IS USERS: AN EMPIRICAL STUDY

Dr. Abby (Abhijit) Chaudhury[1]

[1]*Professor, Information Systems and Analytics, Bryant University*

Abstract

Information Systems (IS) security lapses are viewed as a strategic threat to firms. Repeatedly, it has been seen that the individual user is the weak link in the security chain. Much of the research used to model this behavior has been based on theories that view individuals as making conscious and rational choices to maximize their utility, when research has established that it is negligent, unconscious, and careless behavior that leads to security breaches. Drawing on psychoanalytic literature, we identify threats and psychosomatic symptoms as potential factors that lead to dysfunctional behavior. Our model provides empirical evidence that perceived threat by an individual's ego leads to symptoms of anxiety, which in turn leads to behavior characterized by denial of security threats and reactive behavior that exhibits indifference. This is one of the earliest papers to use psychoanalytic models relating to ego defense mechanisms to understand user behavior in the IS security context.

Keywords

Ego defense mechanism, Denial, Reactive Behavior, IS Security

Introduction

Carelessness of users and poor configuration of systems by information systems administrators were identified in Symantec's report of 2021[1] as it made them open to SMS phishing. Employees of firms were targeted by email-based threats such as spam, phishing, and malware. The Oracle and KPMG Cloud Threat Report 2020 identifies poor security habits of the user community and a "lack of security-first culture" as factors that promoted the success of targeted attacks on firms' systems.[2] According to the PwC report of 2018 on the "Global State of Information Security," "threats attributed to insiders such as third parties, including suppliers" play a major role in security failures.[3] As per these industry reports, it is simple: user-targeted attacks such as spear phishing using emails, voice mails, and text messages are effective in seducing an user to click on a virus-laden document and thus creating a pathway from the hacker to the sensitive data trove inside a firm.

[1] https://symantec-enterprise-blogs.security.com/blogs/feature-stories/symantec-security-summary-january-2021
[2] https://www.oracle.com/cloud/cloud-threat-report
[3] https://www.pwc.com/us/en/services/consulting/cybersecurity/l b a y/ nformation-security-survey.html

Moody et al. (2018) showed that "employees seldom followed the appropriate ISS actions prescribed in the security policies" and employees behaved in an insecure manner even if they were aware of said policies. Boss et al. (2015) showed that user carelessness, bad intent, and indifference lead to breaches. The goal of this paper is to use psychoanalytic theory to establish the causal factors that underlie dysfunctional behavior on the part of individual IS users.

Background

Understanding poor security behavior has been the focus of IS security literature, and several theories have been used to explain it that draw from fields such as criminology, health psychology, and social theories (Johnston et al. 2015). IS research on user behavior continues to rely on rational choice behavior models such as the theory of reasoned action (Fishbein and Aizen 1975) and theory of planned behavior (Aizen 1991). In their summary table, Moody et al. (2018) showed that models uniformly employ intention as a predictor of behavior with intention predictors such as costs, rewards, desire, and social influence—that is, the theories assume an individual is able to do a cost-benefit analysis that determines their security behavior.

Literature Survey

Early models of IS users' behavior such as protection motivation theory (Heratha and Rao 2009) had rational, conscious, and cognitive roots in the theory of reasoned action (TRA) and technology adoption model (TAM). Protection motivation theory tried to explain compliance intention based on efficacy and cost of security policies. It was followed by technology threats and avoidance theory (Liang and Xue 2010), which used perceived threats and safeguards to explain avoidance behavior. Bulgurcu et al. (2012) modeled compliance intention based on information systems policies and a rational awareness and beliefs about the same. According to this rational view of human nature, compliance is based on a cognitive evaluation of costs and benefits associated with compliance, with stable attitudes and beliefs relating to perceived threats, social norms, and security-related attitudes.

D'Arcy and Lowry (2017) pointed out that these theories do not take into account affective and emotional factors. While the rational choice-based theories continued to dominate, new affective factors such as fear came to be introduced by Johnston and Warkentin (2010) and Johnston et al. (2015). Similarly, Wall and Busche (2017) popularized fear appeal theories where perceived threats were used to explain intention to comply. Randolph and Martin (2017) highlighted that most of the choices we make in the context of IS security are made out of habit. Moody et al. (2018) continued to use affect as an additional factor to rational cost-benefit analysis, and social factors to predict intention.

In the literature, several deficiencies of rational and cognitive approaches have been pointed out: (1) Not just rational considerations, but emotions also drive IS security compliance (D'Arcy and Lowry 2017). (2) Unconscious habits drive decisions in the IS security world (Randolph and Martin 2017). (3) TRA, TAM, and other models have shown a close linkage between intention and subsequent behavior only when there is a short time gap between the intention and the behavior (D'Arcy and Lowry 2017). But often there is a large gap between, say, intention to purchase a diet and then following up on the diet through the year. Living through a diet and buying a diet plan do not share all the same behavioral roots. This is not unlike wishing to comply with IS security rules and then living through the hassles of coping with them during every hour of work. (4) In these models driven by rational choice theory, compliance and noncompliance are taken as two distinct poles, when in working life, one may comply with some rules some days and other rules other days. Survey questions that only ask about intention to comply miss out on the richness of real-life behavior. We may intend to follow IS security rules, but then fail to live up to our plan due to exasperation and delays relating to compliance, failure to remember, tiredness, and so on.

On the other hand, our basis here is the psychoanalytic model of ego defense mechanisms, where the focus is on immature and careless behaviors and unconscious habits relating to denial, disinterestedness, projection, and passive aggression. In psychoanalysis, the ego defense mechanism (EDM) is taken to operate at the unconscious level and is involuntary in nature (Freud 1938).

EDM provides a richer vocabulary and a very different perspective. We often fail to pay for and update antivirus protection on home machines through which we log into office networks. In the EDM world, this would be viewed as a mixture of denial that security threats are real and repression of unpleasant thoughts relating to 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. According to EDM terminology, this would be characterized as displacement behavior where the aggressive impulse is redirected away from management toward the firm's policies.

Research Question

We investigate the question: *"Does the ego defense mechanism model help explain denial and reactive behavior on the part of IS users?"*

The paper is organized as follows: We set up our framework for ego defense mechanisms in the next section, then elaborate on our research model, which is followed by analysis of data and a concluding section.

Theoretical Framework

In contrast to rationality-based models, the primary focus of the psychoanalytic world is on individuals' irrational and dysfunctional behavior and its causes and development. It furnishes a rich vocabulary of human behavior relating to phobias, aggression, indifference, psychosis, and guilt. EDM is a fundamental model of psychoanalysis first proposed by Anna Freud (1936) and used in this study. According to Wikipedia, "a defense mechanism is an unconscious psychological mechanism that reduces anxiety arising from unacceptable or potentially harmful stimuli." These mechanisms are strategies that our unconscious minds employ in order to protect against feelings of anxiety, guilt, and shame to maintain our ego's self schema of the world. Our unconscious minds distort and manipulate reality through mental defense mechanisms such as suppression of our awareness, denial of a uncomfortable reality, burying of painful feelings, rationalization of harmful behavior, and so on. Healthy individuals also use defense mechanisms to proceed through life; they become pathological only when their use leads to maladaptations in the real world and adverse health effects. In psychoanalysis, ego defense is seen as the mind's control system that scans the environment for threats, observes rising tension in the psyche, and then decides on a defensive action to best restore the equilibrium that preceded the threats perceived in the environment.

Ours is one of the earliest studies to apply EDM to study user behavior in IS security situations. This is a data-survey-based model that establishes that threats perceived by an individual lead to psychosomatic symptoms, here called anxiety. In this paper, anxiety relates to cognitive, physiological, and affective aspects such as fear, which in turn leads to dysfunctional behavior such as denial that the threat exists and reactive behavior seeking to convince oneself and others that if the threat factor exists, it does not matter to the individual. While the ego, id, and superego were suggested by Sigmund Freud as multiple agents in the psychic apparatus and he started the work on defense mechanisms, his daughter spent her life detailing defense mechanisms such as repression, regression, reaction, sublimation, and others (Freud 1936). The clinical model that is employed in patient treatment and analysis uses the notion of Self, of which ego is an important element. In psychoanalytic 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). According to Beresford (2012), the ego perceives an environmental threat, observes the threat disturbing it, and initiates behavior to release that tension. To defend against the feeling and discomfort of anxiety, the ego adopts strategies relating to manipulation, denial, and distortion. Basic ego defense mechanisms include denial, which is denying the observable reality; repression, which is burying the painful awareness of the situation; reaction, which is pretending to oneself and others that one is indifferent to the situation; and displacement, which is shifting impulses from a less acceptable target to a more acceptable one.

The list of defense mechanisms is extensive, and no theoretical classification has ever been agreed upon. However, many hierarchies have been suggested. Hierarchies use the notion of precedence: that is, more elementary reactions underlie more mature reactions. The most popular hierarchy was proposed by Vaillant (1993) and ranged from psychotic defenses to mature defenses such as altruism, humor, and sublimation. Denial, reactions, and projections are taken as less than mature responses and are often the stages before the more mature ones emerge. One resource used the Defense Style Questionnaire (DSQ-40) to identify denial and reaction as elements of EDM. Andrews et al. (1993) proposed a three-level

arrangement of the DSQ-40—mature, neurotic, and immature—which was also adopted by Beresford (2012).

Denial

Denial is a defense mechanism proposed by Anna Freud (1938) that involves a refusal to accept reality, thus blocking external events from awareness. If a situation is just too much to handle, the person may respond by refusing to perceive it or denying that it exists. As you might imagine, this is a primitive and dangerous defense—no one disregards reality and gets away with it for long! It can operate by itself or, more commonly, in combination with other, more subtle mechanisms that support it. Many people use denial in their everyday lives to avoid dealing with painful feelings or areas of life they do not wish to confront. For example, a husband may refuse to recognize obvious signs of his wife's infidelity, or a student may refuse to recognize their obvious lack of preparedness for an exam.

Reaction

Reaction formation is a psychological defense mechanism in which a person goes beyond denial and behaves in a way opposite to the way he or she thinks or feels. This is the next stage after denial. While denial may be fully unconscious, here the individual consciously overcompensates for anxiety[4] regarding socially unacceptable unconscious thoughts or emotions. Usually, a reaction formation is marked by exaggerated behavior, such as showiness and compulsiveness. By using the reaction formation, the id is satisfied while keeping the ego in ignorance of the true motives. Therapists often observe reaction formation in patients who claim to strongly believe in something and become angry at everyone who disagrees.

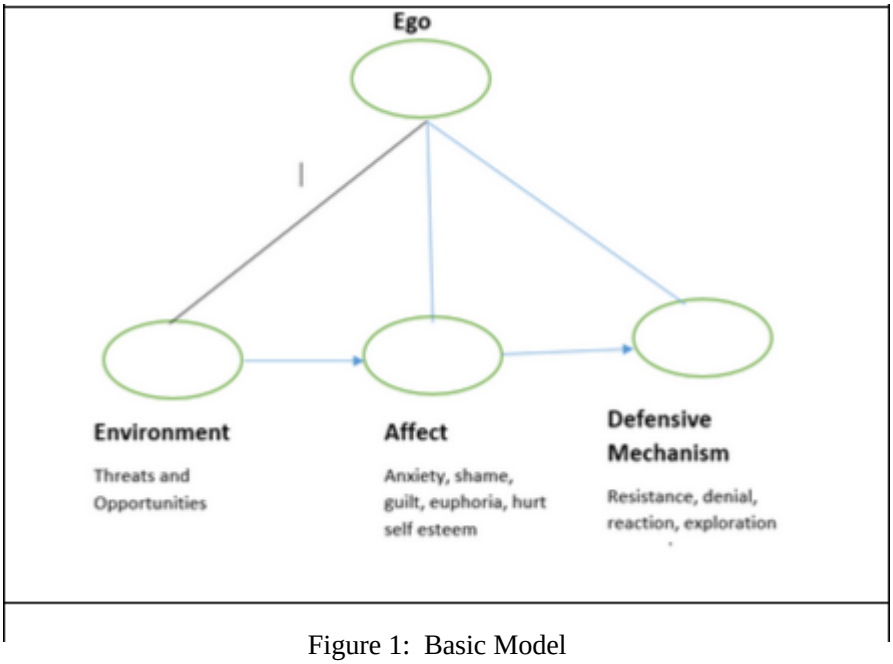

Figure 1: Basic Model

Research Hypothesis

Waqas et al (2015) attributed anxiety on the part of medical students to stress in the lives of the students. Stressful situations in the lives of adolescents lead to enhanced anxiety (Arrujo et al. 1998). Eum and Rice (2011) also established stress levels in a testing environment to be a source of anxiety. Wall and Busche (2017) established that the combination of threats and their likelihood creates fear among subjects. Cramer (2015) reported an experiment where during stressful tests, measures of diastolic pressure (DBP) and skin conductance level (SCL) were taken. It was found that increasing stress led to increased DBP and SCL. The relationship between stressful situations and anxiety has been fundamental in the world of psychoanalysis, and so we propose:

[4] https://www.simplypsychology.org/defense-mechanisms.html

H1: Increasing threat levels lead to higher anxiety levels

Waqas et al. (2015), using the ego defense model, showed how anxiety on the part of medical students led to dysfunctional behaviors such as denial, suppression, displacement, and others. Similarly, using the same model, Eum and Rice (2011) established that cognitive anxiety related to test environments led to avoidance orientation and poor academic performance. Araujo et al. (1998) showed how anxious adolescents engaged in denial, regression, and passive aggression. In our model, anxiety consists of multiple elements, including fear as an affect, cognitive dimensions of fear, physiological response to fear, and escapism. In the context of IS security, Wall and Busche (2017) proposed a spare version of our model: only threat was considered and they proposed that threat leads to negligent behavior. Goldstein (1980) and Ottengen (1996) found that when a diagnosis of serious illness was presented to patients, they would suffer bouts of anxiety, and dysfunctional behavior would result where the patients sometimes denied their illness and acted as if it were no concern. Schlund et al. (2020) found that threatening situations led to avoidance and denial. Similarly, Alex Meyer et al. (2019) found that anxiety led to avoidance behavior. As early as 1977, in the field of MIS, Bariff and Lusk (1977) had found that users would exhibit behavior similar to denial of an entire system if the users did not feel comfortable with it. Hence we posit:

H2: Anxiety levels influence denial and reactive behavior

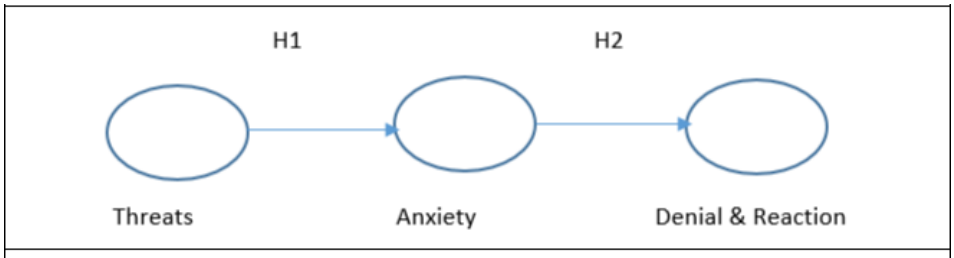

Figure 2: Research Model & Hypothesis

Methodology

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 1. In our research and survey, the unit of analysis is the individual engaged in an activity in a group setting assisted by technology. In socio-cultural theories, the unit of analysis is groups of individuals participating in broad systems of practices (Lave and Wenger 1991). Socio-constructivist theories, on the other hand, focus on individual students and view learning as an act of participation in a society (Palincsar 1998).

Our model variables are all formative in nature. In psychoanalytic models, multiple independent factors are often in play. These factors have their own causal chains, and while they may often appear together, it is not uncommon for them to appear independent of each other. Formative constructs are to be used as per Andreev, Heart et al. (2009) when the elements cause the construct and are not its reflection, the elements are not replaceable because they have different themes and causal reasons, they do not covary, and their antecedents are different. All these conditions are individually met by our three constructs: stress, anxiety, and denial and reactive behavior.

Variables

Dependent Variables: We are interested in inappropriate behavior, such as denial that IS security exists and is of consequence, and reactive behavior where the user exhibits evidence of not caring about such threats. A formative construct is used that is composed of these two elements.

Independent Variables: Threats, as a formative construct made up of risk severity, risk threats, and domain understanding. The first three elements of the formative construct were obtained from the IS security research of Ng et al. (2009) and Herath and Rao (2009).

Mediating Variables: A formative construct made up of items from the Pain Anxiety Symptoms scale has been used (PASS 20). McCracken and Dhingra (2002) used four sub-scales—cognitive, escape, fear, and physiological anxiety—to make up their construct of anxiety.

Table 6 provides the sources used to develop our items in this study.

Data Collection

A single student makes up the unit of data collection. Undergraduate students at two private business schools in New England and the Midwest were surveyed. About 125 workable surveys were received.

Respondents	**% respondents**	**Respondents**	**% respondents**
Male	63	Freshman and Sophomore	57%
Female	37	Junior and Senior	43%
Age below 20 years	31%	Age equal to or above 20 years	69%
Table 1:	**Sample**	**Demographics**	

Results

Assessment of Measurement and Structural Models

Formative Constructs: The authors assess the formative measurement model differently. The validity of formative constructs is assessed at two levels: the indicator level and the construct level. According to Chin (1998), indicator validity is assessed by indicator weights or coefficients greater than 0.1, which is the case here, and VIF values below 10 (Gujarati 2003). Inter-construct correlations are used to assess the formative construct at construct level, and their correlations are less than 0.7 (Table 3) (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)

Construct	**CR**	**CA**	**AV**		**Weight(formative)**	**VIF**
Stress			**E**	**Indicator**		
(formative)	n/a	n/a	n/a	Likl	0.7	1.0
				Sever	0.7	1.0
				Under	-0.8	1.0
Anxiety	n/a	n/a	n/a	Cognit	0.3	1.0
(formative)				Esc	0.1	1.0
				Fear	0.4	1.6
				Physio	0.5	1.6
Denial & Reaction	n/a	n/a	n/a	Denl	0.9	1.0
(formative)				React	1.0	1.0
Table 2: Psychometric properties of formative constructs						

Stress	Stress NA	Anxiety	Denial & Reaction
Anxiety	0.31	NA	
Denial & Reaction	0.11	0.53	NA

Table 3: Latent Variable Correlation

Variance inflation factor (VIF) is used to measure the multicollinearity among constructs according to Diamantopolous and Siguaw (2006). VIF for formative constructs varied from 1.0 to 2.0. The higher threshold value for VIF is 3.3. This shows that multicollinearity is not an issue with this model.

	Anxiety	Denial&Reaction	Stress
Cognit	*0.57*	-0.20	0.36
Esc	*0.31*	-0.13	0.16
Fear	*0.80*	-0.47	0.18
Physio	*0.85*	-0.47	0.18
Denl	-0.03	*0.56*	-.09
React	0.08	*0.98*	-0.12
Likl	0.21	-0.19	*0.68*
Sever	0.08	-0.10	*0.63*
Under	-0.21	-0.05	*0.68*

Table 4: Loadings and Cross Loadings

Table 5 displays the PLS structural model. The research model accounts for 15% of variance in denial and reactive behavior and 29% in anxiety outcome.

Denial & Reaction R-square = 0.149 Anxiety=0.29			
Path Effects	**Path Coefficient**	**T Statistics**	**P value /Result**
H1: Stress →Anxiety	0.34	4.05	0.0001/ ****Significant*
H2: Anxiety →Denial and Reaction	-0.55	7.92	0.0001/ ****Significant*

***p< 0.01; **p<0.05

Table 5: Test of Hypotheses

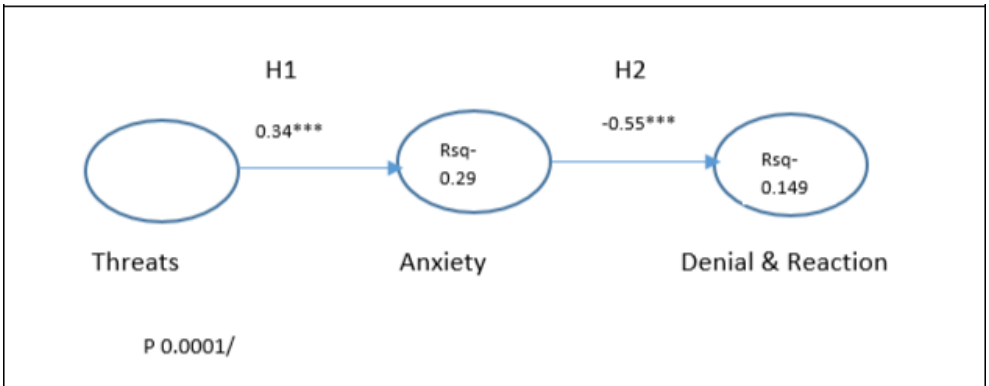

Figure 3: PLS Test of the Structural Model

Conclusion

This research moves away from a single unitary dimension of compliance. The dependent variable is a composite of denial and reactive behavior, unlike in other IS security behavior research, where the dependent variable is almost always the intent to comply. The goal here was to explore the model of defensive mechanism of the ego, which is the basis of all psychoanalysis. The study validates the hypothesis of the research that threats create anxiety and anxiety leads to dysfunctional behavior, such as denial that the threat is present and reactive behavior where even though the ego recognizes the threat, the individual publicly behaves as if the threat is of no concern. The survey data was obtained from students doing undergraduate studies in business at a Midwestern and a New England institution. In ego defense

research, it is common to use student populations, as in Waqas et al. (2005) and Eum and Rice (2011). The major contribution of our research is that we have moved past assumptions inherent in the rational and cognitive models that have been predominant in IS research on users' security-related behavior.

While the basic model in this research has similarity to fear appeal models (Wall and Busche 2017), the underlying causal structure is different and therefore leads to practical recommendations that are different in nature. Ego defense mechanisms have been studied in various domains, including clinical patients with serious medical problems but also routine cases relating to behavior modification for conditions like excess weight, smoking, hypertension, and diabetes (Oettingen 1996, Goldstein 1980). The repertoire of behavior studied in psychoanalysis is vast. In the future, we intend to study behaviors such as displacement, regression, and aggression that have previously been studied in organizational settings, but in the context of security-related behavior, such as in Bovey and Hede (2001).

Implications for Practitioners and Researchers

The world of psychoanalysis differentiates between coping mechanisms that individuals exhibit and defense mechanisms. The former involve a purposeful and conscious reaction, while the latter occur without conscious intentionality and function to manage a stress situation. Coping mechanisms are considered to be a part of a situation, whereas defense mechanisms are mostly a part of the individual and their mental characteristics. According to this approach, management needs to make employees conscious of their behavior so that they can promote adaptive behavior, reduce dysfunctional behavior, and recognize situations where dysfunctional behavior is automatically triggered.

Both individual and group therapy can help employees help themselves by recognizing their own patterns of behavior. Studies have shown (Cramer 2006) that immature behavior is replaced by mature behavior over time as individuals and groups become aware of the roots of their unconscious behavior. This has been shown by using the Global Assessment function (Bond and Perry 2004). The changes in defense mechanisms that occur in therapy have been described in clinical cases such as Perry, Beck, Constantinides, and Foley (2009).

Limitations of the Research and Findings

This is one of the earliest papers that uses a psychoanalytic approach to model IT users' dysfunctional behavior. The study thus was exploratory in nature and has several limitations. It was conducted in the US in private universities and in their business schools, which limits its generalizability. The survey method imposes its own limitations as well. In web-based surveys, users tend to provide responses that make them look good in their own eyes. The quantitative data provided by respondents reflect their perceptions of the issues. The causal directions are based on theoretical induction and no statistical analysis can confirm the link causalities.

References

Ajzen, Icek. (1991). "The theory of planned behavior," *Organizational Behavior and Human Decision Processes*, *50(*2), 179–211. AAAAA

Alex, Kirka Johanna and Meyer, M., et al (2019) Safety behaviors, experiential avoidance, and anxiety: A path analysis approach, *Journal of Anxiety Disorders*, 64, 9-15 AAA

Andrews, G., Singh, M., & Bond, M. (1993). "The Defense Style Questionnaire," *Journal of Nervous and Mental Disease* (181:4), 246-256. AAAA

Andreev, Pavel, and Heart, Tipsi, et al. (2009). Validating Formative Partial Least Squares (PLS) Models: Methodological Review and Empirical Illustration, *Thirteen International Conference on Information Systems, Phoenix, Arizona*, AAA

Araujo, K., Ryst, E., Steiner, H. (1999). "Adolescent defense style and life stressors," *Child Psychiatry Human Development*,(30), 19–28 AAA

Balozian, Puzant, and Leidner, Dorothy. (2016). "IS security menace: When security creates insecurity," *Thirty-Seventh International Conference on Information Systems*, Dublin.

Bariff, M. and Luck, E. J. (1977) Cognitive and Personality Tests for the Design of Management Information Systems, *Management Science*, 23(8) AAAA

Beresford, Thomas. (2012). *Psychological Adaptive Mechanisms: Ego Defense Recognition in Practice and Research*, NY: Oxford University Press. AAA

Bond, M., and Perry, J. (2004) Long term changes in defense styles with psychodynamic therapy for depressive, anxiety and personality disorders, *American Psychiatric Association*, https://doi.org/10.1176/appi.ajp.161.9.1665 AAA

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., and Polak, P. (2015). "What do users have to fear? Using fear appeals to engender threats and fear that motivate protective behavior in users," *MIS Quarterly* (39), 837-864. AAA

Bovey, Wayne H., and Hede, Andrew. (2001). "Resistance to organizational change: The role of defense mechanisms," *Journal of Managerial Psychology* 16(7), 534-548.

Bulgurcu, Burcu, Cavusoglu, Hasan, and Benbasat, Izak. (2012). "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness," *MIS Quarterly*, 34(3), 523-548. AAA

Chaudhury, Abhijit and Mallick, Debasish. (2018) Can an Ego Defense Mechanism Model Help Explain Dysfunctional IS Security Behavior? *Twenty-fourth Americas Conference on Information Systems*, New Orleans.

Chin, W. W. (1998). "The partial least squares approach to structural equation modeling," in *Modern Methods for Business Research*, G.A. Marcoulides (ed.), Mahwah, New Jersey: Lawrence Erlbaum Associates, 295-336. AAA

Cramer, Phebe (2015), Understanding Defense Mechanisms, *The American Academy of Psychoanalysis and Dynamic Psychiatry*, 43(4), 523-552 AAA

Davis, F. D. (1989). "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS Quarterly* ,13(3), 319-340.

D'Arcy, John, and Lowry, Paul Benjamin. (2017). "Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study," *Information Systems Journal*, 1-27. AAAA

Eum, KoUn and Rice, Kenneth, G. (2011). "Test anxiety, perfectionism, goal orientation, and academic performance," *Anxiety, Stress, & Coping*, 24(2), 167-178 AAA

Fisbein, M., and Ajzen, I. (1975). *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*, MA: Addison-Wesley. AAA

Fornell, Claes and Larcker, David, (1981) Structural Equation Models with Unobservable Variables and Measurement Error: Algebra and Statistics, *Journal of Marketing Research, Volume*, 18(3), 382-388 *AAA*

Freud, Anna. (1938). *The Ego and the Mechanisms of Defense*, NY: International University Press. AAAA

Goldstein, A. M. (1980). The "Uncooperative" patient: Self-destructive behavior in hemodialysis patients. In N. L. Farberow (Ed.), *The many faces of suicide: Indirect self-destructive behavior*, 89-98. New York: McGraw-Hill. AAA

Goel, Sanjay, Williams, Kevin, and Dincelli, Ersin. (2017). "Got phished? Internet security and human vulnerability," *Journal of the Association for Information Systems* 18(1), 22-44. V3

Gujarati, D.(2003). *Basic Econometrics*, New York: McGraw-Hill AAA

Henseler, J., Ringle, C.M. and Sinkovics, R.R. (2009), "The use of partial least squares path modeling in international marketing", Sinkovics, R.R. and Ghauri, P.N. (Ed.) *New Challenges to International Marketing*: *Advances in International Marketing*, v 20,AAA

Hofmann, Stephen, and Hay, Aleena (2018) Rethinking avoidance: Toward a balanced approach to avoidance in treating anxiety disorders, *Journal of Anxiety Disorders*

Volume 55, 14-21 AAAA

Heratha, Tejaswini, and Rao, H. R. (2009). "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness," *Decision Support Systems* (47), pp. 154–165. AAA

Heratha, Tejaswini, and Rao, H. R. (2009). "Protection motivation and deterrence: A framework for security policy and compliance in organizations," *European Journal of Information Systems* (18), 106-125. AAAA

Haeussinger, Felix, and Kranz, Johann. (2017). "Antecedents of employees information security awareness—review, synthesis and directions for future research," in *Proceedings of the 25th European Conference on Information Systems*, Guimaraes, Portugal.

Johnston, Allen C., and Warkentin, Merrill. (2010). "Fear appeals and information security behaviors: An empirical study," *MIS Quarterly*, 34(3), 549-566.

Johnston, Allen C., Warkentin, Merrill, and Siponen, Mikko. (2015). "An enhanced fear appeal rhetorical framework: Leveraging threats to human asset through sanctioning rhetoric," *MIS Quarterly* , 39(1), 113-134. AAAA

Lave, J. & Wenger, E. (1991) *Situated learning*, Cambridge, Cambridge University Press
AAA

Levin, Jonathan, and Milgrom, Paul. (2004). "Introduction to Choice Theory," available-https://web.stanford.edu/~jdlevin/Econ%20202/Choice%20Theory.pdf.

Lewthwaite, Rebecca. (1990). "Threat perception in competitive trait anxiety: The endangerment of important goals," *Journal of Sports and Exercise Psychology* (12). 280-300.

Liang, Huiganag, and Xue, Yajiong. (2010). "Understanding security behaviors in personal computer usage: A threat avoidance perspective," *Journal of the Association for Information Systems*, 11(7), 394-413. AAAA

Lowry, Paul Benjamin, and Moody, Gregory D. (2014). "Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organizational information security policies*," Information Systems Journal*, (92), 433-463.

McCracken, Lance M., and Dhingra, Lara. (2002). "A short version of the P in Anxiety Symptoms Scale (PASS-20): Preliminary development and validity," *Pain Resolution Management* (7:1), pp. 45-50. AAAA

Moody, Gregory D.; Siponen, Mikko; Pahnila, Seppo (2018) Towards a unified model of information security compliance, MIS Quarterly . Mar2018, Vol. 42 Issue 1, p285AAA

Neiva, Rabelo Elaine, Ros, Maria, and daPaz, Maria das Gracas. (2005). "Atttudes towards organizational change: Validation of scale," *Psychology in Spain*

Ng, Boon-Yuen, Kankanhalli, Atreyi, and Xu, Yunjie. (2009). "Studying users' computer security behavior: a health belief perspective," *Decision Support Systems* (46), pp. 815-825. AAAA

Nunnally, J. C., and Bernstein, I. H. (1994). *Psychometric Theory*, NY: McGraw-Hill. PricewaterhouseCoopers. 2015.

Oettingen, G. (1996). Positive fantasy and motivation. In P. M. Gollwitzer & J. A. Bargh (Eds.),*The psychology of action: Linking cognition and motivation to behavior*, 236-259. New York: Guilford. AAA

Palinscar, Sullivan (1998), Social Constructivist Perspectives on Teaching and Learning, *Annual Review of Psychology*, (49):345-375 AAA

Perry, J., Beck, Stephen, et al (2009) Studying Change in Defensive Functioning in Psychotherapy Using the Defense Mechanism Rating Scales: Four Hypotheses, Four Cases. In: Levy R.A., Ablon J.S. (eds) *Handbook of Evidence-Based Psychodynamic Psychotherapy. Current Clinical Psychiatry*. Humana Press AAAA

Randolph, Adrianne B., and Martin, Neale.(2017). "Towards a more secure HRIS: The role of HCI and unconscious behavior," *Transactions on Human-Computer Interaction*, 99(1), 59-74. AAA

Rousseau, David L., and Garcia-Retamero, Rocio. (2007). "Identity, power, and threat perception: A cross-national experimental study," *Journal of Conflict Resolution* 51(5), 744-771.

McCracken, Lance M., and Dhingra, Lara. (2002). "A short version of the P in Anxiety Symptoms Scale (PASS-20): Preliminary development and validity," *Pain Resolution Management* 7(1), pp. 45-50

Moody, Gregory D., Siponen, Mikko and Pahnila, Seppo (2018) Towards a unified model of information security compliance, *MIS Quarterly* , 42(1), 285-A22

Silva, Leiser. (2007). "Post-positivist review of Technology Acceptance Model," *Journal of Information Systems* 8(4), 255-256.

Schlund, Michael, Ludlum, Maddona, et al. (2020) Renewal of fear and avoidance in humans to escalating threat: Implications for translational research on anxiety disorders

Journal of the Experimental Analysis of Behavior, 113 (1), 153–171 AAAA

Stepanchuk, Ekaterina, Zhirkov, Anatoly, and Yakoleva, Anastasia. (2013). "The coping strategies, psychological defence mechanisms and emotional response to the disease in Russian patients with chronic leukemia," *Social and Behavioral Sciences* (86), 248-255.

Urbach, N., and Ahlemann, F. (2010). "Structural equation modeling in information systems research using partial least squares," *Journal of Information Technology Theory and Application* 11(2), 5-40.

Vance, Anthony, Siponen, Miko, and Pahnila, Seppo. (2012). "Motivating IS security compliance: Insights from Habit and Protection Motivation Theory," *Information and Management* , 49(4), 190-198.

Valillant, George. (1993). *The Wisdom of the Ego*, Cambridge: Harvard University Press.

Waqas, A., Rehman, A., Malik, A., et al. (2015). "Association of Ego Defense Mechanisms with Academic Performance, Anxiety and Depression in Medical Students: A Mixed Methods Study," Cureus 7(9), 1-16 AAA

Wall, Jeffrey, and Busche, Mari W. (2017). "To fear or not to fear? A critical review and analysis of fear appeals in the information security context," *Communications of the Association for Information Systems, 41(*13), 277-300 AAAA

Zafar, Humayun, Randolph, Adriance, and Martin, Neale. (2017). "Towards a more secure HRIS: The role of HCI and unconscious behavior," *Transactions on Human-Computer Interaction*, pp. 59-74.

Table 6: Indicator Sources and Definitions

ANXIETY Formative construct	COGNIT	Faced with hacking, I will find it hard to concentrate on a solution	McCracken and Dhingra 2002
	PHYSIO	Thinking about IT Security issues makes me feel sick and nervous	McCracken and Dhingra 2002
	FEAR	Issues about IT Security are terrifying to me	McCracken and Dhingra 2002
	ESC	It is difficult to protect one's system against hacking	McCracken and Dhingra 2002
DENIAL & REACTIVITY Formative construct	DENL	I do not fear getting hacked	Andres et al. 1993 (DSQ-item 42)
	REACT	I can keep security related problems out of my mind till I have time to deal with it.	Andres et al. 1993 (DSQ-item 03)
STRESS Formative construct	UNDER	I am familiar with IS security technologies	Ng et al. 2009
	SEVER	Having my computer hacked would be a serious problem for me	Heratha and Rao 2009
	LIKL	There is a likelihood that my system will get hacked and cause extreme damage	Heratha and Rao 2009