Malicious Insiders: Who Might Be the Ephialtes in Your Organization?

Nan (Peter) Liang
nan.liang@okstate.edu

David Biros
david.biros@okstate.edu

Abstract - Malicious insiders continue to post great threats to organizations. With their knowledge about organization and access to organizational resources, malicious insiders could bypass security countermeasures easily and result in devastating consequences. In this study we compare 30 malicious insiders with 30 benign insiders with respect to the personality and other psychometrics. We found that avoidant personality, antisocial personality and disruptive mood differentiate malicious insiders with the benign ones. Also, if an insider is both narcissistic and disgruntled, he / she tends to launch the malicious attack. The implication for this research has two aspects: first, we validated the characteristics of malicious insiders proposed by previous research, second, the findings suggest that organizations should be more sensitive to employees who exhibit certain behavioral precursors.

Categories and Subject Descriptors

K.5.2 [Legal Aspects of Computing]: Governmental Issues – Regulation.

General Terms

Legal Aspects, Security

Keywords

Malicious Insiders, Text Mining, Cyber Security, Characteristics

1. BACKGROUND

Malicious insider threat is nothing new. In 480 BC, Ephialtes betrayed his homeland and led the invaders through a path to attack Spartan forces from behind, resulting the failure of King Leonidas and the fall of Spartan[1]

In a 2016 Information Systems Audit and Control Association (ISACA) survey of nearly 3000 security professionals, insider threat is the third most organizational security concern among domestic companies and the second most among international respondents. Insiders are legitimately empowered to access, represent and manipulate organization's resources [1] therefore they know the valuable assets of the organization as well as the weak points of the organization's information security posture [2]. As a result, once the insiders turn malicious, it's not only much easier for them to launch the attack, but also could result in more devastating consequences with respect to financial loss, disruption to organization, damage to reputation as well as long term impact to organizational culture [3].

The problem of malicious insiders has drawn plenty of attention. The US Secret Service and Carnegie Mellon University conducted a series of studies in this area [4, 5]. Also, the U.S. Department of Defense's Personnel Security Research Center (PERSEREC) released series of reports for espionage cases in the United States [6]. In the UK, the Center for the Protection of National Infrastructure also put malicious insiders' threat as high priority and incorporated the malicious insider study into security planning and security education [7].

However, the current research only looks at the group of malicious insiders and investigate the common characteristics of malicious insiders as well as malicious attack, without comparing them with the benign insiders. We argue that this might result in a major problem: the common characteristic of malicious insiders might not be the characteristics that differentiate them with benign insiders.

---

[1] Herodotus, 480 BC

One potential problem is the lack of data [8] because organizations are reluctant to release data about malicious insider threat as for the fear of reputation [9]. In this study, we collect data from publicly available sources including newspaper report, court document and biography on notorious malicious insiders, in order to empirically test these characteristics proposed by previous research. Our comparison group is randomly selected from founders of Fortune 500 companies to represent the benign insiders. The underlying rationale is that founders won't build a company so he / she could attack it.

The rest of this paper will be arranged as following: in the next section, we will briefly review characteristics of malicious insiders proposed by previous research. Then we will describe our data source and methodology. After that, we will present our observations from the sample and at last, we will discuss the implications of this research for organizational security practice. Finally, the limitations and future research will be discussed.

2. RELATED WORK

In this section, we will review previous research about malicious insiders' characteristics. There are plenty of characteristics proposed by literature. With respect to personality and psychometrics, the most common characteristics are personality disorder, emotional and mood indicators and workplace disgruntlement. A more comprehensive review of the relevant literature can be found at Liang & Biros's work [10]. Here, we focus on the more significant characteristics.

2.1 Personality disorder

Personality disorders includes classic Axis II personality disorders [APA 1994], such as antisocial personality disorder [11], narcissistic personality disorder [6, 11, 12], and psychopathy [11]. Specifically, the immature malicious insiders [7] with the sense of entitlement [4, 13, 14] and grandiosity [15] tend to have an inappropriate sense of self-importance or self-esteem [15, 16] such as Machiavellianism [13, 17] and engage in unrealistic fascination about spy work, imaginary activities [7], power or reputation [13].

2.2 Emotional Indicators

Malicious insiders are suggested to be emotionally unstable [7] and might react to work-related issues negatively instead of constructively, such as feeling of being betrayed or isolated and fear of being excluded [13]. As a result of their inappropriate feelings, they might exhibit anger [4], poor work attitude or being stressed. However, some research states that instead of feeling negatively, malicious insiders might seek sensation as emotional response [13].

2.3 Disgruntlement

Some studies [13, 18] argue that malicious insiders are typically disgruntled employees. Also, a as study examining the Department of Agriculture and IT sabotage in the US critical infrastructure proposes disgruntlement as a potential indicator of malicious insiders. The disgruntlement might be result of unmet expectations [19], lack of appreciation and feelings of injustice or inequality [13].

In this section, we briefly review the relevant literature about characteristics of malicious insiders, in the next section, we will describe our data and our method to assess subjects in order to extract and measure these characteristics.

3. DATA AND METHODOLOGY

3.1 Sampling Criteria

The malicious insiders to be analyzed in this study are drawn from malicious insiders population who were convicted by US courts from 2000 to 2015. Malicious attacks of these convicted include spying, espionage, economic espionage, illegal exports and other security related acts. Due to the infrequency of malicious insider cases, previous research suggests that it is impractical to draw a random sample [4]. In the current study, we utilize the eminence criterion proposed by Simonton [20] to select the sample (n=30). With respect to benign insiders, we randomly select a sample of 30 from founders of Fortune 500 companies. The final dataset contains 60 subjects with the same number of malicious insiders and benign insiders.

3.2 Methodology

After defining our sample, we go through four steps to collect as well as analyze the data. In the first step, we use google search to collect all relevant documents related to a specific subject. Then, we read through documents of malicious insiders as well as previous research and extract all descriptors in these documents describing the subjects. After that, we classify these descriptors to symptoms defined by Diagnostic and Statistical Manual [13] of Mental Disorders [13]. Then, linguistic Inquiry and Word Count (LIWC) software is used to analyze the documents [21] is used to scan and count the number of descriptors and number of corresponding symptoms presented in the portfolio of each subject. Finally, diagnostic criteria defined in DSM is used to assess the mental disorders of subjects. For the purpose of illustration, examples of the symptoms defined in DSM are summarized in table 1.

Table 1: Disorders and symptoms defined in DSM

Disorder	Symptom	Description
Antisocial Personality Disorder	AS1	Failure to conform to social norms with respect to lawful behaviors.
	AS2	Deceitfulness, as indicated by repeated lying, use of aliases, or conning others for personal profit or pleasure
	AS3	Impulsivity or failure to plan ahead
Narcissistic Personality Disorder	NPD1	Has a grandiose sense of self-importance (e.g. Exaggerates achievements and talents, expects to be recognized as superior without commensurate achievements)

Table 1: Disorders and symptoms defined in DSM		
Disorder	**Symptom**	**Description**
	NPD2	Is preoccupied with fantasies of unlimited success, power, brilliance, beauty or ideal love
	NPD3	Believes he or she is special and unique and can only be understood by, or should associate with, other special or high status people (or institution)
Avoidant Personality Disorder	APD1	Avoids occupational activities that involve significant interpersonal contact because of fears of criticism, disapproval or rejection
	APD2	Is unwilling to get involved with people unless certain of being liked
	APD3	Shows restraint within intimate relationships because of the fear of being shamed or ridiculed
Disruptive Mood Dysregulation Disorder	DMDD1	Severe recurrent tempter outbursts manifested verbally and / or behaviorally (e.g. physical aggression toward people or property) that are grossly out of proportion in intensity or duration to the situation or provocation
	DMDD2	The temper outburst are inconsistent with developmental level

Table 1: Disorders and symptoms defined in DSM		
Disorder	**Symptom**	**Description**
	DMDD3	The temper outbursts occur, on average, three or more times per week
Note: AS: Antisocial Personality Disorder; NPD: Narcissistic Personality Disorder APD: Avoidant Personality Disorder DMDD: Disruptive Mood Dysregulation Disorder		

In this section, we described our data and method. In the next part, we will present our observations of the sample.

4. OBSERVATIONS

As aforementioned method, in the current study we measure narcissistic personality, avoidant personality, antisocial personality and disruptive mood dysregulation by number of symptoms exhibited by subjects, and mental disorder diagnosis is made based on DSM diagnosis criteria. The insights from our samples are listed as follows:

Observation #1: The prevalence of avoidant personality disorder in malicious insiders is higher than in the benign insiders.

Observation #2: The prevalence of antisocial personality disorder in malicious insiders is higher than in the benign insiders.

Observation #3: The prevalence of disruptive mood dysregulation disorder in malicious insiders is higher than in the benign insiders.

Observation #4: The prevalence of disgruntlement in malicious insiders is NOT higher than in the benign insiders. However, the co-occurrence of disgruntlement

and narcissistic personality disorder in malicious insiders are higher than in benign insiders.

In this section, we will discuss these four observations in details. For each observation, we first discuss its rationale which takes a relatively large proportion of all subjects. Then we present a case example for the corresponding observation. A summary of all observations is presented in table 2:

Table 2: Summary of observations

	# of Disgruntled and NPD	# of DMDD	# of AS	# of APD
Malicious	5	9	14	4
Benign	1	4	3	1

4.1 Observation #1: The prevalence of avoidant personality disorder in malicious insiders is higher than in the benign insiders.

Among the malicious subjects, 4 have avoidant personality disorder compared to only 1 case of avoidant personality disorder in the benign insiders. Avoidant personality disorder is characterized by social inhibition and unwillingness to get involved with people [APA, 1994]. However, teamwork is important in organizations and social skills are essential in team settings [22]. The inability to work and communicate effectively with others decreases the odds of confronting colleagues with legitimate work-related complaints [4]. Additionally, once the employee experiences stressful personal or work-related events such as demotion or death of significant others [4, 13], isolation resulting from avoidant personality disorder jeopardizes the possibility that they could solve problems constructively [6]. Instead, they might engage in more destructive behavior and launch an insider attack.

Case Example of Avoidant Personality Disorder[2]

One subject, Bradley Manning, served in the U.S. Army at the time of the malicious incident. He leaked nearly three quarters of a million classified or sensitive information and diplomatic documents to WikiLeaks. Manning was dishonorably discharged from the Army and as sentenced to 35 years' imprisonment in August 2013.

Manning has as a gender identity disorder since he was 13. Also, he contacted a gender counselor while serving in the Army. Manning described the experience in military with the gender identity disorder as "great pain" in his email to his supervisor while in the Army. However, Manning was fragile and isolated in the army. As described by his former colleague, he lacked social skills and felt he "could not please anyone", resulting his isolation in the Army. The frustrating situation for Manning was worsened by the "Don't ask, Don't tell" policy in the military and she could not communicate with others or express herself for his problem.

His isolation and the resulting avoidance from others contributed to his violation of military regulation to leak classified information. As stated by Manning in 2010, he felt "isolated and fragile, and was reaching out to someone he hoped might help".

4.2 Observation #2: The prevalence of antisocial personality disorder in malicious insiders is higher than in the benign insiders.

Fourteen out of 30 malicious insiders in our sample have antisocial personality disorder however, only 3 subjects in the benign insiders are observed to have this. If individuals have antisocial personal disorders which is defined as a "pervasive disregard for the law and the rights of others" [23], they tend to aim at whatever they want, no matter whether it is illegal or others might be hurt. Since these insiders know more about the organization [1], and it's hard for them to form

[2] Case is summarized from Wikipedia, https://en.wikipedia.org/wiki/Chelsea_Manning, last assess date, April 09th, 2016

attachment and loyalty to the organization [15], they are prone to attack the organization from inside.

Case Example of Antisocial Personality Disorder[3]

Robert Hanssen spied for Soviet Union and then Russian against United States for 22 years until 2001, resulting in the failure of dozens of intelligence operations and the deaths of CIA assets. In 2001, he was sentenced to 15 life terms without the possibility of parole. Hanssen is a living example of antisocial personality. He had affair with a stripper, failed to obey social norms and the loyalty to his wife. He used to recklessly race his car, ignored the safety of himself as well as others. He even secretly videotaped his sexual activity with his wife and shared them with his colleague, disregard the feeling and welfare of his spouse.

Hanssen's antisocial personality makes him disregard laws and regulations, and he had no remorse after his arrest. He described his activities as part of a "spy game" and shows no regret for what he did.

4.3 Observation #3: The prevalence of disruptive mood dysregulation disorder in malicious insiders is higher than in the benign insiders.

Among the malicious subjects, 9 show evidence of disruptive mood dysregulation disorder (DMDD) symptoms, compared to only 4 cases in the benign insiders group. DMDD is one type of mental health disorder which is featured by persistently outburst of temper or often irritable mood [APA, 2013]. DMDD [23] is structurally linked to emotion regulation and is highly associated with negative emotional response such as emotional instability or bursts of anger [24]. Studies about malicious insiders report high correlation between the presence of emotional dysregulation and malicious intent [25].

[3] Case is summarized from Wikipedia, https://en.wikipedia.org/wiki/Robert_Hanssen, last assessed April 08, 2016

Case Example of Disruptive Mood Dysregulation Disorder[4]

Terry Child was a network administrator working for the City of San Francisco. He is distinguished people as Cisco Certified Internetworking Engineer and Childs shares this distinction with less than 20,000 people world-wide. He was mainly in charge of building and managing the FiberWAN network, a city-wide complex network which is the core of all city services. As a dedicated engineer and the sole administrator of the network, Childs was described as on call for 7-24-365. However, when his supervisor asked him to share the password of the network, he shut down the network and wiped out the network configurations, resulting in a huge loss for the city.

Child always loses his temper at work, based on the report we cited, he will get "red in his face whenever" he talked about his department. Also, his colleagues described him as "having a bad temper", and the bad temper put him in a terrible relationship with his supervisor. Child was seen belligerently confronting his supervisor and colleagues on many occasions.

The defensive character of Child and his always emotional mood cause him to overact when his supervisor asked him to share the password. Instead of solving the problem in a constructive manner, he took an unprofessional action and locked down the network.

4.4 Observation #4: The prevalence of disgruntlement in malicious insiders is NOT higher than in the benign insiders. However, the co-occurrence of disgruntlement and narcissistic personality disorder in malicious insiders is higher than in benign insiders.

In our samples, 50 out of 60 subjects expressed dissatisfaction in their job. However, almost half of them quit their job and started a new company while the

[4] Case is summarized from the InfoWorld report, http://www.infoworld.com/article/2653004/misadventures/why-san-francisco-s-network-admin-went-rogue.html, last assessed April 08, 2016

other half attacked the organization from the inside. This show that disgruntlement alone could not differentiate malicious insiders with benign insiders. However, the number of malicious subjects who are disgruntled at work and have narcissistic personality disorder as well is 5, compared to only 1 case in the benign insiders group.

Narcissistic personality disorder is characterized by grandiosity and sense of entitlement [APA, 1994]. One with the sense of grandiose and superiority typically believes that they possess unparalleled skills or talent [15], and with their self-perceived abilities, they are prone to fantasize about power, success, and attractiveness [11], as well as perceive themselves as deserving special, or preferential, treatment [6]. If the narcissistic insiders are disgruntled, their craving for admiration and special attention cannot be met, they might seek validation and affirmation of their self-importance from other sources such as competitors or opponents [15]. Even if they don't seek ego fulfillment themselves, their eagerness for recognition subjects them to showboating and manipulation [6].

Case Example of Both Disgruntlement and Narcissistic Personality Disorder[5]

Aldrich Ames, who becomes notorious after his arrest, was first evaluated as an "enthusiastic employee at the beginning of his CIA career. As recognition for his outstanding performance, he eventually gained top-level security clearances and access to countless classified intelligence materials. Ames is now serving a life sentence without the possibility of parole.

Ames's narcissistic personality made him believe that he is above the law and would never been caught. His feeling of grandiosity contributed to his compromise of classified materials. One time when he was on the way to see a CIA contact, he even left the briefcase containing information about this contact on the subway train. Besides the narcissistic personality, Ames was also disgruntled after he was

[5] Case is summarized from Weiner, T., D. Johnston, and N.A. Lewis, Betrayal: The Story of Aldrich Ames, an American Spy. 2014: Random House.

passed over for a promotion. His colleague described him as "being pushed from one extreme to another" because of the frustrated ambition.

5. IMPLICATIONS FOR ORGANIZATION'S SECURITY PRACTICES

The ultimate goal of malicious insider research is to predict and prevent malicious insider attacks. In the previous section, we could see insiders with certain characteristics tend to attack the organization from inside. However, to apply these findings to organization's security practice requires extra caution. In the following sections, we make some suggestions for security practice, but with do so with caution. To be noted, human behavioral pattern is so complex that even insiders with all these aforementioned "dangerous" characteristics will not necessary turn against organization. Our purpose, with respect to organization's security practice, is to provide a framework to red flag potential malicious insiders and to facilitate organizational intervention, in order to effectively communicate with them and to help them to address their problems constructively.

5.1 We should pay extra attention to the antisocial employees

Antisocial personality is characterized by unethical behavior, deceitfulness, irresponsibility and inconsiderate of others [APA, 2015]. This kind of employee is dangerous in a team therefore organizations should be cautious about them. In case of presence, these kinds of employees should raise red flags.

5.2 We should communicate with avoidant employees

Avoidant personality could possibly be observed in several ways, such as unwilling to get involved with people, taking criticism personal or reluctant to take occupational activities [APA, 2015]. In organization, managers should not only monitor the outcome of work, but also pay attention to the situation of our employees. If avoidant personality is present, it is strongly recommended that managers effectively communicate with such employees to help them to fit in.

5.3 We should have effective channel for employees to legitimate express their complaint

Job dissatisfaction alone would not indicate a potential insider attack, however, when the disgruntlement becomes radical and finally turns into outburst, it should raise the attention of organization. One way to prevent this is to establish effective grievance channel in order to let employees express themselves legitimately.

5.4 Narcissism is a double edged sword

Narcissistic alone might not be destructive. Research even show narcissism is relatively prevalent among presidents of the United States [27]. It instills confidence. However, in cases where narcissism and disgruntlement are exhibited together, problems could occur.

6. LIMITATIONS, FUTURE DIRECTIONS AND DISCUSSION

Although we analyzed 60 subjects in the current study, the sample size is still relatively small compared to the complexity of the problem. In the future, we will gather more data points from various sources therefore provide more support for our analysis. We see this study as a proof of concept. Another limitation is associated with the characteristic extraction procedure. In the current study, descriptors of malicious insiders are directly associated with symptoms. However, the same descriptors might have different meaning in different linguistic context. For example, "entitled" might mean the subject feels entitled or the document mentioned a book entitled with a book name. The problem is corrected manually in the current research. In the future, we are going to build rule based extraction procedure, such as "combination: {third personal pronoun} + {synonym of feel} + entitled", in order to increase extraction accuracy.

In this study we examined open source data to determine if malicious insiders exhibit certain characteristics more than benign insiders and found considerable support for our findings. To date, the study of malicious insiders has been limited to individual cases or small samples. However, by examining larger groups of malicious insiders we believe that common characteristics can be identified and

strategies to mitigate this threat can be developed. Because the impact of a malicious insider incident can be quite high, we believe continued research in this domain is a necessity.

REFERENCES

[1] Bishop, M. and C. Gates. Defining the insider threat. in 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. 2008. ACM.

[2] Willison, R. and M. Warkentin. Motivations for employee computer crime: understanding and addressing workplace disgruntlement through the application of organisational justice. in Proceedings of the IFIP TC8 International Workshop on Information Systems Security Research. International Federation for Information Processing. 2009.

[3] Hunker, J. 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, 2011. 2(1): p. 4-27.

[4] Band, S.R., et al., Comparing insider IT sabotage and espionage: A model-based analysis. 2006, DTIC Document.

[5] Shaw, E., K. Ruby, and J. Post, The insider threat to information systems: The psychology of the dangerous insider. Security Awareness Bulletin, 1998. 2(98): p. 1-10.

[6] Shaw, E.D. and L.F. Fischer, Ten tales of betrayal: The threat to corporate infrastructure by information technology insiders analysis and observations. 2005, DTIC Document.

[7] CPNI, CPNI INSIDER DATA COLLECTION STUDY: Report of Main Findings. 2013.

[8] Noy, N.F. and D.L. McGuinness, Ontology development 101: A guide to creating your first ontology. 2001, Stanford knowledge systems laboratory technical report KSL-01-05 and Stanford medical informatics technical report SMI-2001-0880.

[9] Willison, R. and M. Warkentin, Beyond deterrence: An expanded view of employee computer abuse. Mis Quarterly, 2013. 37(1): p. 1-20.

[10] Liang, N. and D. Biros. Validating Common Characteristics of Malicious Insiders: Proof of Concept Study. in 2016 49th Hawaii International Conference on System Sciences (HICSS). 2016. IEEE.

[11] Shechter, O.G. and E.L. Lang, Identifying Personality Disorders that are Security Risks: Field Test Results. 2011, DTIC Document.

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

[13] Nurse, J.R., et al. Understanding insider threat: A framework for characterising attacks. in Security and Privacy Workshops (SPW), 2014 IEEE. 2014. IEEE.

[14] Shaw, E.D. and H.V. Stock, Behavioral risk indicators of malicious insider theft of intellectual property: Misreading the writing on the wall. White Paper, Symantec, Mountain View, CA, 2011.

[15] Gelles, M., Exploring the mind of the spy. Employees' guide to security responsibilities: Treason, 2005. 101.

[16] Turner, J.T. and M. Gelles, Threat assessment: A risk management approach. 2012: Routledge.

[17] Maasberg, M., J. Warren, and N.L. Beebe, The Dark Side of the Insider: Detecting the Insider Threat Through Examination of Dark Triad Personality Traits.

[18] Greitzer, F.L., et al., Predictive modelling for insider threat mitigation. Pacific Northwest National Laboratory, Richland, WA, Tech. Rep. PNNL Technical Report PNNL-60737, 2008.

[19] Moore, A.P., D.M. Cappelli, and R.F. Trzeciak, The "big picture" of insider IT sabotage across US critical infrastructures. 2008: Springer.

[20] Simonton, D.K., Significant samples: The psychological study of eminent individuals. Psychological Methods, 1999. 4(4): p. 425.

[21] Pennebaker, J.W., M.E. Francis, and R.J. Booth, Linguistic inquiry and word count: LIWC 2001. Mahway: Lawrence Erlbaum Associates, 2001. 71: p. 2001.

[22] Morgeson, F.P., M.H. Reider, and M.A. Campion, Selecting individuals in team settings: The importance of social skills, personality characteristics, and teamwork knowledge. Personnel psychology, 2005. 58(3): p. 583-611.

[23] Association, A.P., Diagnostic and statistical manual of mental disorders, text revision (DSM-IV-TR). 2000: American Psychiatric Association.

[24] Etkin, A. and T.D. Wager, Functional neuroimaging of anxiety: a meta-analysis of emotional processing in PTSD, social anxiety disorder, and specific phobia. American Journal of Psychiatry, 2007. 164(10): p. 1476-1488.

[25] Greitzer, F.L., et al., Psychosocial modeling of insider threat risk based on behavioral and word use analysis. e-Service Journal, 2013. 9(1): p. 106-138.

[26] Weiner, T., D. Johnston, and N.A. Lewis, Betrayal: The Story of Aldrich Ames, an American Spy. 2014: Random House.

[27] Simonton, D.K., Presidential personality: biographical use of the Gough Adjective Check List. Journal of Personality and Social Psychology, 1986. 51(1): p. 149.