2015 48th Hawaii International Conference on System Sciences

The Dark Side of the Insider: Detecting the Insider Threat Through Examination of Dark Triad Personality Traits

Michele Maasberg
The University of Texas at San Antonio
michele.maasberg@utsa.edu

John Warren
The University of Texas at San Antonio
john.warren@utsa.edu

Nicole L. Beebe
The University of Texas at San Antonio
nicole.beebe@utsa.edu

Abstract

Efforts to understand what goes on in the mind of an insider have taken a back seat to developing technical controls, yet insider threat incidents persist. We examine insider threat incidents with malicious intent and propose an explanation through a relationship between Dark Triad personality traits and the insider threat. Although Dark Triad personality traits have emerged in insider threat cases and deviant workplace behavior studies, they have not been labeled as such and little empirical research has examined this phenomenon. This paper builds on previous research on insider threat and introduces ten propositions concerning the relationship between Dark Triad personality traits and insider threat behavior. We include behavioral antecedents based on the Theory of Planned Behavior and Capability Means Opportunity (CMO) model and the factors affecting those antecedents. This research addresses the behavioral aspect of the insider threat and provides new information in support of academics and practitioners.

1. Introduction

Computer and internet related crimes continue to rise, and Information Systems (IS) security continues to be one of the top managerial concerns [1], [2]. Of the IS security concerns, one of the greatest is the organizational insider [2]. Statistics regarding these internal sources of human threats have been underreported by organizations, due to fear of loss of reputation [2]. Breaches from an organizational insider are viewed as more costly than those from the outside [1]. In light of the insider threat, researchers are recognizing that security efforts must account for individual, social, and organizational influences, and that security controls must expand outside of an almost entirely technological approach to detection [1], [3].

Insiders have unique access to information systems [4]. They are often classified by role, such as permanent and temporary employees, vendors, contractors, suppliers, or ex-employees, or characterized in terms of the boundary in which they operate [2], [5], [6]. Compared to an outsider, insiders typically have some level of access, authorization, and/or advanced organizational knowledge [4]. The insider threat occurs when trusted members of an organization "behave in ways that put our data, our systems, our organizations, and even our businesses' viability at risk" [7, p. 169]. Table 1 shows a more granular breakout of insiders by category of malicious intent developed by the Carnegie Mellon University's Software Engineering Institute's Computer Emergency Response Team's (CERT) Division Insider Threat Center [8]. These categories include espionage, intellectual property (IP) theft, fraud, and information technology (IT) sabotage [8], [9]. Table 1 includes a definition of each category and the general characteristics of insiders extracted from past cases in these categories.

Table 1. Insider threat categories. Adapted from [5], [9]–[13]

Category	Definition	Insider Profile
Espionage	Classified or proprietary info to foreign entities	Currently employed, citizen, non-technical
IT Sabotage	Inflict damage on some area of organization	Former employee, technical, outside normal hours
Fraud	PII or customer info that leads to identity crime	Non-technical current employee, authorized access
Theft of IP	Steal trade secrets, customer info	Technical current employees, authorized access

Exploration of insider threat detection through examination of what goes on inside the mind of an insider has taken a back seat to information systems research and development of increasingly complex technical measures, particularly with regard to design and implementation [3], [14]. Although increasingly comprehensive technical controls prevent undesirable behavior, they can give a false sense of problem identification and solution, and the insider threat may

1530-1605/15 $31.00 © 2015 IEEE
DOI 10.1109/HICSS.2015.423

still happen. For example, former NSA analyst Ronald Pelton, convicted of espionage, memorized what he read and wrote it down, thereby subverting technical detection mechanisms [14].

Not only can insiders thwart technical detection, such mechanisms are limited to post-hoc detection of actual insider threat activity. They fail to provide indication and warning of imminent, rather than active insider threat activity.

This research distinguishes between insider threat *ability* and insider threat *probability*, by focusing on the root cause of the insider threat—motivation. We contend that the insider threat problem is a subjective issue of an individual's underlying psychology, and therefore, insider threat detection cannot be solved by objective technology alone [14].

This article seeks alternate explanations of insider threat behavior, thereby providing new signals useful for detection. We extend Dark Triad theory as an alternative explanation coupled with *negative attitude* and *malicious intent* as predictors of insider threat viewed through the lenses of the Theory of Planned Behavior and the Capability, Motive, and Opportunity (CMO) model. The *motive* and *trigger* (initiating negative event) constructs are external antecedents to the internal thought processes of the insider.

The remainder of the paper is outlined as follows. First, we position our discussion of Dark Triad personality traits as an extension of the Five-Factor Model (FFM) of personality, and provide definitions. Next we discuss past research and illuminate important research gaps. Then, we introduce constructs related to our proposed theoretical model based on the Theory of Planned Behavior and the CMO model supporting a set of 10 theoretical propositions. Finally, we provide a theoretical model and conclude with future research and concluding comments.

2. Theoretical Background

The development of the Five-Factor Model (FFM) is a result of the search for a structure of personality and has wide acceptance among personality researchers [15]. The Big Five traits consist of five constructs of personality that are a robust structure across major personality inventories and across cultures. These include extraversion, agreeableness, conscientiousness, neuroticism, and openness to experience [15].

The FFM has faced criticism for failing to fully account for all individual differences in personality-related human behavior, particularly traits reflecting antisocial behavior [16]. Recent research has shown that additional traits and dimensions can be added to the present FFM to represent socially malevolent behavior [16]. Paulhus and Williams [17] brought attention to three personality characteristics that were not redundant, but had empirical and conceptual overlap, and that could only be accounted for in part by the Big Five personality factors. This construct is known as the Dark Triad of personality.

2.1. Dark Triad Personality Traits

The Dark Triad are considered socially aversive personalities and are categorized as Machiavellianism, narcissism, and psychopathy [17]. Common personality characteristics shared by all three traits include a socially malevolent character, self-promotion, emotional coldness, duplicity, and aggressiveness. The Dark Triad personality traits are also collectively associated with feelings of superiority, privilege, lack of remorse, lack of empathy, and a tendency to exploit others [17].

Machiavellianism is considered the manipulative personality [17]. It refers to personality characteristics that reflect relational strategies marked by self-interest, deception, and manipulation [18]. Machiavellian personalities are likely to exploit others, are unlikely to be concerned about others beyond their own self-interest, and the personality is negatively correlated with empathy.

Narcissism is a subclinical form of the clinical personality disorder retaining the clinical elements of grandiosity, entitlement, dominance, and superiority [18]. Individuals displaying narcissism have an inflated self-view and focus largely on themselves [19].

Psychopathy, like narcissism, is adapted to the subclinical level from a clinical personality disorder [17]. Characteristics of psychopathy include high impulsivity and thrill-seeking along with low empathy and low anxiety [17]. Three significant qualities that characterize psychopathy include an arrogant and deceitful interpersonal style, deficient affective experience, and impulsive and irresponsible behavior [18].

Dark Triad personality traits are distinct from the Big Five personality traits yet show correlation. For example, a negative correlation was found with agreeableness for all three of the Dark Triad traits [17], [20]. Psychopathy was found to be marked by low neuroticism [17]. Machiavelli and psychopathy both show low levels of conscientiousness, and narcissism shows small positive associations with cognitive ability [17].

Recent research has shown that Dark Triad traits are informative in predicting workplace behavior [20]. In fact, Dark Triad personality traits have come up frequently in insider threat research and studies of insider threat cases at the individual level, although the studies have not labeled these traits as formal constructs for explaining insider behavior [21]. For example, insider threat research uses the term antisocial behavior to describe malicious insiders with regard to workplace deviance [7]. Independent of the FFM or Dark Triad models, researchers have identified lack of empathy and sense of entitlement as personality characteristics with direct implication for risk for insider threat [22], [23]; yet, lack of empathy is associated with all three Dark Triad personality traits, and sense of entitlement is included under narcissistic traits [17], [18].

Current research has reported insider threat cases with personality characteristics similar to Dark Triad personality traits [9]. For example, many convicted insiders were documented as "outwardly charming but manipulative sociopaths who appeared normal" [9, p. 75]. Specific case examples include Aldrich Ames, who was reported to have suffered from a narcissistic personality disorder that caused him to believe he was bulletproof, and former FBI agent Robert Hanssen, who was reported to lack a conscience [9]. Table 2 shows documented insider threat cases with known Dark Triad personality characteristics:

Table 2. Insider threat cases and Dark Triad personality characteristics. Adapted from [9].

Dark Triad Personality Characteristics in Insider Threat Cases	Brian Regan	Robert Hanssen	Aldrich Ames	Timothy Smith	Ryan Anderson	Ronald Hoffman	Michael Peri
Unusual need for attention	x	x	x	x	x	x	
Sense of entitlement / above the rules	x	x	x	x	x	x	
Arrogance	x	x	x	x	x	x	
Compensatory behaviors for self esteem	x	x	x	x	x	x	
Lack of impulse control	x	x	x	x	x		x
Lack of conscience	x	x	x	x	x		x
Chronic rule violations as in sociopathy	x	x	x	x	x		x

Although Dark Triad personality traits have emerged in insider threat cases and deviant workplace behavior studies, little empirical research has been done to study the comprehensive internal processes of insiders, or constructs between general personality traits (specifically Dark Triad) and insider threat behavior. Research has linked the FFM to deviant workplace behavior through the Theory of Planned Behavior, with personality traits determined to be antecedents of attitude, and in some cases the personality traits directly linked to intent, preceded by past behavior*,* or proposed to predict behavior directly [24]–[26].

Addressing this gap in the literature, we propose a comprehensive model of the internal thought process of the insider threat, using the Theory of Planned Behavior, based on the idea that Dark Triad personality traits will influence insider threat behavior when attenuated by the presence of the immediate factors of attitude and intent. As research has linked the FFM with deviant workplace behavior, we propose replacement of that construct in our model with Dark Triad personality traits based on apparent relationship of the traits. The relationship of the traits is particular to agreeableness, which past research has shown to have a negative relationship with workplace deviant behavior [26]. Based on a positive correlation between low agreeableness and all three Dark Triad personality traits, we propose that Dark Triad personality traits will also have a positive relationship with workplace deviant behavior, specifically insider threat, through connecting constructs attitude (specifically negative attitude) and intent (specifically malicious intent) in the Theory of Planned Behavior model [26], [27].

2.2. Negative Attitude

Attitude in general refers to a dichotomous evaluation of a psychological object, characterized by dimensions such as positive-negative, favorable-unfavorable, good-bad, and likable-dislikable [28], [29]. The expectancy-value model contributes to the conceptualization of attitude by including the ideas of formation of beliefs, association of belief with an attribute regarding the object, and overall attitude being determined by subject value of object attributes in interaction with strength of association [28].

Attitudes are relatively stable with an individual's core beliefs as their foundation, typically manifesting with a positive or negative shift. Attitude is also often regarded in terms of an automatic process of cognitive formation and from a multi-component view including cognition as well as affect, inclusive of beliefs and feelings regarding an object [28]. Strong attitudes are stable over time and believed to be resistant to persuasion. For strong attitudes, cognitive flexibility and willingness to change one's attitude is lower from early to middle adulthood and then increases in late adulthood [28].

Attitude serves a number of functions. These include adaptation to the environment, social adjustment, and ego defense [28]. Attitude is the construct that serves as the seat of bias for judgment and memory. A focus of continued research is the ability of attitudes to predict behavioral intentions and behavior.

For this paper, we view attitude as a dichotomous variable (i.e., positive or negative) and present the idea that a *negative attitude* should be associated with Dark Triad personality traits and subsequent deviant insider behavior. Viewing the insider threat through the lens of Dark Triad personality traits coupled with the Theory of Planned Behavior, we offer the following proposition.

Proposition 1: Dark Triad personality traits positively influence negative attitude in an insider threat incident.

2.3. Malicious Intent

Research has shown attitudes and personality traits to have poor predictive validity on behavior; they are implicated in human behavior, but their influence is by the presence of the immediate factor of intent [27]. In philosophical and legal literature, the concept of intent in relation to behavior is predicated on an individual's choice and is related to the ideas of consequences, aim, purpose, and objective [30]. Intent often includes the concept of desire, and is distinguished from trying, as an individual can intentionally refrain from a behavior without trying to do so in the case of omissions [30]. According to the Theory of Planned Behavior, intention to engage in a behavior is an indication of an individual's willingness to engage in the behavior in the presence of a given person or object and how much effort they are planning to exert in order to execute it [27], [31]. If intention to engage in a behavior is stronger, performance of that behavior has a higher likelihood [27]. Intention in this context also includes the idea that an individual is able to decide at will whether or not to perform the behavior, meaning the behavior is under volitional control [27].

The Theory of Planned Behavior combines intent and motive in the same construct, as it states "intentions are assumed to capture the motivational factors that influence a behavior" [27, p. 181]. Although confusion as to whether or not intent and motive are the same construct has occurred in the many venues [30], [32], insider threat and legal literature consider them separate concepts [9], [10], [21], [22], [30], [33]–[36].

Insider threat research differentiates intent and motive as it states "to prevent or mitigate threating insider behaviors, we must analyze all possibilities, intentional or not, with or without malicious motivation [7, p. 172]. In insider threat research, insider threat intent is most often differentiated by either the terminology *malicious intent* or the opposite construct that uses the terminology *no malicious intent, without malicious intent, well intentioned*, *inadvertent*, *unintentional* (we will refer to this construct as *unintentional insider threat (UIT)* based on CERT insider threat research [2], [7], [21], [33]. Malicious intent refers to a desire to cause harm to an organization or its information assets [2] and is the basis of the four categories of malicious insider incidents previously characterized in Table 1.

Malicious intent leading to the four categories of criminal insider threat in Table 1 is the specific construct in this study, due to the proposed connection to Dark Triad personality traits and deviant insider threat behavior. In legal literature, this type of intent is referred to as malice. Malice refers to wrongful intention or ill will (malevolence) and is defined as the intent to commit a wrongful act without justification [35].

Aside from intent, the legal term malice can also be applied to behavior and ulterior intent (motive). Insider threat research uses the word *malicious* to describe many potential elements of an insider threat nomological net to include intent, behavior, the individual, means, and motive [2], [3], [7], [9], [22], [37]–[42]. This extension of the legal term *malice* in the insider threat context demonstrates not only the legitimate exploration of legal literature for terminology in this paper but also the necessity of a study of the internal workings of an insider to determine who, what, when, where, how, and why malice exactly relates to a potential insider threat incident in order to apply an appropriate control.

In legal literature, insider threat *malicious intent* is comparable to the *criminal intent* of a defendant expressed in the concept of *mens rea* (Latin for "guilty mind"), which refers to the mental state of an individual that must be proven by the prosecution in a criminal case [30], [35]. The legal definition of intent refers to the state of mind accompanying an act, particularly an illegal act, coupled with the determination to do it [35]. Although tort law focuses more on negligence, tortious intention involves the element of deliberateness to do harm or conscious indifference to risk (recklessness) and can be a stronger basis for fault in a civil case [30].

In contrast to malicious intent in insider threat literature, an UIT is considered as such if an insider inadvertently causes harm to the confidentiality, integrity, or availability of organizational resources [33]. User error or ignorance can result in denial of service. For example, in 2007 Alex Greene tried to update his subscription to a Department of Homeland Security intelligence bulletin but mistakenly hit “reply all” and sent more than 2.2 million emails resulting in a shutdown of the email server after 7,500 emails were sent. The intent behind UIT can be difficult to determine. These events can result from mistakes, naiveté, or purposeful but nonmalicious violations of known security policy [7]. Although we are not focused on UIT for this study, it is important to note the difference in the literature for model clarity.

Like insider threat research, legal literature also separates intent and motive, as it states “the wrongdoer’s immediate intent, if he has one, is his purpose to commit the wrong; his ulterior intent, or motive is his purpose in committing it” [34, p. 659]. For this study, we will separate intent and motive, and focus on malicious intent, based on insider threat and legal literature and our desire to separate the internal thought processes of the insider from the external antecedents that motive often embodies. We will thus use a cross discipline based definition of malicious intent, as follows: *having the malevolent desire and willingness to engage (or fail to engage) in a wrongful act and subsequently making the decision to do* so [27], [31], [34], [35]. For this paper, our proposal of Dark Triad personality traits is in relationship to insider malicious intent as opposed to UIT due to the inclusion of malevolence in both the definitions of malice [35] and in reference to Dark Triad personality traits [17]. We propose malicious intent as a predictor of insider threat behavior based on the Theory of Planned Behavior and we offer the following propositions.

Proposition 2: Negative attitude positively influences malicious intent in an insider threat incident.

Proposition 3: Malicious intent positively influences an insider threat incident.

2.4. Motive

One’s motive is the reason why he or she engages in a behavior or intends its consequences [30]. Motive is often predicated on the evidential circumstance of external circumstances likely to incite an emotion [35]. Examples of insider threat motives include financial gain, curiosity, ideological, thrill, political, personal gain, revenge, ego, religion, terrorism, and competitive advantage [4], [10], [22], [43], [44].

Motive is often referred to as ulterior intent [34], [35]. “Every wrongful act may raise two distinct questions with respect to the intent of the doer. The first of these is: How did he do the act - intentionally or accidentally? The second is: If he did it intentionally, why did he do it? The first is an inquiry into his immediate intent: the second is concerned with his ulterior intent, or *motive*” [34, p. 660].

For this study, although motive will be separated from intent, we propose a direct relationship between the constructs. “An intention to do anything is consistent with any number of motives, and may remain unchanged while the motives vary” [34, p. 658] and “multiple motivations may map into a single intent” [42, p. 15]. We propose motive as a predictor of intent as even though motivation may derive from inside the organization or outside (i.e., personal) [7], the individual still makes a decision to act and then does so based on the Theory of Planned Behavior. We offer the following proposition.

Proposition 4: Motive positively influences malicious intent in an insider threat incident.

2.5. Perceived Behavioral Control and CMO Model

The premise of the perceived behavioral control construct from the Theory of Planned Behavior is that to the extent a person has the needed resources and opportunities (and intention) to perform a behavior, he or she should succeed in doing so [27]. Perceived behavioral control is another way of describing the idea of ability; it is predicated on the idea that behavior is strongly influenced by an individual’s confidence in their ability to perform it and denotes the subjective degree of control over it [27], [29]. This confidence in ability and perceived degree of control depends on nonmotivational factors such as availability of resources (or capability, such as money, skills, cooperation) and opportunities [27], [29].

Our model captures the *capability* and *opportunity* factors in this perceived behavioral control construct and proposes them as antecedents of intent and insider threat as an extension of the Theory of Planned Behavior, as according to the Theory of Planned Behavior, perceived behavioral control together with behavioral intention can be used to directly predict behavior [27]. We reinforce this proposal of antecedents of the specific behavior of insider threat by drawing from insider threat literature Capability Means Opportunity (CMO) model and developing a novel construct combination that fills a gap in the literature with an enhanced behavioral picture of an insider.

The CMO model is widely cited in insider threat research as a model to understand the nature of insider threat incidents particularly as a platform for research of detection and prevention [7], [12], [22], [45]–[47].

The CMO model is related to the concept and acronym of SKRAM [48]–[50], which typically characterizes a threat and is comprised of skills, knowledge, resources, authority, and motives. These characteristics comprising SKRAM are related to the threat source means or capability and the opportunity is related to the vulnerability separate from SKRAM, legitimizing the use of the evolved CMO model for this study [12], [46], [50]–[52].

The CMO model in insider threat research evaluates individual, interpersonal, and organizational factors and postulates that in order for a successful insider threat incident to occur, a perpetrator must have the capability to commit an attack, the motive to do so, and the opportunity to commit the crime [7], [22], [46], [47]. Insider threat literature states that for an insider threat to be able to abuse an organization's assets, motivation, capability & opportunity are the factors that make it possible [22]. The construct of motive has been broken out separately in our proposed model from the CMO model based on theoretical background previously presented and our discussion surrounds capability and opportunity.

Capability refers to the threat level of the insider based on dimensions such as sophistication of the insider, insider's access rights to the system and information, and knowledge level of specific organizational systems [12], [22], [50]. Capability of a potential insider threat source can also be characterized by skills, where the insider has expertise with regard to a particular information systems target, and the tactics used by the insider (for example, the type of attack) [50]. "What makes dishonest employees such a devastating threat is often the high quality of these attributes which are gleaned from the organization" [49, p. 2]. Viewing capability as the threat level of a potential insider threat source through the lenses of the Theory of Planned Behavior and CMO model, we offer the following propositions.

Proposition 5: Capability positively influences malicious intent in an insider threat incident.

Proposition 6: Capability positively influences an insider threat incident.

Opportunity refers to the insider's ability to exploit the vulnerabilities of an organization's information systems [22]. Vulnerabilities are weaknesses in an information system that may allow a threat (insider threat) to cause a compromise of the system through the window of opportunity [48]. Examples of opportunities or security loopholes that can be easily exploited by insiders include unclear, outdated, or nonexistent security policies, poor access control configurations on systems and data, lack of management support for information security, no vulnerability scanning or auditing, failure to implement job rotation or separation of duties, ineffective hiring screening process, and lack of formalized termination procedures where insiders maintain credentials [22], [51], [53]. Viewing opportunity as the ability to exploit a vulnerability through the Theory of Planned Behavior and CMO model, we offer the following propositions.

Proposition 7: Opportunity positively influences malicious intent in an insider threat incident.

Proposition 8: Opportunity positively influences an insider threat incident.

2.6. Trigger

Finally, we examine the concept of a trigger as a positive influence on attitude and motive. A trigger is a negative event, often unexpected by an insider, that initiates cognitive processing [6]. Examples of organizational triggers include abusive supervision, negative evaluations, and loss of employment [6]. Examples of negative events that influence insider beliefs, such as perceived injustices in cognitive processes include being passed over for a promotion, losing control of a critical system or application, failure to receive a bonus or raise, the hiring of a new supervisor, and demotions [10]. The beliefs, such as perceived injustices*,* resulting from these negative organizational events and the initial stage of the cognitive processing of the events are considered part of the attitude construct [6], [28]. Based on the idea that a trigger initiates the cognitive processing, we offer the following proposition.

Proposition 9: Trigger positively influences the effect of negative attitude in an insider threat incident.

A trigger can also either create or intensify a motive. "To identify precursors for a particular environment, it helps to identify motivators that might trigger malicious insider activity. Harrison identified three motivators: greed, political, and anger…Anger can potentially lead to sabotage activities. In this case it is easiest to identify associated triggers that may create or magnify anger. These might include termination, demotion, excessively increased or decreased responsibility, or significant lack of management support"[54, p. 4]. Accordingly, we offer the following proposition.

Proposition 10: Trigger positively influences the effect of motive in an insider threat incident.

2.7. Proposed Theoretical Model

Based on these 10 propositions, we propose the theoretical model shown in Figure 1.

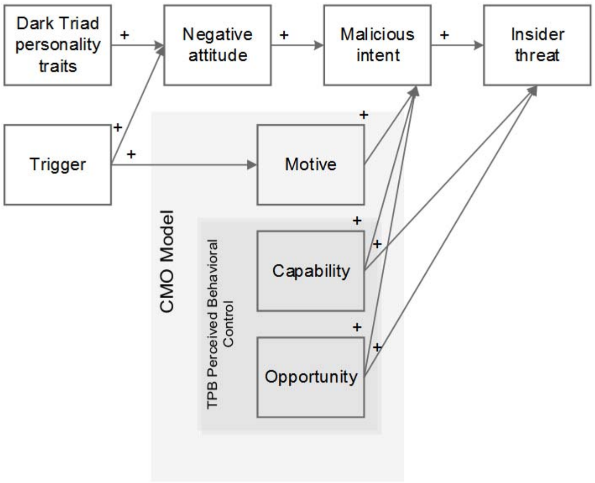

Figure 1. Insider threat model

3. Future Research and Concluding Comments

While the proposed relationship between Dark Triad personality traits, related constructs and external process antecedents were derived from past literature, further empirical research is needed. We propose that a case study analysis, using formal modeling methodology, can determine the retrospective detection probability and viability of this behavioral model. There are challenges, however, in conducting a restricted case study analysis. Specifically, empirical testing will be challenging due to: (1) accessibility of case data (2) availability of case data (3) privacy issues related to case data. Another challenge concerns the complexity of measuring psychosocial factors that lead to the formation of motivation and intention to conduct insider threat criminal behavior [55].

This paper calls for the formal treatment of the relationship between Dark Triad personality traits and insider threat. Accordingly, we use past literature and theory to support ten propositions related to that relationship, as well important connecting and antecedent constructs. Such factors include negative attitude, malicious intent, trigger, motive, capability and opportunity anchored in the Theory of Planned Behavior and CMO model. One of the best ways of reverse engineering an insider threat incident is through profiling [46], and this study illuminates a new way for behavioral profiling through examination of Dark Triad personality traits, thus providing new signals for detection. Practical use of this research includes organizational use of a Dark Triad personality survey instrument similar to [56] to evaluate new employees, similar to how they use Myers-Briggs Type Indicator (MBTI) assessment and the Adjective Check List (ACL) to identify personality and psychological traits. We propose that future research explore these relationships empirically through analysis and testing of previous insider threat cases.

4. Acknowledgements

Michele Maasberg was a Kudla Fellow at the University of Texas at San Antonio while working on this paper. She thanks the Fellowship program for its support during the 2013-2015 academic years.

5. References

[1] K. Bagchi and G. Udo, “An Analysis of the Growth of Computer and Internet Security Breaches,” *Communications of the Association for Information Systems*, vol. 12, no. 46, pp. 684–701, 2003.

[2] R. Willison and M. Warkentin, “Beyond Deterrence: An Expanded View of Employee Computer Abuse,” *MIS Quarterly*, vol. 37, no. 1, pp. 1–20, 2013.

[3] R. E. Crossler, A. C. Johnston, P. B. Lowry, Q. Hu, M. Warkentin, and R. Baskerville, “Future Directions for Behavioral Information Security Research,” *Computers & Security*, vol. 32, pp. 90–101, Feb. 2013.

[4] N. L. Beebe and V. S. Rao, “Improving Organizational Information Security Strategy via Meso-Level Application of Situational Crime Prevention to the Risk Management Process,” *Communications of the Association for Information Systems*, vol. 26, 2010.

[5] L. A. Kramer, H. Jr, R. J, and K. S. Crawford, “Technological, Social, and Economic Trends That Are Increasing U.S. Vulnerability to Insider Espionage,” Defense Personnel Security Research Center Monterey, CA, PERS-TR-05-10, May 2005.

[6] C. Posey, R. J. Bennett, and T. L. Roberts, “Understanding the Mindset of the Abusive Insider: An Examination of Insiders’ Causal Reasoning Following Internal Security Changes,” *Computers & Security*, vol. 30, no. 6–7, pp. 486–497, Sep. 2011.

[7] S. L. Pfleeger, J. B. Predd, J. Hunker, and C. Bulford, “Insiders Behaving Badly: Addressing Bad Actors and Their Actions,” *Information Forensics and Security, IEEE Transactions on*, vol. 5, pp. 169–179, 2010.

[8] M. Hanley, T. Dean, W. Schroeder, M. Houy, R. F. Trzeciak, and J. Montelibano, “An Analysis of Technical Observations in Insider Theft of Intellectual

Property Cases," Carnegie-Mellon University Software Engineering Institute Pittsburgh, PA, CMU/SEI-2011-TN-006, Feb. 2011.

[9] S. R. Band, D. M. Cappelli, L. F. Fischer, A. P. Moore, E. D. Shaw, and R. F. Trzeciak, "Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis," Carnegie-Mellon University Software Engineering Institute Pittsburgh, PA, CMU/SEI-2006-TR-026, Dec. 2006.

[10] A. Cummings, T. Lewellen, D. McIntire, A. Moore, and R. Trzeciak, "Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector," Carnegie-Mellon University Software Engineering Institute Pittsburgh, PA, CMU/SEI-2012-SR-004, Jul. 2012.

[11] K. L. Herbig and M. F. Wiskoff, "Espionage Against the United States by American Citizens 1947-2001," Defense Personnel Security Research Center Monterey, CA, PERSEREC-TR-02-5, Jul. 2002.

[12] A. P. Moore, D. M. Capelli, T. C. Caron, E. Shaw, D. Spooner, and R. F. Trzeciak, "A Preliminary Model of Insider Theft of Intellectual Property," Carnegie-Mellon University Software Engineering Institute Pittsburgh, PA, 2011.

[13] R. Trzeciak and D. Mundie, "Overview of the Threat Posed by Insiders to Critical Assets," DTIC Document, 2013.

[14] Irvin, John A. and Charney, David L., "Stopping the Next Snowden," *POLITICO Magazine*, 2014.

[15] T. A. Judge and J. E. Bono, "Five-factor model of personality and transformational leadership.," *Journal of Applied Psychology*, vol. 85, no. 5, pp. 751–765, 2000.

[16] L. Veselka, J. A. Schermer, and P. A. Vernon, "The Dark Triad and an Expanded Framework of Personality," *Personality and Individual Differences*, vol. 53, no. 4, pp. 417–425, Sep. 2012.

[17] D. L. Paulhus and K. M. Williams, "The Dark Triad of Personality: Narcissism, Machiavellianism, and Psychopathy," *Journal of Research in Personality*, vol. 36, no. 6, pp. 556–563, 2002.

[18] S. Jakobwitz and V. Egan, "The Dark Triad and Normal Personality Traits," *Personality and Individual Differences*, vol. 40, no. 2, pp. 331–339, Jan. 2006.

[19] E. A. Giammarco and P. A. Vernon, "Vengeance and the Dark Triad: The Role of Empathy and Perspective Taking in Trait Forgivingness," *Personality and Individual Differences*, Feb. 2014.

[20] A. Furnham, S. Richards, L. Rangel, and D. N. Jones, "Measuring Malevolence: Quantitative Issues Surrounding the Dark Triad of Personality," *Personality and Individual Differences*, Feb. 2014.

[21] S. L. Pfleeger and S. J. Stolfo, "Addressing the Insider Threat," *Security & Privacy, IEEE*, vol. 7, pp. 10–13, 2009.

[22] K. Roy Sarkar, "Assessing Insider Threats to Information Security Using Technical, Behavioural and Organisational Measures," *Information Security Technical Report*, vol. 15, no. 3, pp. 112–133, Aug. 2010.

[23] E. D. Shaw, J. M. Post, and K. G. Ruby, "Inside the Mind of the Insider," *Security Management*, vol. 43, pp. 34–44, Dec. 1999.

[24] G.-J. de Bruijn, J. Brug, and F. J. Van Lenthe, "Neuroticism, Conscientiousness and Fruit Consumption: Exploring Mediator and Moderator Effects in the Theory of Planned Behaviour," *Psychology & Health*, vol. 24, no. 9, pp. 1051–1069, Nov. 2009.

[25] M. Conner and C. Abraham, "Conscientiousness and the Theory of Planned Behavior: Toward a more Complete Model of the Antecedents of Intentions and Behavior," *Personality and Social Psychology Bulletin*, vol. 27, no. 11, pp. 1547–1561, Nov. 2001.

[26] H. Farhadi, O. Fatimah, R. Nasir, and W. S. Wan Shahrazad, "Agreeableness and Conscientiousness as Antecedents of Deviant Behavior in Workplace," *Asian Social Science*, vol. 8, no. 9, Jun. 2012.

[27] I. Ajzen, "The Theory of Planned Behavior," *Organizational Behavior and Human Decision Processes*, vol. 50, no. 2, pp. 179–211, Dec. 1991.

[28] I. Ajzen, "Nature and Operation of Attitudes," *Annual Review of Psychology*, vol. 52, no. 1, pp. 27–58, 2001.

[29] I. Ajzen, "Perceived Behavioral Control, Self-Efficacy, Locus of Control, and the Theory of Planned Behavior1," *Journal of Applied Social Psychology*, vol. 32, no. 4, pp. 665–683, Apr. 2002.

[30] P. Cane, "Mens Rea in Tort Law," *Oxford Journal of Legal Studies*, vol. 20, no. 4, pp. 533–556, Dec. 2000.

[31] M. Fishbein and I. Ajzen, "Attitudes and Opinions," *Annual Review of Psychology*, pp. 487–544, 1972.

[32] W. R. P. Kaufman, "Motive, Intention, and Morality in the Criminal Law," *Criminal Justice Review*, vol. 28, no. 2, pp. 317–335, Sep. 2003.

[33] The CERT Insider Threat Center, "Unintentional Insider Threats: Social Engineering," Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, CMU/SEI-2013-TN-024, 2014.

[34] W. W. Cook, "Act, Intention, and Motive in the Criminal Law," *The Yale Law Journal*, vol. 26, no. 8, pp. 645–663, Jun. 1917.

[35] B. A. Garner, T. Jackson, and J. Newman, Eds., *Black's Law Dictionary*, Eighth Edition. St. Paul, MN: West Publishing Co., 2004.

[36] L. A. Kramer and R. J. Heuer, "America's Increased Vulnerability to Insider Espionage," *International Journal of Intelligence and CounterIntelligence*, vol. 20, no. 1, pp. 50–64, 2007.

[37] K. Brancik and G. Ghinita, "The Optimization of Situational Awareness for Insider Threat Detection," *Proceedings of the first ACM conference on Data and application security and privacy*, pp. 231–236, 2011.

[38] F. L. Greitzer and R. E. Hohimer, "Modeling Human Behavior to Anticipate Insider Attacks," *Journal of Strategic Security*, vol. 4, no. 2, pp. 25–48, Jun. 2011.

[39] M. Hanley and J. Montelibano, "Insider Threat Control: Using Centralized Logging to Detect Data Exfiltration Near Insider Termination," Carnegie-Mellon University Software Engineering Institute Pittsburgh, PA, CMU/SEI-2011-TN-024, Oct. 2011.

[40] S. Furnell, “Enemies Within: The Problem of Insider Attacks,” *Computer Fraud & Security*, vol. 2004, pp. 6–11, 7.

[41] H. Chivers, J. A. Clark, P. Nobles, S. A. Shaikh, and H. Chen, “Knowing Who to Watch: Identifying Attackers Whose Actions are Hidden Within False Alarms and Background Noise,” *Information Systems Frontiers*, vol. 15, no. 1, pp. 17–34, Mar. 2013.

[42] J. Hunker and C. W. Probst, “Insiders and Insider Threats—An Overview of Definitions and Mitigation Techniques,” *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 2, no. 1, pp. 4–27, 2011.

[43] M. Maybury, P. Chase, B. Cheikes, D. Brackney, S. Matzner, T. Hetherington, B. Wood, C. Sibley, J. Marin, and T. Longstaff, “Analysis and Detection of Malicious Insiders,” DTIC Document, 2005.

[44] T. Walker, “Practical Management of Malicious Insider Threat – An Enterprise CSIRT Perspective,” *Information Security Technical Report*, vol. 13, pp. 225–234, 11.

[45] M. Kandias, N. Virvilis, and D. Gritzalis, “The Insider Threat in Cloud Computing,” in *Critical Information Infrastructure Security*, S. Bologna, B. Hämmerli, D. Gritzalis, and S. Wolthusen, Eds. Springer Berlin Heidelberg, 2013, pp. 93–103.

[46] E. E. Schultz, “A Framework for Understanding and Predicting Insider Attacks,” *Computers & Security*, vol. 21, no. 6, pp. 526–531, Oct. 2002.

[47] C. Xiaojun, S. Jinqiao, P. Yiguo, and Z. Haoliang, “An Intent-Driven Masquerader Detection Framework Based on Data Fusion,” in *Trustworthy Computing and Services*, Y. Yuan, X. Wu, and Y. Lu, Eds. Springer Berlin Heidelberg, 2013, pp. 450–457.

[48] R. Rowlingeon, “The Convergence of Military and Civil Approaches to Informaton Security?” Defence Evaluation and Research Agency, Malvern United Kingdom, Feb. 2000.

[49] R. Willison and M. Siponen, “Overcoming the Insider: Reducing Employee Computer Crime Through Situational Crime Prevention,” *Communications of the ACM*, vol. 52, no. 9, pp. 133–137, 2009.

[50] B. Wood, “An Insider Threat Model for Adversary Simulation,” *SRI International, Research on Mitigating the Insider Threat to Information Systems*, vol. 2, pp. 1–3, 2000.

[51] S. Bosworth, M. E. Kabay, and E. Whyne, *Computer Security Handbook*, 5th ed., vol. 1, 2 vols. New Jersey: Hoboken: John Wiley and Sons, Inc, 2009.

[52] D. B. Parker and B. S. Parker, *Fighting Computer Crime: A New Framework for Protecting Information*. New York: John Wiley and Sons, 1998.

[53] H. F. Tipton, *Official (ISC)2 Guide to the CISSP CBK*, Second. FL: Boca Raton: Taylor and Francis Group LLC, 2010.

[54] K. Nance and R. Marty, “Identifying and Visualizing the Malicious Insider Threat Using Bipartite Graphs,” presented at the 2011 44th Hawaii International Conference on System Sciences (HICSS), 2011, pp. 1–9.

[55] M. Warkentin, D. Straub, and K. Malimage, “Featured Talk: Measuring Secure Behavior: A Research Commentary,” in *7th Annual Symposium on Information Assurance (ASIA ’12) Secure Knowledge Management (SKM ’12) - A Workshop*, Albany, NY, 2012.

[56] D. N. Jones and D. L. Paulhus, “Introducing the Short Dark Triad (SD3) A Brief Measure of Dark Personality Traits,” *Assessment*, vol. 21, no. 1, pp. 28–41, 2014.