Curiosity Killed the Organization: A Psychological Comparison between Malicious and Non-Malicious Insiders and the Insider Threat

Marc Dupuis
University of Washington
Box 358534
Bothell, Washington 98011
marcjd@uw.edu

Samreen Khadeer
University of Washington
Box 358534
Bothell, Washington 98011
samreen@uw.edu

ABSTRACT
Insider threats remain a significant problem within organizations, especially as industries that rely on technology continue to grow. Traditionally, research has been focused on the malicious insider; someone that intentionally seeks to perform a malicious act against the organization that trusts him or her. While this research is important, more commonly organizations are the victims of non-malicious insiders. These are trusted employees that are not seeking to cause harm to their employer; rather, they misuse systems—either intentional or unintentionally—that results in some harm to the organization. In this paper, we look at both by developing and validating instruments to measure the behavior and circumstances of a malicious insider versus a non-malicious insider. We found that in many respects their psychological profiles are very similar. The results are also consistent with other research on the malicious insider from a personality standpoint. We expand this and also find that trait negative affect, both its higher order dimension and the lower order dimensions, are highly correlated with insider threat behavior and circumstances. This paper makes four significant contributions: 1) Development and validation of survey instruments designed to measure the insider threat; 2) Comparison of the malicious insider with the non-malicious insider; 3) Inclusion of trait affect as part of the psychological profile of an insider; 4) Inclusion of a measure for financial well-being, and 5) The successful use of survey research to examine the insider threat problem.

Keywords
Insider threat; malicious insiders; non-malicious insiders; governance; risk management; compliance; intentional acts; unintentional acts; personality; trait affect; psychological factors; human factors; cyber security; organizational security.

1. INTRODUCTION
Insider threats remain a harsh reality within organizations as the technological industry continues to grow. As Internet related crimes increase exponentially, providing adequate security measures maintains its spot in the list of the top managerial concerns.

An insider threat occurs when trusted members of the organization behave in a manner that puts it at risk. Exploring the reasons behind insider threats winds down to one broad concept—motivation. We strive to step inside the mind of an insider and discover exactly what it is that compels an insider to commit a potentially troubling act in the first place.

However, we also seek to go one step further and examine both the malicious and non-malicious insider. Traditionally, research has been focused on the malicious insider; someone that intentionally seeks to perform a malicious act against the organization that trusts him or her. This research is important and it is the malicious insider that is generally responsible for revealing trade secrets or causing intentional sabotage to an organization. However, more commonly organizations are the victims of non-malicious insiders. These are trusted employees that are not seeking to cause harm to their employer; rather, they misuse systems—either intentionally or unintentionally—that results in some harm to the organization.

In this paper, we first discuss the insider threat and various traits related to the typical insider. This includes personality, emotions, social theories, business factors, and cultural factors. Next, we discuss the methods employed in this study. This includes the development and validation of an instrument to measure both malicious and non-malicious insiders and the administration of a large-scale survey using this instrument and others. Next, we analyze the results found and discuss what they may mean. Finally, we end with some concluding remarks and suggestions for future research.

RIIT'16, September 28-October 01 2016, Boston, MA, USA

ACM 978-1-4503-4453-1/16/09…$15.00
DOI: http://dx.doi.org/10.1145/2978178.2978185

2. BACKGROUND
2.1 Insider Threats and Personality
An insider's personality is one of the largest contributing factors to their overall motivation. Increasing awareness of alarming personality traits can lend a hand in early detection and prevention of insider crimes. The Dark Triad Theory along with negative attitude and malicious intent are substantial predictors of insider threat. The Dark Triad personality traits are Machiavellianism, narcissism, and psychopathy [1]. These personality traits are often associated with emotions such as superiority, lack of remorse, lack of empathy, and privilege [2]. Recent research has demonstrated that the Dark Triad personality traits are useful in predicting workplace behavior [2]. Lack of empathy and a sense of entitlement have been identified as personality traits directly related with risk for an insider threat. Lack of empathy has especially been noted as a factor of all of the Dark Triad personality traits [2]–[4] .

Attitude is another factor of an insider's personality that can be useful in predicting the chance of an insider threat. An individual's attitude tailors how likable he or she is, how adaptable they are to an environment, their social adjustment, and

ego defense [2]. Nonetheless, personality traits and attitude must be evaluated coherently with the idea of intent. Intent includes the concept of desire and is related to the ideas of consequences, aim, purpose, and objective [2]. It captures the motivational factors that actually influence an insider to commit a crime.

The Capability Means Opportunity (CMO) model evaluates individual, interpersonal, and organizational factors in an attempt to understand the nature of insider incidents for detection and prevention in the case of future insider threats [2]. Taking into account personality traits as well as an insider's motivation, capability, and window of opportunity, future insider threats can be detected and prevented early on.

In this study, we will be looking at personality by using The Big Five Inventory [5]–[7].

2.2 Insider Threats and Emotions

The greatest challenges in predicting an insider threat before it occurs are defining the events leading up to the attack and developing a mechanism that integrates those indicators [3]. In various insider crimes, supervisors have indicated that they had noticed signs of stress and disgruntlement but no alarms had been raised [8]. Knowing when to identify an emotional signal can lead to early detection and prevention of an insider threat. Recent studies reported that in nine out of ten cases of insider crimes, nearly every single subject had shown significant personnel problems, such as disgruntlement, prior to the attack [8]. It had also been noted that there was a window of opportunity for dealing with the personnel problems before the attack [8]. In many cases, management was aware of these personnel problems long before the attack [8]. It is clear that many of the threats could have been prevented if there had been timely and effective action.

Some of the common emotional indicators reported were disgruntlement, issues dealing with anger, unable to accept feedback, disengagement, lack of respect for authority, performance issues, stress, confrontational behavior, personal issues, lack of dependability, and high rates of absenteeism [8], [9] . Management training in helping supervisors detect these emotional signs is necessary in taking a step towards the prevention of insider threats.

The Psychosocial Model, a data driven approach based on personnel data, uses the indicators listed above in an effort to provide training to help supervisors better understand the nature of the insider threat [8], [9]. It is important to consider the implication that judgments based on observations can be highly subjective when evaluating emotional indicators of insider threats [8]. Nonetheless, this model can be useful in providing "leads" for cyber security officers to pursue before the actual crime even occurs [8].

In this study, we will be looking at trait affect. Trait affect represents a generally stable and life-long type of affect. It is composed of the higher order dimensions positive affect and negative affect, which represent the valence of mood descriptors (e.g., afraid, scared, guilty, active, alert, excited). We will also be looking at the lower level dimensions that reflect the specific qualities of the individual affects (i.e., joviality, self-assurance, attentiveness, shyness, fatigue, serenity, surprise, fear, hostility, guilt, and sadness) [10]–[12].

2.3 Insider Threats and Financial Status

Many economic pressures have come into play as a result of economic problems like global recessions that in turn have an effect on an insider's overall motivation.

As discussed earlier, motivation is the driving force for whether or not an insider crime is committed in the first place. As a result of economic problems, many companies have to cut back on costs and increase revenue which can lead to wage cuts or termination of long-term employees [3]. Recent studies have indicated a direct correlation between a decline in national prosperity and the increase in crime rates [3]. This illustrates the belief that the more negative experiences the economy has on employees, the more likely they are to lash out and contribute to crimes. Recent data shows that 35% of IT workers have admitted to accessing corporate information without authorization and 74% of survey respondents stated that they could circumvent security controls that prevent access to internal information [3]. These recent studies and recent data demonstrate the increase in likelihood of insider crimes as the economy declines.

Another key factor in the relationship between insider threats and financial status is the effect that a decrease in financial stability can have on an insider's emotional state. Specifically, how falling into debt is positively correlated with emotional distress [13]. Recent studies showed that when a person is in debt they tend to show characteristics of low focus of control, low self-efficacy, and held a perception of money as a sense of power and prestige [14]. It is clear that for people that are facing financial strains, they view finances as the key to happiness, power, and prestige. The financial strain ignites quite a bit of negative characteristics within an individual and can begin to compel them to commit an insider threat act because they see no other opportunities to help relieve their economic conditions [14].

In this study, we will be looking at the financial well-being of individuals by employing the InCharge Financial Distress/Financial Well-Being Scale (IFDFW) [15].

2.4 Insider Threats and Social Theories

Analyzing the literature on insider threats has shown that many of the methods directed at detecting insider threats stem from the analysis of theories surrounding criminology and social behavior. Applying these theories can help detect an insider threat as soon as possible.

General Deterrence Theory (GDT) is the idea that people make logical decisions based on maximizing their benefit and minimizing any cost [16]. It suggests that when the chances of punishment increase with severe sanction, potential insiders will be deterred from committing a crime [17]. In an effort to deter computer abuse, the principles of GDT have been applied to develop the Security Action Cycle.

The Security Action Cycle targets handling computer abuse in the stages of deterrence, prevention, detection, and consequence [17]. It identifies the aim of security management to be the maximization of the number of potential offenders deterred and prevented abusive acts as well as the minimization of the number of detected and punished potential offenders [17].

The Social Bond Theory (SBT) is based on the hypothesis that despite an offender's inclination towards committing crime, strong social bonds can deter him or her away from committing the crime [17]. This theory is broken down into four types of social bonds: attachment, commitment, involvement, and beliefs [17]. An insider may not engage in criminal activity for fear of losing social surroundings, reputation, and involvement in conventional activities. However, if an insider has a weak belief system and maintains an antisocial background, the chances of an insider crime occurring increase exponentially.

The Social Learning Theory (SLT) claims that a person commits a crime because he or she has been associated with delinquent peers who transmit delinquent ideas [17]. This is the simple concept that the people individuals surround themselves with continue to have a lasting impact on them. Recent studies have shown a strong correlation between an individual engaging in computer abuse and the involvement of his or her friends in similar acts [17].

The theories stated above and those similar in nature demonstrate the influence that an insider's environment and involvement and social settings has on the likelihood on committing an actual crime. Analyzing these patterns also contribute to the early detection and prevention of potential insider crimes.

Another mechanism for preventing insider crimes stem from the Theory of Situational Crime Prevention. This mechanism focuses on making the criminal act appear more difficult by requiring more effort, making the criminal act appear more dangerous, reducing the benefit a person is expecting to receive, and removing the excuses a person can make in order to justify his or her actions [17]. Adopting these strategies into an organization's infrastructure can help prevent an insider from even thinking to execute the steps in order to commit an insider crime.

2.5 Insider Threats and Business Factors

In today's technological industry, many large scale companies have used outsourcing as a means to cope with rapidly changing requirements.

The amount of third-party companies given access to an organization's critical information and systems is growing exponentially [3]. Constant inclusion of third-party companies turns hundreds of outsiders into insiders, sometimes blurring the distinction between company full-time employees and third-party personnel [4]. These third-party employees are given some of the same access as full-time employees. Many companies have even begun to outsource their security infrastructure. The problem that arises from outsourcing confidential information is the fact that these third-party personnel don't have a history working with this company. This can be dangerous because they don't have an emotional connection to the organization. Often times, insiders stray away from actually executing the crime because they are afraid of the impact it will have on their social environment [3], [17]. The Social Bond Theory discussed earlier illustrates how insiders are affected by attachment and commitment. However, third-party personnel are much more unlikely to have this type of attachment and commitment that would prevent them from committing an insider crime.

2.6 Insider Threats and Cultural Factors

An insider's working environment can be directly related to the likelihood of whether or not an insider crime is committed. There are two cultural perspectives—organizational culture and regional culture—that can sometimes motivate an insider to commit a crime.

The organizational culture relates to changes in an organization's structure and management. If changes are not addressed properly they can invoke emotions such as fear, uncertainty, and doubt in long-term employees that can impact their overall attitude towards security [3]. When an insider is experiencing negative emotions such as fear, uncertainty, and doubt they are more likely to feel emotions that invoke a feeling of lack of recognition or privilege [2], [3]. These negative emotions diminish the commitment insiders have to an organization if they feel as if that bond is not being reciprocated. Often times, when an organization makes dramatic changes without making sure the employees are making smooth transitions, the likelihood of an employee turning against an organization increases. Therefore, focusing on maintaining a positive relationship with employees during dramatic transitions can help diminish the possibility of insider threats.

Regional culture relates to regional and national attitudes that need to be understood when working with employees across different cultures. Many organizations have locations worldwide where the regional practices are dramatically different than what is found in America. There are many language and cultural barriers that surface when working worldwide that must be addressed properly [3]. If an organization fails to be respectful of an international employee's cultural practices and doesn't work to ensure that they are understanding all requirements, the likelihood of that employee feeling negative emotions like neglect, lack of privilege, and lack of remorse increase. These negative emotions in turn contribute to creating the motivation to commit an insider crime within an organization [2], [3]. If organizations focus on appearing much more culturally conscious and focus on integrating international employees to the best of their ability, it can help in preventing insider crimes from outsourced employees.

3. METHODS

In this section we discuss the participants used in this study. Next the development and validation of a survey instrument designed to measure both the malicious and non-malicious insider is described. Finally, we discuss the process employed to conduct a large-scale survey combining the newly developed instrument with previously validated instruments.

3.1 Participants

This study involves human participants and an assessment of their beliefs, attitudes, opinions, and self-reported behavior. Therefore, we sought and obtained IRB approval prior to conducting the study. With respect to the development of an instrument to measure insider threat behavior, both malicious and non-malicious, we recruited subject matter experts that participated in multiple rounds of a consensus exercise.

For the large-scale survey, participants were recruited using Amazon's Mechanical Turk, which has been shown to be an effective and efficient technique for the recruitment of participants with quality generally regarded to be as high as other methods [18].

In order to check for quality, we incorporated two quality control questions into the survey instrument. If participants failed either quality control question then their responses were stripped from further analysis. The acceptance rate was approximately 91%. Participants were randomly assigned to one of two versions of the survey: approximately half of them completed a survey that had measures to assess personality factors while the other version had measures to assess factors related to trait affect. There were a total of 575 responses for the former compared to 557 for the latter.

3.2 Instrument Development

Our primary focus in this study was to assess the degree to which individuals have partaken in insider threat types of behavior, whether malicious or non-malicious, and determine if various psychological factors are related to this behavior. We unsuccessfully sought existing instruments designed to measure this type of behavior. Therefore, following the general guidelines from Churchill (1979) and Straub (1989), we began the process of developing our own [19], [20].

First, we began with specifying the domain of the construct under consideration. In the current study, the focus was on identifying

behaviors representative of the types of behaviors malicious and non-malicious insiders commit that may be detrimental to the organization.

Next, we surveyed the literature to help identify some of these behaviors. While several studies were informative in describing some of the behaviors of concern, we were not able to find lists of behaviors for malicious and non-malicious insiders. Nonetheless, this search did prove to be instructive as we continued in the process.

With this information in mind, we initiated a three-round Delphi consensus exercise with subject matter experts [21], [22]. Our eight subject matter experts had backgrounds that included experience in the public sector, private sector, military, government, and education. The approach we used was a modified version of the Delphi technique as all rounds were completed online using survey software. Consensus was considered achieved if 75% or more of the participants were in agreement on a particular item that was identified in the first round.

Once we were satisfied with the content of the items from the Delphi technique, we proceeded with a technical review. This was done to ensure the agreed upon items were worded clearly and in a manner that was not ambiguous [23].

Next, we completed a pretest of these items by conducting cognitive interviews [24], [25]. This was done with individuals that were considered representative of the population of interest. Notes were taken as they proceeded through each of the items. Some minor changes were made to structure, but not content since the content itself was determined by our subject matter experts.

Table 1 identifies 10 items that were identified as behaviors or circumstances that a non-malicious insider might engage in.

Table 1: Non-Malicious Insider Threat Behaviors

Non-Malicious Insider Threat Behaviors or Circumstances
1. Recent affluence or significant increase in financial well being
2. Unmonitored use of thumb drives or other externally attached media
3. Sharing too much information via social media
4. Violating network usage policy
5. Analysis of computer logging activities related to you indicate irregularities
6. Discussing company's proprietary information with non-employees
7. Consistently had/have malware on your work computer
8. Poor work performance
9. Mental health issues
10. Gambling

Table 2 identifies the behaviors or circumstances that might be indicative of a malicious insider.

Table 2: Malicious Insider Threat Behaviors

Malicious Insider Threat Behaviors or Circumstances
1. Accessing or copying sensitive information
2. Large downloads of information
3. Unauthorized release of data from a computer system
4. Inappropriate or unnecessary computer access permissions
5. Sharing certain accounts with others
6. Disciplinary action
7. Unmonitored use of thumb drives or other externally attached media
8. Curiosity about things outside of your normal work activities
9. Scanning/access beyond business requirements in the network
10. Logging into lost/stolen portable device
11. Violating network usage policy
12. Non-standard logins or login attempts
13. Request for unnecessary access to sensitive items
14. Accessing network remotely during odd times or during leave of absence
15. Analysis of computer logging activities related to you indicate irregularities
16. Unusual interest in confidential information
17. Odd hours of working
18. Missing equipment
19. Random unexplained trips to foreign countries
20. Financial problems
21. Drug or alcohol abuse
22. Lack of sharing job responsibilities
23. Discussing company's proprietary information with non-employees
24. Consistently had/have malware on your work computer
25. Poor work performance
26. Bad attitude
27. Negative social interactions with coworkers
28. Personality changes
29. Negative changes in behavior and attitude
30. Negative social media comments
31. Recent affluence or significant increase in financial well being
32. Mental health issues
33. Hostile behavior
34. Illegal activities
35. Gambling

3.3 Large-Scale Survey

Now that our new survey instrument has been developed, we combine it with pre-existing survey instruments designed to measure psychological factors, such as personality and trait affect, as well as an instrument designed to assess one's financial well-being. For trait affect, we used the PANAS-X instrument. In

particular, we assessed both the higher order dimensions of affect—positive and negative—as well as the lower order dimensions of affect—joviality, self-assurance, attentiveness, fear, guilt, hostility, and sadness [26]. In order to measure the five personality traits, we used The Big Five Inventory [5]–[7]. Finally, to assess one's financial well-being we used the InCharge Financial Distress/Financial Well-Being Scale (IFDFW) [15].

As noted before, participants were randomly assigned to one of two versions of the survey. The first version had measures designed to assess one's personality, while the second version assessed various components of trait affect. All versions of the survey had the insider threat and financial well-being measures.

4. ANALYSIS AND DISCUSSION

In this section, we discuss both reliability and the relationships found through our analysis.

4.1 Reliability

We first assessed the reliability of the various constructs measured in this study. Generally speaking, reliability was considered adequate. In the instrument that measures non-malicious insider threat behavior, reliability as measured by Cronbach's Alpha was only 0.647. While this is lower than what is ideal, we also consider this number adequate given the early stages of this research and its exploratory nature. The instrument for malicious insider threat behaviors had a much higher Cronbach's Alpha of 0.916, which is largely a function of the greater number of items (35) compared to the instrument for non-malicious insiders (10). Also, it is worth nothing that the insider threat items were all measured as dichotomous with *yes* or *no* being the only options. It is possible that a scale with more variation would have stronger reliability. This is something worth exploring in the future.

4.2 Relationships Found

Since this study is largely exploratory, we opted to take a very simple approach in assessing possible relationships between the psychological factors and financial well-being measure with the propensity to engage in behavior or circumstances related to a possible insider threat. In Table 3 we present the correlations between the insider threat constructs and the constructs for personality, trait affect, and financial well-being.

Table 3: Pearson Correlations with Insider Threat

Predictor Constructs	Non-Malicious	Malicious
Personality	*N=574*	*N=575*
Extraversion	-0.023	0.028
Agreeableness	-0.191**	-0.179**
Conscientiousness	-0.283**	-0.223**
Neuroticism	0.170**	0.154**
Openness	-0.068	-0.098*
Trait Affect – Higher Order	*N=557*	*N=556*
Positive	-0.055	-0.021
Negative	0.262**	0.201**
Trait Affect – Lower Order	*N=557*	*N=556*
Fear (Negative)	0.237**	0.157**
Hostility (Negative)	0.257**	0.232**
Guilt (Negative)	0.234**	0.205**
Sadness (Negative)	0.272**	0.220**
Joviality (Positive)	-0.052	-0.013
Self-Assurance (Positive)	0.024	0.037
Attentiveness (Positive)	-0.087*	-0.034
Shyness (Other)	0.184**	0.205**
Fatigue (Other)	0.172**	0.105*
Serenity (Other)	-0.091*	-0.066
Surprise (Other)	0.165**	0.216**
Financial Well-Being	*N=1,131*	*N=1,131*
IFDFW	-0.036	-0.072*
* Significant at the 0.05 level ** Significant at the 0.01 level		

The results indicate several interesting but perhaps not too surprising relationships. With respect to personality, individuals with lower levels of agreeableness and conscientiousness and higher levels of neuroticism are more likely to engage in behavior or circumstances related to those done by both a malicious and non-malicious insider. Additionally, lower levels of openness were found to be related to higher levels of behavior and circumstances consistent with that seen by malicious insiders. Extraversion was not statistically significant in either case.

Next, we turn our attention to trait affect. The interesting thing found with respect to trait affect is the strong relationship various components of trait negative affect have with both insider threat constructs. In each and every instance higher levels of trait negative affect, both the higher order dimension and every lower order dimension, were associated with higher levels of behaviors and circumstances associated with both malicious and non-malicious insiders. The same was not found for the higher order dimension trait positive affect and its lower order dimensions of joviality, self-assurance, and attentiveness. Only attentiveness was found to be related to the behavior and circumstances associated with a non-malicious insider. The less attentive someone is then the more likely he/she is to engage in such behavior or circumstances consistent with a non-malicious insider. This makes sense since non-malicious insiders generally perform acts detrimental to the organization when ignorant, curious, and/or simply inattentive with respect to their behavior.

Beyond the trait affect dimensions with valence, there were four other lower order dimensions we examined: shyness, fatigue, serenity, and surprise. Higher levels of shyness, fatigue, and surprise were all associated with higher levels of behavior and circumstances associated with the insider threat, both malicious and non-malicious. Lower levels of serenity were associated with higher levels of behavior and circumstances related to non-malicious insiders, but not for malicious insiders.

Finally, we look at the results for financial well-being. Our results suggest that lower levels of financial well-being—those that might be struggling to make ends meet—are more likely to engage in behavior and circumstances consistent with a malicious insider.

Overall, the relationships found here are supported by other evidence on insiders from a psychological standpoint as detailed in the literature review. However, some important components added in the current research are the inclusion of a measure for the non-malicious insider, an examination of trait affect, and the financial well-being of individuals. Furthermore, given the consistency of the results with prior research this suggests that survey research may be one other mechanism in which we can better understand the insider threat, both malicious and non-malicious.

Traditionally, survey research has perhaps been thought to be too problematic for this type of research given the percentage of insiders and the low likelihood that participants would reveal insider threat types of activity. However, this was mitigated by collecting responses from a large number of participants and using an approach that helped them remain anonymous from the research team.

5. CONCLUSION

The insider threat poses a large and significant challenge for organizations. Malicious insiders seek to use their position within an organization to cause harm to the organization. In contrast, non-malicious insiders have greatly different motivations and in fact may not intentionally be trying to cause harm.

This research took a close look at both the malicious and non-malicious insider, developed and validated survey instruments that can be used to measure this behavior, and compared this behavior with various psychological factors and their financial well-being. This allowed us to compare the profile of a malicious insider with a non-malicious insider. The differences between the two were not too great, which suggests that individuals engaging in behavior and activities without intent to cause harm to the organization may also be the same individuals that eventually do seek to engage in activities with malicious intent.

Additional research will help us better ascertain the similarities and differences between malicious and non-malicious insiders. Likewise, it may be valuable to delve more deeply into different types of non-malicious insiders. For example, some non-malicious insiders may very well know they're violating organizational policy, while others may not. Are they psychologically the same? And does one have a greater propensity to eventually engage in malicious activities than the other? Survey research may be one avenue to pursue answers to these questions.

6. REFERENCES

[1] M. Maasberg, J. Warren, and N. L. Beebe, "The Dark Side of the Insider: Detecting the Insider Threat through Examination of Dark Triad Personality Traits," in *System Sciences (HICSS), 2015 48th Hawaii International Conference on*, 2015, pp. 3518–3526.

[2] C. Grebitus, J. L. Lusk, and R. M. Nayga, "Explaining differences in real and hypothetical experimental auctions and choice experiments with personality," *J. Econ. Psychol.*, vol. 36, pp. 11–26, 2013.

[3] F. L. Greitzer, L. J. Kangas, C. F. Noonan, A. C. Dalton, and R. E. Hohimer, "Identifying at-risk employees: Modeling psychosocial precursors of potential insider threats," in *System Science (HICSS), 2012 45th Hawaii International Conference on*, 2012, pp. 2392–2401.

[4] C. Colwill, "Human factors in information security: The insider threat – Who can you trust these days?," *Inf. Secur. Tech. Rep.*, vol. 14, no. 4, pp. 186–196, Nov. 2009.

[5] V. Benet-Martínez and O. P. John, "Los Cinco Grandes across cultures and ethnic groups: Multitrait-multimethod analyses of the Big Five in Spanish and English.," *J. Pers. Soc. Psychol.*, vol. 75, no. 3, p. 729, 1998.

[6] O. P. John, E. M. Donahue, and R. L. Kentle, "The big five inventory—versions 4a and 54," *Berkeley Univ. Calif. Berkeley Inst. Personal. Soc. Res.*, 1991.

[7] O. P. John, L. P. Naumann, and C. J. Soto, "Paradigm shift to the integrative big five trait taxonomy," *Handb. Personal. Theory Res.*, vol. 3, pp. 114–158, 2008.

[8] J. D'Arcy, A. Hovav, and D. Galletta, "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Info Sys Res.*, vol. 20, no. 1, pp. 79–98, 2009.

[9] M. Voors, T. Turley, A. Kontoleon, E. Bulte, and J. A. List, "Exploring whether behavior in context-free experiments is predictive of behavior in the field: Evidence from lab and field experiments in rural Sierra Leone," *Econ. Lett.*, vol. 114, no. 3, pp. 308–311, Mar. 2012.

[10] D. F. Grös, M. M. Antony, L. J. Simms, and R. E. McCabe, "Psychometric properties of the State-Trait Inventory for Cognitive and Somatic Anxiety (STICSA): Comparison to the State-Trait Anxiety Inventory (STAI).," *Psychol. Assess.*, vol. 19, no. 4, pp. 369–381, Dec. 2007.

[11] D. Watson, L. A. Clark, and A. Tellegen, "Development and Validation of Brief Measures of Positive and Negative Affect: The PANAS Scales," *J. Pers. Soc. Psychol.*, vol. 54, no. 6, pp. 1063–1070, Jun. 1988.

[12] D. Watson and L. Walker, "The long-term stability and predictive validity of trait measures of affect.," *J. Pers. Soc. Psychol.*, vol. 70, no. 3, pp. 567–77, 1996.

[13] S. Brown, K. Taylor, and S. Wheatley Price, "Debt and distress: Evaluating the psychological cost of credit," *J. Econ. Psychol.*, vol. 26, no. 5, pp. 642–663, Oct. 2005.

[14] L. Wang, W. Lu, and N. K. Malhotra, "Demographics, attitude, personality and credit card features correlate with credit card debt: A view from China," *J. Econ. Psychol.*, vol. 32, no. 1, pp. 179–193, 2011.

[15] A. D. Prawitz, E. T. Garman, B. Sorhaindo, B. O'Neill, J. Kim, and P. Drentea, "InCharge financial distress/financial well-being scale: Development, administration, and score interpretation," *J. Financ. Couns. Plan.*, vol. 17, no. 1, 2006.

[16] M. Theoharidou, S. Kokolakis, M. Karyda, and E. Kiountouzis, "The insider threat to information systems and the effectiveness of ISO17799," *Comput. Secur.*, vol. 24, no. 6, pp. 472–484, Sep. 2005.

[17] F. L. Greitzer and D. A. Frincke, "Combining traditional cyber security audit data with psychosocial data: towards predictive modeling for insider threat mitigation," in *Insider Threats in Cyber Security*, Springer, 2010, pp. 85–113.

[18] M. Dupuis, B. Endicott-Popovsky, and R. Crossler, "An Analysis of the Use of Amazon's Mechanical Turk for Survey Research in the Cloud," presented at the International Conference on Cloud Security Management, Seattle, Washington, 2013.

[19] G. A. Churchill, "A paradigm for developing better measures of marketing constructs.," *J. Mark. Res.*, vol. 16, no. 1, pp. 64–73, 1979.

[20] D. W. Straub, "Validating Instruments in MIS Research.," *MIS Q.*, vol. 13, no. 2, 1989.

[21] C. Duffield, "The Delphi Technique," *Aust. J. Adv. Nurs. Q. Publ. R. Aust. Nurs. Fed.*, vol. 6, no. 2, 1988.

[22] F. Hasson, S. Keeney, and H. McKenna, "Research Guidelines for the Delphi Survey Technique," *J. Adv. Nurs.*, vol. 32, no. 4, pp. 1008–1015, 2000.

[23] D. Krathwohl, *Methods of educational and social science research : an integrated approach*, 2nd ed. Long Grove Ill.: Waveland Press, 2004.

[24] P. Housen, "What the Resident Meant to Say: Use of Cognitive Interviewing Techniques to Develop Questionnaires for Nursing Home Residents," *Gerontologist*, vol. 48, no. 2, pp. 158–169, 2008.

[25] M. Rosal, E. Carbone, and K. V. Goins, "Use of cognitive interviewing to adapt measurement instruments for low-literate Hispanics.," *Diabetes Educ.*, vol. 29, no. 6, 2003.

[26] D. Watson and L. A. Clark, "The PANAS-X: Manual for the Positive and Negative Affect Schedule - Expanded Form." University of Iowa, 1994.