



---

Annual ADFSL Conference on Digital Forensics, Security and Law

2015  
Proceedings

---

May 21st, 8:30 AM

## Identifying Common Characteristics of Malicious Insiders


Nan Liang

Oklahoma State University, Spears School of Business, [nan.liang@okstate.edu](mailto:nan.liang@okstate.edu)

David Biros

Oklahoma State University, Spears School of Business, [david.biros@okstate.edu](mailto:david.biros@okstate.edu)

Follow this and additional works at: <https://commons.erau.edu/adfsl>

 Part of the Aviation Safety and Security Commons, Computer Law Commons, Defense and Security Studies Commons, Forensic Science and Technology Commons, Information Security Commons, National Security Law Commons, OS and Networks Commons, Other Computer Sciences Commons, and the Social Control, Law, Crime, and Deviance Commons

---

### Scholarly Commons Citation

Liang, Nan and Biros, David, "Identifying Common Characteristics of Malicious Insiders" (2015). *Annual ADFSL Conference on Digital Forensics, Security and Law*. 8.  
<https://commons.erau.edu/adfsl/2015/thursday/8>

This Peer Reviewed Paper is brought to you for free and open access by the Conferences at Scholarly Commons. It has been accepted for inclusion in Annual ADFSL Conference on Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact [commons@erau.edu](mailto:commons@erau.edu).

**EMBRY-RIDDLE**  
Aeronautical University™  
SCHOLARLY COMMONS

(c)ADFSL



# IDENTIFYING COMMON CHARACTERISTICS OF MALICIOUS INSIDERS

Nan Liang  
Oklahoma State University  
Spears School of Business  
Stillwater, Ok 74075  
nan.liang@okstate.edu

David Biros  
Oklahoma State University  
Spears School of Business  
Stillwater, Ok 74075  
david.biros@okstate.edu

## ABSTRACT

Malicious insiders account for large proportion of security breaches or other kinds of loss for organizations and have drawn attention of both academics and practitioners. Although methods and mechanism have been developed to monitor potential insider via electronic data monitoring, few studies focus on predicting potential malicious insiders. Based on the theory of planned behavior, certain cues should be observed or expressed when an individual performs as a malicious insider. Using text mining to analyze various media content of existing insider cases, we strive to develop a method to identify crucial and common indicators that an individual might be a malicious insider.

**Keywords:** malicious insider, insider threat, the theory of planned behavior, text mining

## 1. INTRODUCTION

In the field of information security, the subject of “insider threat” garners a lot of attention, yet has been deprived of sound empirical investigation. However, there is considerable anecdotal mention of the insider threat issue. In a recent report, the FBI noted 10 examples of insider attacks reported in recent years including the theft of trade secrets, corporate espionage, and the unauthorized disclosure of information (FBI report, 2010). These insider incidents resulted in financial losses in the millions of dollars.

Some researchers believe that insider threat, as opposed to outsider attacks, is easier to achieve as insiders are more familiar with the security structure of the in organizations in which they work (Anderson, 1999; Chinchani, Iyer, Ngo, & Upadhyaya, 2005). Insiders of an organizations either have legitimate access to organizational resources (Bishop, Engle, Peisert, Whalen, &

Gates, 2009) or have knowledge about the operations of the organization (Probst, Hunker, Gollmann, & Bishop, 2010). With their knowledge and legitimate access, they can bypass security protocols and exploit the trust the organization has placed on them (Bellovin, 2008).

## Information Age

The information age has brought on new outcomes from insider threat. Consequences of insider attacks have multi-dimensional loss, including financial loss, disruption to the organization, loss of reputation, and long-term impacts on organizational culture (Hunker & Probst, 2011). When compared to consequences of outsider attack, insider attack yields incidents with higher impacts (Chinchani et al., 2005) since insiders are familiar with countermeasures

of organizations and know how to find their targets.

The topics of insider and insider threat have received significant attention from both practitioners and academia in the information age. On one hand, insider threat is considered as one of the most serious security concerns (Anderson, 1999) as noted in the results of the 2008 CSI Computer Crime and Security Survey that listed “insider threat” second only to computer viruses a significant security concern. However, insider threat has received a relatively low level of scientific investigation (Chinchani et al., 2005). One important reason for this lack of attention is due to the difficulties in dealing with insider threat. Some of the reasons contributing to this gap in the research include lack of data for analysis and few useful methods for investigating the topic. As such, organizations employ technical controls such as firewalls and limit user access or order to prevent possible insider breaches of security.

Unfortunately, technical controls do little to isolate suspicious and malicious insider activities without unacceptable false positive alarms. For example, access control based on authentication and authorization has an important assumption that insiders would always use legitimate privileges to perform harmful activities and thus be caught, but once this assumption is violated, access control will lose its power.

Monitoring, another prevailing technique dealing with insider threat, is based on assumption that abnormal system usage indicates suspicious insiders. But monitoring is more of a post-hoc confirmation method to confirm already suspicious insiders of interest (Hunker & Probst, 2011), and thus brings into question if it can serve as a deterrent. (Pfleeger, 2008)

Technical approaches to insider threat combat suffer for two major shortcomings: First, malicious insider intention can be unobservable (Hunker & Probst, 2011) and behavioral patterns of insiders vary significantly. However, all insider attacks have one thing in common: they are performed by insiders with motivation. In a 2005 study about insider incidents in the

banking and financing sector Randazzo, et al. (2005) found that in 23 insider incidents from 1996 to 2003, 81% incidents involved perpetrators were motivated by financial gains, other than that, 23% for revenge, 15% for dissatisfaction and 15% for desire for respect. Other research suggests that anger, resentment or feelings of revenge could be root causes of insider attacks (De Cremer, 2006).

The extant research also tries to identify psychological indicators of malicious insiders’ motivation. Greitzer and Frincke (2010) developed 12 indicators of suspicious malicious insiders, top three of which are disgruntlement, accepting feedback and anger management issues. They also relayed that these indicators are fairly good predictors. However, these indicators are all factors which might be observed at workplace and assumption behind this is that a potential or ongoing malicious insider would reveal this at work. This may not always be the cases as disciplined insiders may stay “under the radar” and not exhibit such indicators. Further, these indicators have yet to be empirically validated.

The current state of the insider threat phenomenon is more oriented toward preventing possible perpetrators and less concerned with the identification and capture. This study aims to advance the existing research on identifying malicious insiders by employing information technology to validate insider threat indicators with empirical evidence.

The rest of this paper is arranged as follows: in the next section, we will review extant research on insider threat and introduce a research model to guide our investigation of potential indicators. Following that, we will discuss our data collection plan and methodology for analyzing that data. Finally, we will conclude by discussing some challenges and limitations in our forthcoming study.

## 2. LITERATURE REVIEW

In this section, we will first review definitions of both insider and insider threat and then the theory of planned behavior is discussed as

theoretical basis for the current research. Last but not the least, indicators of malicious in extant research are reviewed and organized into our framework.

## 2.1 Terminology

### Insiders

One of the challenges insider threat research is the lack of a widely accepted definition of insider. The term, *insider*, can be defined in several dimensions (Hunker & Probst, 2011):

**Access to the system:** an insider is defined as legitimate user (Chinchani et al., 2005) who is or previously has been authorized the access to an information system. Other definitions, instead, extend the meaning of access to include physical access and, an insider is defined as having logical or physical access (Randazzo, Keeney, Kowalski, Cappelli, & Moore, 2005).

**Action based definition:** “access to the system” definition defines who insiders are but action based definition defines what insiders do. Bishop and Gates (2008) defines an insider someone as who “violate security policy”.

**Intention based definition:** Hayden (1999) defines four categories of insider: traitor, zealot, browser and well-intentioned insider. Zealot strongly believes correctness should be made insider the organization; browser is a category of individuals who are overly curious in nature; traitor category includes those who have a malicious intent to “destroy, damage, or sell out their organizations”.

Moreover in more general sense, some research removes information system context (Bishop, Gollmann, Hunker, & Probst, 2008) and some combined several dimensions together, such as Wood’s definition which classified insider into different categories based on their system roles, intention and system consequences (Wood, 2000).

As stated by Hunker and Probst (2011), the definition of insider highly depends on research questions and situations of interest. In this research we focus on all kinds of insiders not confined to the information technology context and all malicious actions performed by these

insiders. For this research, we use the definition by Bishop and Gollmann (2008):

*An insider is a person that has been legitimately empowered with the right to access, represent, or decide about one or more assets of the organization’s structure.*

However as noted above, there exists various kinds of insiders and the subject of this research are malicious insiders, whose profiles are consistent with the description of Hunker and Probst: an individual deeply embedded in an organization, highly trusted and in a position to do great damage if so inclined.

### Insider Threat

The definition of insider threat depends on how insider is defined. Intuitively, insider threat is a threat posed by insiders. However, this definition is problematic since we could not have clear understanding of “threat” or evaluate “risk” of this threat even if “insider” were well defined. As argued by Hunker and Probst (2011), each factor used to determine insider can be used to determine taxonomy.

Although the majority of extant research defines insider threat as certain type of actions, no widely accepted taxonomy of insider threat exists. Hunker and Probst (2011) defines insider threats as potential misuses and actions which result in misuse. Chinchani and colleagues (2005) define insider threat as abuse of privileges with consequence of damage or losses. In other places in Chinchani’s research, insider threat is also defined as “violation of policies”. Specifically, Randazzo defines insider threat as actions affected the security of the organization’ data, system or operation (Randazzo et al., 2005).

Other research classified insider threats into different categories by different factors from different perspectives. Based on intentions, insider threat is classified into malicious or inadvertent actions (Brackney & Anderson, 2004). Combined with technical expertise dimension, actions are categorized into international destruction, detrimental misuse, dangerous tinkering, naïve mistakes, aware

assurance and basic hygiene (Stanton, Stam, Mastrangelo, & Jolton, 2005).

As noted in extant research, there exists various insiders and characteristics of insiders are inherently different in multi-dimensions. Consequently, definitions of insider threat depended heavily on the context of the study as well as research questions. Some research embraces this idea and suggests defining insider threat in a loose and general way to avoid “fine nuances” (Flegel, Vayssiere, and Bitz, 2010) while other research defines insider threat as a contextual taxonomy based on characteristics of the individual, the organization, the system and the environment (Predd, Pflieger, Hunker, & Bulford, 2008).

In this research, we adopt a broad definition of Predd et al. (2008) as:

*Insider threat: an insider’s action that puts an organization or its resources at risk.*

Predd et al.(2008), also extends this definition by specifying a contextual way as shown below (Figure 1). This diagram states that instead of defining insider threat as a term including various types of activities in a universal way, it’s better to include its context, including organization, system, environment and individuals as part of its definition. However, they do not differentiate non-malicious or careless insiders from malicious insiders

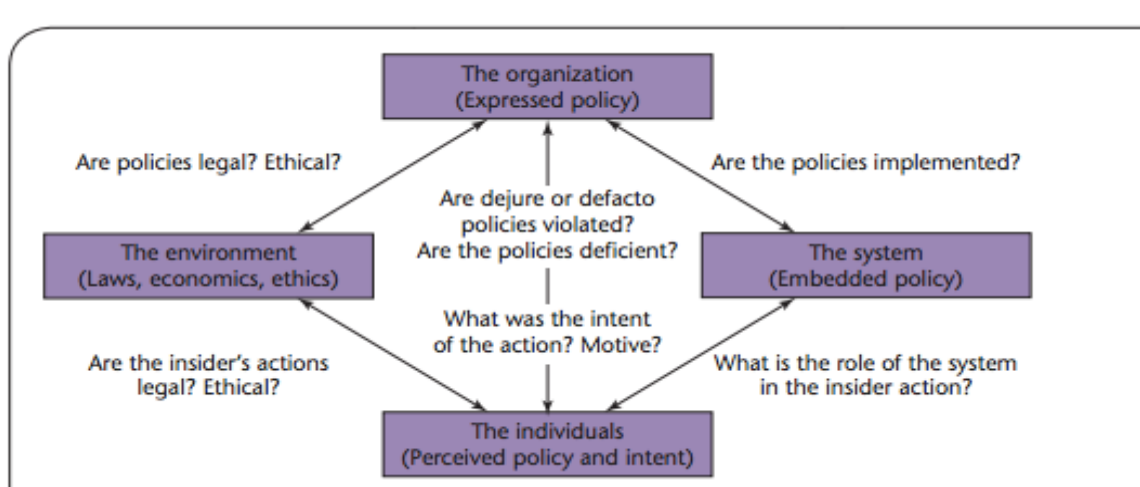


Figure 1 A Framework Of Insider Threat

This definition is adopted by two reasons:

First, Predd’s definition is consistent with our adopted taxonomy of insider. Research (Predd et al., 2008), from which we adopt definition of insider, defines insider threat as:

*“an insider threat is an individual with privileges who misuses them or whose access results in misuse.”*

This definition is consistent with respect to system usage as well as organizational consequence. What’s more, it broadens Hunker’s definition by adding context and

offering a top-down method in order to map different scenarios.

Second, Predd’s definition is consistent with our research question. The intended contribution of this study is to empirically identify common characteristics of *malicious insiders*. Our study focuses on identifying indicators that might help identify malicious insiders before they exploit their privileged access.

## 2.2 Criminology Theory and The Theory of Planned Behavior

As stated by previous research, certain theories in criminology are relevant to insider threat detection and prevention (Hunker & Probst, 2011) such as earlier theories of deterrence (Kankanhalli, et. al., 2003; Straub & Welke, 1998), social bonds (Lee et.al., 2004), and social learning (Hollinger, 1993; Parker & Parker, 1976; Skinner & Fream, 1997) which are integrated into the theory of planned behavior (Dugo, 2007; J. Lee & Lee, 2002; Peace, et.al., 2003).

Additionally, the Theory of Planned Behavior (TPB) was developed to explain and predict specific behaviors in a specific context (Ajzen, 1991). According to the theory, human behavior is guided by three kinds of considerations: behavioral beliefs, normative beliefs, and control beliefs (Ajzen, 1985). Behavioral beliefs are an individual's expectation of outcomes and their evaluations of these outcomes; normative beliefs represent other's expectation and individual's willingness to comply with these expectations and the last one refers to external factors which facilitate individual's intended action. From the framework of planned behavior, an individual's behavior is the result of motivation (behavioral beliefs), environments (normative beliefs) and opportunities (control beliefs).

The relevance of TPB is confirmed by both survey, in which among 23 insider incidents, 81% of related insiders planned their job; (Randazzo et al., 2005), as well as by theoretical model which includes risk-averse nature and planned action as factors affecting an insider's action (Wood, 2000). Further, Predd et al. (2008) argue that insider threat should be defined as specific to its context which makes it suitable for applying criminology into the study of insider threat.

## 2.3 Factors Affecting Incidents of Insider Threat

Based on Predd's (2008) work, an insider's actions are shaped by four factors: organization, individual himself/herself, environment and system. Organization sets up security rules and policy, as well as affect insider's action via organization culture. *System* reflects implemented policy; environments shape and constrain both organizational behavior and an insider's behavior through social or ethical norms; last but not the least, the individual's motivation directly affects how he/she plans and mount insider attacks. In this section, we will start with this framework and review related researches about organizational factors (including system), the insider's motivation and environmental effects.

### 2.3.1 Organizational Factors

According to Predd, organizational factors affecting insider threat include organizational security policy and organizational culture. Organizational security policy includes not only articulated policy but also implemented policy (the system). Besides, organizational culture affects insider threat via leveraging its employee's awareness and compliance of security policy as well as its management styles.

#### (1) Policy

Three aspects of policy will influence the effect of policy: capability of policy language, stated policy and implemented policy. First, as stated by Hunker and Probst, (2011), capability of policy language is not adequate to effectively prevent insider threat and this is the inherent shortcomings of policy language. This disadvantage originates from complex and dynamic situation which policy are facing. And he also suggests that deployment of domain-specified policy which could clarify situations in which execution could only be authorized when discretionary circumstances justify them. Second, policy taking place is not inherently the same kind as argued by Hunker, four hierarchy exist as oracle policy, feasible policy, configured policy and real time policy. Unawareness and

misunderstanding of policy hierarchy could result in policy absence or policy conflict.

What's more, policies are not always explicit but sometimes implicit and gap exists between stated policy and observed policy (Puhakainen, 2010), which could be mitigated by security training programs (Vance, 2012) and increased participation of top managers (Hu, 2012).

## (2) Organization Culture

Specifically, organization culture affect incidents of insider threat in the following aspects:

First, whether security policy support or interfere with organizational work flow will affect compliance with security policy.

Second, levels of security awareness to organization members will affect insider strategy (Hunker & Probst, 2011). Levels of security awareness includes perception, understanding and prediction (Shaw, Post, & Ruby, 1999).

Third, organizational purpose and management structure will affect security structure and policy.

### 2.3.2 Motivation of Insiders

We note that extant research focusing on motivations of insider and insider threats does not differentiate terms of "psychological profile" and "motivation". The former focuses more on personal or internal motivations and the latter focuses more on goals of insiders' actions.

In another study, (Wood, 2000) lists four major goals of malicious insiders: profit; provoking change such as change in policy; subverting mission of organization; and personal goals such as being respected or gaining power.

On the other hand, when considering psychological profile, Stolfo and colleagues (2008) list 10 types of motivation which might be most harmful:

- (1) making unintentional mistake;
- (2) trying to accomplish needed tasks;

- (3) trying to make the system do something for which it was not designed as a form of innovation to make the system more useful or usable;
- (4) trying innocently to do something beyond the authorized limit, without knowing the action is unauthorized;
- (5) checking the system for weakness, vulnerabilities or errors, with the intention of reporting problems
- (6) testing the limits of authorization; checking the system for weaknesses, vulnerabilities or errors, without the intention of reporting problems;
- (7) browsing, killing time by viewing data;
- (8) expressing boredom, revenge or disgruntlement;
- (9) perceiving a challenge: treating the system as a game to outwit;
- (10) acting with the intention of causing harm, for reasons such as fame, greed, capability, divided loyalty or delusion.

Additionally, Greitzer and Frinke (2010) identified several psychological indicators such as disgruntled, anger management issues and ignorance of authority, and in a case study about sabotage and espionage, common characteristics such as antisocial and narcissistic personalities have been identified (Moore, et. al, 2008).

These indicators mentioned above are just a small piece of the big picture. Harmful actions performed by insiders include espionage, sabotage (Gelles, 2005; Krofcheck & Gelles, 2005) or just accidental mistakes (Predd et al., 2008) or innocent errors (Salem, Hershkop, & Stolfo, 2008). Motivations of these actions are just as diverse as types of actions (Salem et al., 2008).

### 2.3.3 Environmental Factors

Predd argues that environment defines whether an action is legal or ethical and emphasizes punishment enforced by law (Nance & Marty,

2011). What's more, cultural differences and attitude toward what is appropriate will also affect bounds of insiders as well as definitions of malicious. For example, Edward Snowden appears to believe he was "doing the right thing" when he exposed NSA information.

As mentioned before, complex and dynamic of external environment will affect policy making as well as policy implementation (Hunker & Probst, 2011), as a result, affect incidents of insider attacks.

### 2.3.4 System

System is implemented policy (Predd et al., 2008) and techniques support, technically, the realization of security policy. Current techniques to mitigate insider threat include access control, monitoring, integrated approaches, trusted system and predicting model.

#### 2.3.4.1 Access Control

Access control has two aspects: authentication and authorization. Authentication defines who you are and authorization defines what you can do. However, access control has limitations such as it could not prevent users who are using legitimate privileges to behave as malicious insiders.

#### 2.3.4.2 Monitoring

This paper talks about two types of monitoring and several techniques to perform monitoring. These two types are misuse detection and anomaly detection.

Misuse detection and modeling identifies defined types of misuse through rule-based detection. But limitation is this method could only detect known type of insider attack. Framework to perform this includes finite state machine, petri nets or regular expression.

Anomaly Detection flags significant deviation from expected normal behavior as a proxy for unknown misuse. Method and theories used here include co-currence of multiple events, high-order of markov chain, naïve Bayesian network. Problems with monitoring includes no evidence as deterrent and violation of privacy.

#### 2.3.4.3 Integrated Approaches

Integrated approaches take combined several techniques together, including honey pots, network level sensor, physical logs, and model of insiders and pre-attack insiders to infer malicious intent.

#### 2.3.4.4 Trusted System

Key characteristic of trusted system is reference validation (Neumann, 2010): each execution could be tracked back to specific users. This characteristic makes trusted system as resistant to insiders as well as to outsiders. In operations, a trusted system is implemented by isolating executing privilege domains with less privilege domains, isolating one user's access from another user's access (Saltzer, 1974) or assigning user specific random domains (Neumann, 2010).

#### 2.3.4.5 Predicting Model

Predicting model uses system usage as predictors of insider attacks, such as inconsistent digital behaviors (Dimkov, 2011) and unusual access (Probst, 2009).

## 3. INTRODUCTION OF RESEARCH MODEL

In this section, we will first build our model based on the planned behavior theory and other related theories and research. Then constructs and their corresponding measures will be discussed.

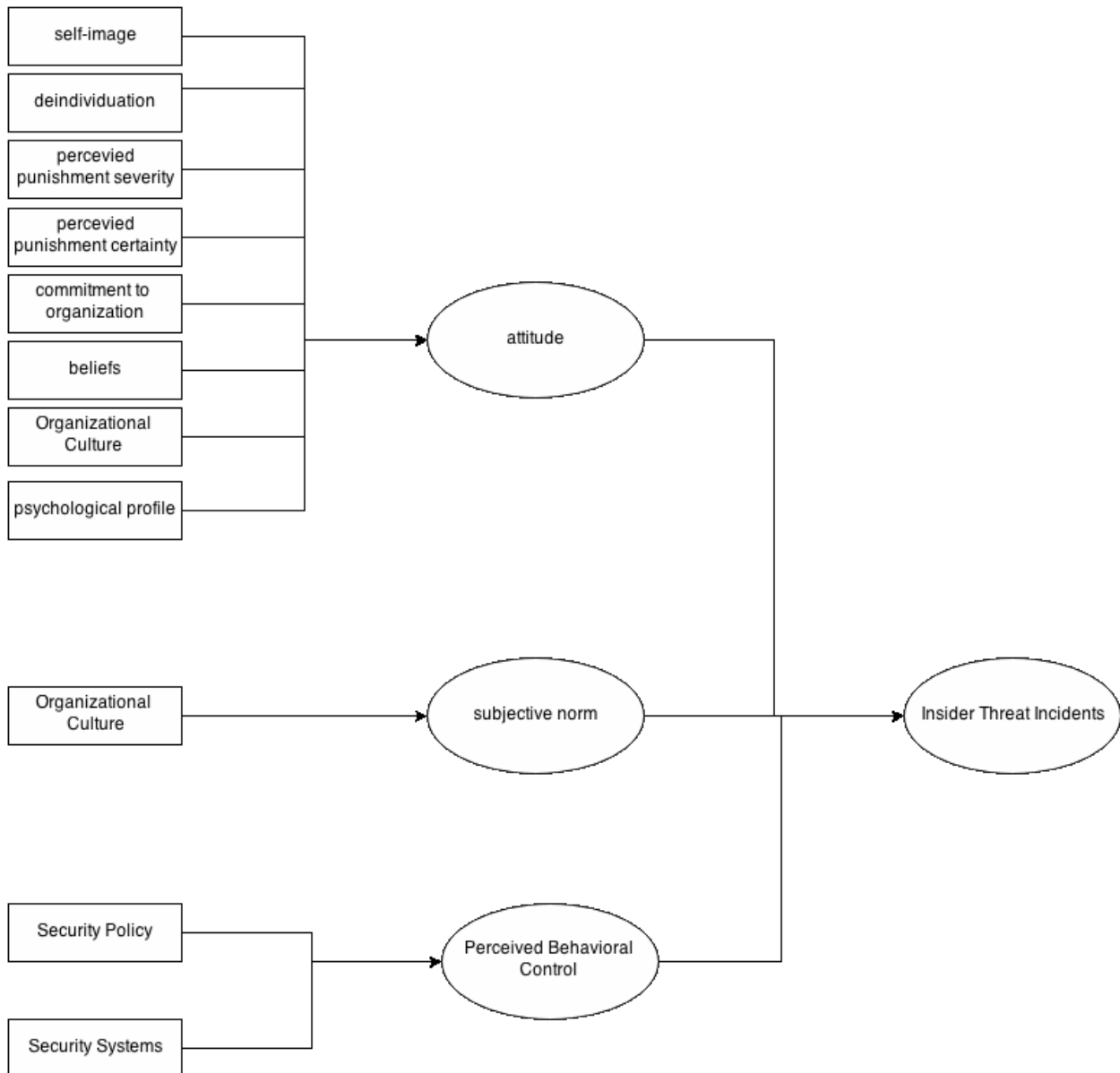
### 3.1 Model Derivation

There has been a considerable amount of work with respect to individual motivations in the literature. Researchers from various disciplines propose that the constructs depicted in the table are indicators of insider threat. As noted, our motivation is to validate those constructs.

Figure 2 shows our model derived from the Theory of Planned Behavior, in which insider threat incident behavior is preceded by three



constructs: attitude, subjective norm and perceived behavioral control.



**Figure 2: Research Model**

**3.1.1 Attitude**

Attitude refers to “the degree to which a person has a favorable or unfavorable evaluation or

appraisal of the behavior in question” (Ajzen, 1991).

Internal as well as insider’s perception about external factors would affect the insider’s attitude towards what he or she is doing or plan to do. From previous literature, factors affecting an insider’s attitude towards himself or herself include both internal and external factors:

### 3.1.1.1 Internal Factors

- (1) Self-image (Loch & Conger, 1996; Randall, 1989)
- (2) Deindividuation (Lee & Lee, 2002; Loch & Conger, 1996)
- (3) Commitment to organization (Dugo, 2007; Lee & Lee, 2002; Li, et al., 2010)
- (4) Beliefs (Loch & Conger, 1996; Vance, et al., 2012;)
- (5) Psychological Indicators (Greitzer & Frincke, 2010; Moore et al., 2008)

### 3.1.1.2 External Factors or Insider’s Perception about External Factors

- (1) Perceived punishment severity and perceived punishment certainty (Cox, 2012; Dugo, 2007; Ifinedo, 2012; Li, et al., 2010; Peace et al., 2003; Peach, et al., 2010; Son, 2011; Vance, et al., 2012)
- (2) Security culture (Hu et al., 2012)
- (3) Organizational culture (Cox, 2012; Hu et al., 2012)

### 3.1.2 Subjective Norm

Subjective norm is a social factor and refers to “perceived social pressure to perform or not to perform or not to perform the behavior” (Ajzen, 1991). Therefore, in the context of insider threat research, subjective norm is specified as how co-workers and senior works feel about insiders’ actions (Lee & Lee, 2002).

But in this research, we extend Lee’s scope of subjective norm to include influences from family or any other sources, not limited to influences exerted from workplaces.

### 3.1.3 Perceived Behavioral Control

Perceived behavioral control refers to people’s perception of the ease or difficulty of performing the behavior of interest (Ajzen, 1991).

Although in the theory of planned behavior, perceived behavioral control is one predictor of intention of behavior, actual level of behavioral control was also used as a predictor (Bulgurcu, Cavusoglu, & Benbasat, 2010). In Bulgurcu’s research, number of security staffs and number of security systems in use are used as predictor of IT security policy compliance behavior. Predicting power of actual behavioral control is also confirmed by Ajzen (1991), one of the builder of the theory of planned behavior, arguing perceived behavioral control serves as a proxy for actual behavioral control.

Factors affecting perceived behavioral control in existing research include:

- (1) punishment certainty (Peace et al., 2003)
- (2) security policy and security systems (Lee & Lee, 2002)
- (3) locus of control (Cox, 2012)

## 3.2 Definition of Constructs

There has been a considerable amount of work with respect to individual motivations in the literature. Researchers from various disciplines propose that the constructs depicted below. As noted, our motivation is to validate those constructs.

### 3.2.1 Self-image

In previous research, demographic characteristics of insiders include gender, age, education, socioeconomic status, religion, marriage status, professions and position in organization (Randall, 1989). And self-image is the characteristic an individual defines himself or herself (Loch & Conger, 1996). As argued by Loch & Conger, if an individual defines himself or herself by religion, he or she is mostly likely to comply with rules of that religion. Therefore, characteristic used by individual to define himself or herself serves as one measure of his or her attitude.

### 3.2.2 Deindividuation

Deindividuation is first defined as a feeling of “being estranged or separated from others that can lead to behavior violating established norms of appropriateness” (Zimbardo, 1969). What’s more, it is widely used in insider threat researches as an antecedent of insider threat (Lee & Lee, 2002; Loch & Conger, 1996). People with deindividuation has less interaction with others and will be less likely to perform socially accepted behaviors.

### 3.2.2 Perceived Punishment Severity/Certainty

If an individual’s perceived punishment severity is high and perceived probability to be discovered is high, he or she would perceived a high level of behavioral control.

### 3.2.3 Commitment to Organization/Beliefs

Commitment to organization refers to “one is committed to conformity by not only what one has but also what one hopes to attain” (Hirschi, 2002). And beliefs refer to strength of individual’s feeling about whether he or she should comply with organizational rules. Therefore, the more an individual is committed

to organization, the less likely he or she is to commit malicious threat to organization (Dugo, 2007; Lee & Lee, 2002).

### 3.2.4 Organizational Culture

Organizational culture refers to whether the organization is goal-oriented or rule-oriented. For a goal-oriented organization, insiders comply with organization by fulfilling organizational goals, however, rule-oriented organization requires insiders comply with procedures and regulations (Cox, 2012; Hu et al., 2012).

### 3.2.5 Security Policy and Systems

Security policy and security systems refer to official and implemented security policies in organization. Quality of security-whether stated policy covers potential risk emerging area-as well as implemented policy-how many security systems are used- will affect organizational security level (Hu et. al. 2012).

### 3.2.6 Psychological Indicators

Twelve psychological indicators are suggested by Greitzer & Frincke (2010) as shown in Table 1:

Table 1 Psychological Indicators

Indicator	Description
Disgruntlement	Employee observed to be dissatisfied in current position.
Accepting Feedback	The employee is observed to have a difficult time accepting criticism.
Anger Management Issues	The employee often allows anger to get pent up inside.
Disengagement	The employee keeps to self, is detached, withdrawn and tends not to interact with individuals or groups; avoid meetings.
Disregard for authority	The employee disregards rules, authority or policies.
Performance	The employee has received a corrective action based on poor performance.
Stress	The employee appears to be under physical, mental or emotional strain or tension that he or she has difficulty handling.
Confrontational Behavior	Employee exhibits argumentative or aggressive behavior or is involved in bullying or intimidation.
Personal Issues	Employee has difficulty keeping personal issues separate from work.
Self-Centeredness	The employee disregards needs or wishes of others, concerned primarily with own interests and welfare.
Lack of Dependability	Employee is unable to keep commitments or promises; unworthy of trust.
Absenteeism	Employee has exhibited chronic unexplained absenteeism.

## 4. Methodology

As noted above, previous research often focuses on preventing insider incidents as opposed to actually identifying malicious insiders. Further, while some malicious insider characteristics have been proposed, many have not had to stand the scrutiny of empirical investigation. We aim to close these gaps by using text mining and classification to exam third party data; namely past reports on captured malicious insiders and empirically examine their characteristics. Then we intend to use those empirically supported characteristics in an attempt to better predict and identify potential malicious insiders.

### 4.1 Data Sample

Data used in this study are mainly from two sources: public reports and previous research. We will begin by text mining public reports for keywords of name (the insider) involved in discovered insider incidents. Once we identify a satisfactory number of cases, we will then text-mine for indicators of the characteristics posited by previous research.

### 4.2 Research Methods

The method we propose to use in this research is based on the process introduced by Greitzer and Frincke (2010). In this process, data collected is first refined into observations and then these observations are clustered into different indicators. In this section, we first briefly introduce Greitzer and Frincke's information extraction model and then specify the process and method we will use in this research.

#### 4.2.1 Introduction of the Method

In Greitzer and Frincke's (2010) approach data in the form of text based reports is collected. *Data* represents direct available information about activities of individuals such as timecard

records, VPN login records and so on. When these data are collected, algorithms will be employed to calculate observations. Fuller, et. al. (2009) demonstrated how decision trees, neural networks, and logistic regression can be used in similar law enforcement cases.

Once the data is mined and classified, observations can be made. *Observations* are inferences from data to reflect a certain state. In previous example, timecard records (data) and VPN login could be used to calculate Time At Work (observation). From observations, indicators can be derived. *Indicators* are referred to actions or events that are precursors of a certain behavior. In previous examples, unusual late work hour (indicator) could be derived from time at work (observation).

#### 4.2.2 Extension of Previous Method

In this research, our interest has a wider perspective including but not limited to psychological indicators of malicious insiders as Greitzer and Frincke (2011) did. Therefore, we extend the scope in terms of data, observation and indicator, but stay with the framework.

We intend to use direct descriptions about extant malicious insiders from public reports, national or local media, and previous research as raw data in our current study. These unstructured data are processed into structural observations using information extraction text-mining. In this process, heuristic methods are employed: we mine and extract descriptions of malicious insiders and refined them into observations (a reflection of certain characteristic or state of insider), then the next piece of data is processed. If the observation extracted from data already exists (i.e., has already been identified), then a new record of that observation is added to the others. However, if the item has not yet been observed then a new observation will be created and recorded.

A major difference between our method and Greitzer's method is that indicators in our research are not refined and extracted from observations, but instead they are predefined by previous research. Therefore, observations are clustered into indicators specified in Section 3

using clustering text mining techniques. However, we note that having predefined observations will not preclude use from identifying potential new observations, and we expect to find some. Modern text mining and classification techniques are quite powerful and can yield results not found by human observation (Fuller, et al., 2011).

## **Conclusion**

The problem of malicious insider threat is of concern to practitioners and academic alike, yet the phenomenon has yet to be significantly examined beyond the domains of psychology and criminal science where mainly human observation is the only means of data collection. We aim to employ a form of data mining, namely text mining along with observation classification to expand and aggregate finding from multiple historical insider threat cases. In doing so, we believe we can develop better indicators for identifying the characteristics of malicious insiders. However, our work has just begun. Our next step is to collect cases of malicious insider threat and all reports and articles covering each case. Then, we will employ our text-mining and classification techniques identified above to validate the indicators derived from previous research and possibly identify additional indicators. Finally, we hope to build a common set of validated indicators of malicious insiders. We hope this proposed method will garner discussion and endorsement from other researchers pursuing and solution to the insider threat problem.

## REFERENCES

- [1]Adkins, M., Twitchell, D. P., Burgoon, J. K., & Nunamaker Jr, J. F. (2004). *Advances in automated deception detection in text-based computer-mediated communication*. Paper presented at the Defense and Security.
- [2]Ajzen, I. (1985). *From intentions to actions: A theory of planned behavior*: Springer.
- [3]Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes*, 50(2), 179-211.
- [4]Anderson, R. H. (1999). Research and Development Initiatives Focused on Preventing, Detecting, and Responding to Insider Misuse of Critical Defense Information Systems: DTIC Document.
- [5]Bellovin, S. M. (2008). The insider attack problem nature and scope *Insider Attack and Cyber Security* (pp. 1-4): Springer.
- [6]Bishop, M., Engle, S., Peisert, S., Whalen, S., & Gates, C. (2009). *Case studies of an insider framework*. Paper presented at the System Sciences, 2009. HICSS'09. 42nd Hawaii International Conference on.
- [7]Bishop, M., & Gates, C. (2008). *Defining the insider threat*. Paper presented at the Proceedings of the 4th annual workshop on Cyber security and information intelligence research: developing strategies to meet the cyber security and information intelligence challenges ahead.
- [8]Bishop, M., Gollmann, D., Hunker, J., & Probst, C. W. (2008). *Countering insider threats*. Paper presented at the Dagstuhl Seminar.
- Brackney, R. C., & Anderson, R. H. (2004). Understanding the Insider Threat. Proceedings of a March 2004 Workshop: DTIC Document.
- [9]Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *Mis Quarterly*, 34(3), 523-548.
- [10]Chinchani, R., Iyer, A., Ngo, H. Q., & Upadhyaya, S. (2005). *Towards a theory of insider threat assessment*. Paper presented at the Dependable Systems and Networks, 2005. DSN 2005. Proceedings. International Conference on.
- [11]Cox, J. (2012). Information systems user security: A structured model of the knowing-doing gap. *Computers in Human Behavior*, 28(5), 1849-1858.
- [12]De Cremer, D. (2006). Unfair treatment and revenge taking: The roles of collective identification and feelings of disappointment. *Group Dynamics: Theory, Research, and Practice*, 10(3), 220.
- [13]Dugo, T. (2007). The insider threat to organizational information security: a structural model and empirical test.
- [14]Flegel, U., Vayssiere, J., & Bitz, G. (2010). A state of the art survey of fraud detection technology *Insider Threats in Cyber Security* (pp. 73-84): Springer.
- [15]Fuller, C. M., Marett, K., & Twitchell, D. P. (2012). An examination of deception in virtual teams: Effects of deception on task performance, mutuality, and trust. *Professional Communication, IEEE Transactions on*, 55(1), 20-35.
- [16] Fuller, C.M., Biros, D.P. and Wilson R.L., "Decision Support for Determining Veracity via Linguistic Based Cues," *Decision Support Systems*, 46, 2009, 695-703.
- [17] Fuller, C., Biros, D., Delen, D. "Data and Text Mining methods applied to the task of Detecting Deception in Real World Crime Investigation Records," *Expert Systems with Applications*, June 2011
- [18]Gelles, M. (2005). Exploring the mind of the spy. *Employees' guide to security responsibilities: Treason*, 101.
- [19]Greitzer, F. L., & Frincke, D. A. (2010). Combining traditional cyber security audit data with psychosocial data: towards predictive modeling for insider threat mitigation *Insider Threats in Cyber Security* (pp. 85-113): Springer.
- Hayden, M. (1999). The insider threat to US government information systems: DTIC Document.
- [20]Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for

security policy compliance in organisations. *European Journal of Information Systems*, 18(2), 106-125.

[21]Hirschi, T. (2002). *Causes of delinquency*: Transaction publishers.

Hollinger, R. C. (1993). Crime by computer: Correlates of software piracy and unauthorized account access. *Security Journal*, 4(1), 2-12.

[22]Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture\*. *Decision Sciences*, 43(4), 615-660.

[23]Hunker, J., & Probst, C. W. (2011). Insiders and insider threats—an overview of definitions and mitigation techniques. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 2(1), 4-27.

[24]Kankanhalli, A., Teo, H.-H., Tan, B. C., & Wei, K.-K. (2003). An integrative study of information systems security effectiveness. *International journal of information management*, 23(2), 139-154.

[25]Krofcheck, J., & Gelles, M. (2005). Behavioral consultation in personnel security: Training and reference manual for personnel security professionals. *Yarrow Associates, Fairfax, Virginia*.

[26]Lee, J., & Lee, Y. (2002). A holistic model of computer abuse within organizations. *Information Management & Computer Security*, 10(2), 57-63.

[27]Lee, S. M., Lee, S.-G., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management*, 41(6), 707-718.

[28]Li, H., Zhang, J., & Sarathy, R. (2010). Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems*, 48(4), 635-645.

[29]Loch, K. D., & Conger, S. (1996). Evaluating ethical decision making and computer use. *Communications of the ACM*, 39(7), 74-83.

[30]Moore, A. P., Cappelli, D. M., & Trzeciak, R. F. (2008). *The “big picture” of insider IT sabotage across US critical infrastructures*: Springer.

[31]Nance, K., & Marty, R. (2011). *Identifying and visualizing the malicious insider threat using bipartite graphs*. Paper presented at the System Sciences (HICSS), 2011 44th Hawaii International Conference on.

[32]Parker, D. B., & Parker, D. (1976). *Crime by computer*: Scribner New York.

[33]Peace, A. G., Galletta, D. F., & Thong, J. Y. (2003). Software piracy in the workplace: A model and empirical test. *Journal of Management Information Systems*, 20(1), 153-178.

[34]Pfleeger, C. P. (2008). Reflections on the insider threat *Insider Attack and Cyber Security* (pp. 5-16): Springer.

[35]Predd, J., Pfleeger, S. L., Hunker, J., & Bulford, C. (2008). Insiders behaving badly. *IEEE Security & Privacy*, 6(4), 0066-0070.

[36]Probst, C. W., Hunker, J., Gollmann, D., & Bishop, M. (2010). Aspects of Insider Threats *Insider Threats in Cyber Security* (pp. 1-15): Springer.

[37]Randall, D. M. (1989). Taking stock: Can the theory of reasoned action explain unethical conduct? *Journal of Business Ethics*, 8(11), 873-882.

[38]Randazzo, M. R., Keeney, M., Kowalski, E., Cappelli, D., & Moore, A. (2005). Insider threat study: Illicit cyber activity in the banking and finance sector: DTIC Document.

Salem, M. B., Hershkop, S., & Stolfo, S. J. (2008). A survey of insider attack detection research *Insider Attack and Cyber Security* (pp. 69-90): Springer.

[39]Shaw, E. D., Post, J. M., & Ruby, K. G. (1999). Inside the Mind of the Insider. *Security Management*, 43(12), 34.

[40]Skinner, W. F., & Fream, A. M. (1997). A social learning theory analysis of computer crime among college students. *Journal of research in crime and delinquency*, 34(4), 495-518.

[41]Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security*, 24(2), 124-133.

[42]Stolfo, S. J., Bellovin, S. M., Hershkop, S., Keromytis, A. D., Sinclair, S., & Smith, S. (2008). *Insider attack and cyber security: beyond the hacker* (Vol. 39): Springer.

[43]Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: security planning models for management decision making. *Mis Quarterly*, 441-469.

[44]Vance, A., Siponen, M., & Pahlila, S. (2012). Motivating IS security compliance: insights from habit and protection motivation theory. *Information & Management*, 49(3), 190-198.

[45]Wood, B. (2000). An insider threat model for adversary simulation. *SRI International, Research on Mitigating the Insider Threat to Information Systems*, 2, 1-3.

[46]Zimbardo, P. G. (1969). *The human choice: Individuation, reason, and order versus deindividuation, impulse, and chaos*. Paper presented at the Nebraska symposium on motivation.

[47] Dimkov, T., Pieters, W., & Hartel, P. (2011). Portunes: representing attack scenarios spanning through the physical, digital and social domain. In *Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security* (pp. 112-129). Springer Berlin Heidelberg.

[48] Probst, C. W., & Hansen, R. R. (2009, May). Analysing access control specifications. In *Systematic Approaches to Digital Forensic Engineering, 2009. SADFE'09. Fourth International IEEE Workshop on* (pp. 22-33). IEEE.



