Psychological Profiling of Hacking Potential[1]

Joana Gaia
Department of Management Science and Systems
University at Buffalo, SUNY

Bina Ramamurthy
Department of Computer Science and Engineering
University at Buffalo, SUNY

G. Lawrence Sanders
Department of Management Science and Systems
University at Buffalo, SUNY

Sean Patrick Sanders
Department of Computer Science and Engineering
University at Buffalo, SUNY

Shambhu Upadhyaya
Department of Computer Science and Engineering
University at Buffalo, SUNY

Xunyi Wang
Department of Management Science and Systems
University at Buffalo, SUNY

Chul Woo Yoo
Information Technology and Operations Management
Florida Atlantic University

Abstract

This paper investigates the psychological traits of individuals' attraction to engaging in hacking behaviors (both ethical and illegal/unethical) upon entering the workforce. We examine the role of the Dark Triad, Opposition to Authority and Thrill-Seeking traits as regards the propensity of an individual to be interested in White Hat, Black Hat, and Grey Hat hacking. A new set of scales were developed to assist in the delineation of the three hat categories. We also developed a scale to measure each subject's perception of the probability of being apprehended for violating privacy laws. Engaging in criminal activity involves a choice where there are consequences and opportunities, and individuals perceive them differently, but they can be deterred if there is a likelihood of punishment, and the punishment is severe.

The results suggest that individuals that are White Hat, Grey Hat and Black Hat hackers score high on the Machiavellian and Psychopathy scales. We also found evidence that Grey Hatters oppose authority, Black Hatters score high on the thrill-seeking dimension and White Hatters, the good guys, tend to be Narcissists. Thrill-seeking was moderately important for White Hat hacking and Black hat hacking. Opposition to Authority was important for Grey Hat hacking. Narcissism was not statistically significant in any of the models. The probability of being apprehended had a negative effect on Grey Hat and Black Hat hacking. Several suggestions will be made on what organizations can do to address insider threats.

1. Introduction

International Data Corporation (IDC) [1] estimates that the amount of data stored will grow from 33 zettabytes to 175 zettabytes by 2025 (a zettabyte is a trillion gigabytes). The ongoing protection of this batholith of organization and personal information is a major challenge because a substantial amount of that data has monetary and information value. The Privacy Rights Clearinghouse has been keeping a running tab since 2005 on the number of data breaches. In 2005 the number of data breaches made public was 8,804. Now that number is approaching 11.6 billion [2] records. The eighteen largest breaches in 2018 involved more than 10.3 million individuals [3].

The dark side of the abundance of personal information is that the information, even legally protected information can be compromised by trusted insiders and by external hackers. A substantial portion of privacy violations including funds embezzlement, pilfering of trade secrets, theft of customer information, theft of competitive information, and related fraudulent activities can be traced to insiders [4]. The losses from insider attacks can be significant [5]. The average cost of an insider attack is $8 million per year [6]. But the fallout from a breach can lead to long-term loss of customers, lawsuits and severely damaged reputations. Insiders can be current and former employees, contractors, and business partners

[1] This material is based upon work supported by the NSF under grant No. DGE-1754085

URI: https://hdl.handle.net/10125/64014
978-0-9981331-3-3

that have access to an organization's network, system, or data. Insiders can engage in malicious or unintentional activity that negatively affects the confidentiality, integrity, and availability of an organization's information system [7].

However, despite the importance of insiders in security management, an understanding of how their hacking intention is motivated and developed based on personal traits is still lacking. Particularly, examining different hacking intentions as a white hat, a black hat, and a grey hat has not been attempted in the literature. This study addresses this gap in the literature by bringing attention to Dark Triad, Opposition to Authority and Thrill-Seeking traits regarding the propensity of an individual and examining their influence on the white hat, black hat, and grey hat hacking intention.

The current study seeks to address two research questions:

1. *Are the Dark Triad personality traits consisting of Machiavellianism, Narcissism, and Psychopathy, along with the Opposition to Authority and Thrill-Seeking constructs related to behavioral intentions to engage in White Hat, Black Hat, and Grey Hat hacking?*
2. *Does the perception of being caught engaging in illegal violations of privacy laws moderate the relationship, and is it inversely related to hacking propensity?*

To answer these questions, we conducted a survey with 439 individuals that will soon enter the workforce.

This research note makes a twofold contribution to the security literature. The first major distinguishing contribution of our study is that we developed a set of dependent variable scales to measure behavioral intentions to engage in legal White Hat, illegal Black Hat, and hacktivist Grey Hat hacking. They are the White Hat, Black Hat, and Grey Hat hacking personas. We also used a short form of the Dark Triad called the Dirty Dozen, and we incorporated thrill-seeking and opposition to authority constructs.

The second major contribution of our study is that we also integrated the economics of crime and rational choice theory frameworks with the psychological profile of the subjects. Engaging in criminal activity involves a choice where there are consequences and opportunities, and individuals perceive them differently, and individuals can be deterred when there is a likelihood of punishment, and the punishment is severe [8]. We also included a construct to determine if the propensity to engage in one of the hacking activities is moderated by the probability of being apprehended.

This paper is organized as follows: first, a literature review on hacking motivation and dark triad is provided, followed by the economics of crime literature. Then, we propose core hypotheses for the empirical examination. Next, the research method employed for validating the instrument and data collection is discussed, followed by a test of the structural model using partial least squares (PLS)-based structural equations. Our empirical findings are then summarized, and possible explanations are provided. Lastly, in the final section, the theoretical and practical implications of these results are examined, and recommendations for future research directions are offered.

3. Prior Research on Hacking Motivation

Psychological profiling hackers has attracted substantial recent research interest [5, 9-13]. Motivations for participating in hacking behavior include seeking revenge, ideology, fun, thrills, survival, notoriety, recreation, and profit [5, 14, 15].

Madarie conducted a study on what motivates hackers using Schwartz's theory of motivation types and found that many hackers are motivated by what they don't like, rather than what they like [16]. Of particular note, was the discrepancy between what the "experts" suggest is the motivating factor behind hackers, and what actually motivates hackers. Madarie postulates that the discrepancy in the literature reflects a cultural and background bias. That is, hackers may report to experts what they have heard that motivates them, rather than what actually motivates them. Madarie's study found that hacking is a social activity, where the hacking frequency is driven by peer recognition, respect and by the opportunity to engage in team-play and not by the intellectual challenge of the activity, by curiosity and even to seek justice.

Maasberg et al. proposed a research model that integrated the Dark Triad and the Capability, Motive, and Opportunity (CMO) framework [17]. The CMO framework is one of the classical models used to understand insiders and how cyber-attacks occur. In the CMO model, the potential perpetrator needs to have the Capability to commit the attack, the Motive for attacking, and the Opportunity to carry out the breach [18].

The Dark Triad refers to a group of three generally, socially undesirable personality traits, including Machiavellianism (manipulative, deceitful and exploitive), Narcissism (self-centered and attention-seeking) and psychopathy (lack of remorse, cynical and insensitive) [19-21]. These measures are related, but they are nevertheless, distinct constructs [19, 22].

Many of the Dark Triad personality traits are used by the press and by security experts to describe criminal activity by insiders, but as noted by Maasberg there are few studies involving insider threat behavior [17]. We could only find one.

A recent study investigated the relationship between computer abuse, Narcissism, Psychopathy, and some other personality variables [23]. The study involved 235 Amazon Mechanical Turk (AMT) respondents that completed a questionnaire with a large survey with 200 items. The survey included the 88-item Elemental Psychopathy Assessment Short Form (EPA-SF). The subjects also completed the 45 item Computer Crime Index-Revised (CCI-R). This instrument asks respondents if they had been involved in unauthorized computer access (57%), virus creation (12%), identity theft (23%), network monitoring and hacking (23%) and website defacement (11%). Approximately 36% reported never engaging in computer crime. The subjects also completed the 45 item Crime and Analogues Behavior Scale and the 30 item Five-Factor Model Rating form. The psychopathy construct consisted of four sub-scales. Antagonism had a .43 correlation with total computer crime (r-square .19). Emotional Stability had a .08 correlation with total computer crime (r-square .01). Disinhibition had a .37 correlation with total computer crime (r-square .14), and the correlation between Narcissism and total computer crime was .26 (r-square .07).

There are several major differences between our study and the above study. They used an 88 item instrument to measure psychopathy, and we used the shorter Dirty Dozen scale which also includes Machiavellianism and Narcissism. They used AMT to collect the data, and their results relied only on examining 197 correlations to identify relationships among the variables. We used a large sample (439 subjects including 246 students from the School of Management and 193 students from Computer Science) that targeted individuals that are entering the workforce and used partial least squares structural equation modeling to examine the relationships. While their study used a computer crime index, we developed a unique targeted scale to measure the propensity to engage in White Hat, Grey Hat, and Black Hat Hacking. We also integrated the economics of crime construct in the model to examine the perception of the probability of being apprehended in hacking activities.

3. The Genesis of White Hat, Black Hat, and Grey Hat Hacking

The White Hat, Black Hat, and Grey Hat hacker typology has been around for several years, and these terms have also been popular with the hacking communities [24], the academic communities [25-27], and the popular press [28].

White hat hackers, sometimes referred to as ethical hackers [29], assist system owners in detecting and fixing security systems vulnerabilities. They are referred to as ethical hackers because they do not violate laws, even though they use many of the same tools used by Black Hat hackers.

Black Hat hackers, sometimes called crackers, are typically motivated by the personal gain they receive from illegally breaching computer systems, though they might also be social mischief-makers that are in it for the thrill of the attack, for revenge or to seek notoriety.

Grey Hats can have ideological motivations that translate to hacking attacks against an adversarial political position, a company policy that they do not agree with or even a nation-state. They are often referred to as hacktivists. Grey Hat hackers can be White Hats by day and work for organizations and system owners to detect flaws in systems and mitigate them, but they sometimes engage in ideological hacking activities to correct a perceived wrong.

4. Economics of Crime Literature

Black Hat crime is often motivated by economic incentives [30]. These attacks can adversely affect business operations and compromise sensitive customer information. Many security incidents can be traced to existing employees or what is referred to as insider threats. Threats from trusted insiders are difficult to detect, embarrassing, damage the reputation of the organization, often destructive, and cause serious operational disruption [12]. We will investigate the role of economic incentives on the propensity of next-generation workers to violate privacy laws.

Engaging in criminal activity involves a choice where there are consequences and opportunities, and individuals perceive them differently, and individuals can be deterred if there is a likelihood of punishment and the punishment is severe [31, 32]. Becker's seminal paper on the market for criminal activity posits that potential criminals examine returns on criminal activity as a function of the probability of being apprehended and the severity of the punishment. The market model assumes that offenders have expectations about returns, the propensity for being caught, and the resulting punishment [33]. The economics of crime model posits that deterrence will work to counter monetary gains if the penalties are large and if there is a certain level of risk of being caught. Thus, we also include a measure of deterrence in terms of the perception of the probability of being apprehended for violating HIPAA privacy laws.

5. Research Model and Hypothesis

Based on the theoretical discussion above, Figure 1 presents the conceptual model that depicts relationships between hacking motivations, personal traits, and three different types of hacking intention. We argue that five individual factors would influence three types of hacking intention differently, along with the moderating effects of different probabilities of being apprehended in different situations. Thus, in the following section, we propose hypotheses for these relationships.

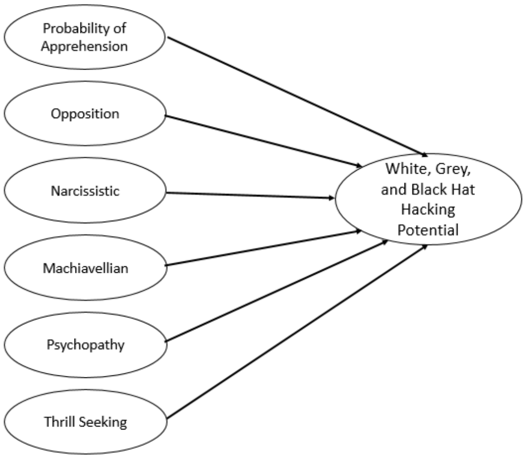
Probability of Apprehension
Opposition
Narcissistic
Machiavellian
Psychopathy
Thrill Seeking
White, Grey, and Black Hat Hacking Potential

Figure 1 - Research Model

Our first hypothesis is related to the psychology of hackers. For example, Maasberg et al. proposed a research model that integrated the Dark Triad and the Capability, Motive, and Opportunity (CMO) framework [17]. We also draw on a research study that investigated the relationship between computer abuse and crime as influenced by Narcissism and Psychopathy as additional justification [23].

H1: The Dark Triad consisting of Machiavellianism, Narcissism, and Psychopathy will be important predictors of interest in White Hat, Grey Hat, and Black Hat hacking.

Thrill-seeking behavior has been consistently touted as a motivation for hacking [34, 35]. As noted by Bachman, thrill-seekers derive pleasure from the excitement of hacking, and black-hat hackers are projected to be attracted to overcoming the barriers and impediments to hacking. Some believe that the days of the thrill-seeker as a hacker have morphed to the larger role of state-sponsored hackers [36]. We included a Thrill Seeking scale because this trait is often used to describe many individuals that are attracted to hacking [23]. For example, Maderie found that most hackers were primarily motivated by fun, thrill-seeking, excitement, and curiosity [16].

H2: Interest in Thrill Seeking will be important predictors of interest in White Hat, Grey Hat, and Black Hat hacking.

Civil disobedience, in the form of hacktivism, has emerged as a go-to strategy to disrupt organizations and even country activities [37]. Trolls and hackers have much in common [38]. There is some evidence that boredom, attention-seeking, and revenge motivate both trolls and hackers. However, they seem to be driven by freedom of expression and an anti-bureaucracy [39] orientation and a mistrust of authority. We included an Opposition to Authority scale to determine if this construct influenced engagement in one of the three hat activities [23].

H3: Opposition to Authority will be an important predictor of interest in White Hat, Grey Hat, and Black Hat hacking.

Engaging in criminal activity involves a choice where there are consequences and opportunities, and individuals perceive them differently, but they can be deterred if there is a likelihood of punishment and the punishment is severe [8]. As noted earlier, the market model for crime assumes that offenders, victims and law enforcement engage in optimizing behavior related to their preferences and that offenders have expectations about returns, the propensity for being caught and the resulting punishment [8]. We also include a construct to determine if the probability of being apprehended moderates the propensity to engage in hacking activities.

H4: The probability of being apprehended will moderate the interest in White Hat, Grey Hat, and Black Hat hacking.

In the next section, we will report the process we used for selecting and adapting scale items to test the research model.

5.1 Scale Development for the Hacking Typology

The scales were developed by examining the academic and professional literature and then by having experts in security and privacy research exam the items. That team included the authors with over 150 research and journal articles and over $13 million in research grants on security, cybercrime, piracy, and privacy-related issues. The six White Hat items are a combination of technical and social engineering hacking behaviors. Social engineering hackers exploit people and systems by social manipulation of people involving interactions using disguises, ploys, and psychological tricks for intrusion behaviors [40]. This is in contrast to technical attacks that require sophisticated knowledge for attacking a system. The four Black Hat items involve financial attacks that are motivated by the personal gain to breach computer systems. These activities are typically illegal. The three Grey hat items are in the middle ground. They are ideological activities engaged in to correct a perceived wrong, and they might be illegal.

The study follows the criteria recommended by [41] for choosing survey items. They recommend removing items that are not relevant to the specific innovation examined in the study and also deleting items that are very similar to other items. By using these criteria, the items selected to ensure complete coverage of the constructs at hand. The various hat items are behavioral intentions to engage in White Hat, Grey Hat, and Black Hat hacking. We originally identified 18 items to be used for the hat typology and then reduced that down to 16 items based on item analyses. We removed two items from the Grey Hat scale because of the overlapping coverage of the construct as manifested by the variance inflation factor being above 5. The final items for the three hats include social engineering, technical questions, financial motivation questions, and hacktivism questions.

6. The Dark Triad and the Dirty Dozen Items

We chose the Dark Triad Dirty Dozen for this study because these concise scales contain only four items for Machiavellianism, Narcissism, and Psychopathy [21]. These scales also have been used extensively, have reasonable psychometric properties acceptable convergent and discriminate validity, and they have been adapted to several cultures [42-45].

In general, the Dark Triad traits are viewed as being undesirable. However, research suggests that these traits have a dark side and a positive side [46]. A German study found that leaders with Machiavellianism and psychopathy personality traits were detrimental to employee well-being whereas subordinates rating leaders that are high on the narcissism scale reported better career success, higher salaries, and more promotions. We suspect that individuals engaged in hacking, whether White Hat or Black Hat, may have manifestations of Machiavellianism and psychopathy. That is, ethical White Hat individuals may exhibit Machiavellianism and psychopathy tendencies. Note here; we are not trying to detect if the respondents are, for example, psychopaths; rather, we are investigating the association between the propensity of engaging in hacking behavior (White, Black, or Grey) and the level psychopathy.

7. Probability of Being apprehended

The probability of being apprehended construct was developed as part of another large study project involving 523 subjects that focused on the economics of crime. The objective of that study was to identify the role that monetary incentives play in violating HIPAA regulations and privacy laws in the next generation of employees [33]. The research model was developed using the economics of crime and rational choice theory frameworks to identify situations where employees might engage in illegal breach behavior.

These scenarios were developed to determine if the probability of being apprehended increases the level of monetary incentives necessary to encourage people to violate HIPAA laws by illegally obtaining health care information and releasing that information to individuals and media outlets. We only used four out of the original five scenarios to develop a latent variable, the **probability of being apprehended**, to measure each subject's perceived probability of being caught.

An example scenario is described below:

"Suppose you are a nurse's aide at a hospital and you earn $30,000 per year, a friend asks you to get them some information on a patient you have been caring for. ... What amount of money would you receive to make this acceptable? ... What do you think is the likelihood of getting caught, if you accept the money? "

8. Data Collection & Analysis

Subjects were obtained from sophomore, and junior undergraduates in majoring in management and computer science enrolled at a state research institution in the northeast. All subjects voluntarily participated in the survey and were advised that they could withdraw from participation at any time without adverse consequence. All the participants were given extra credit for participating in the study.

The questionnaire was refined and distributed to 474 students in an undergraduate statistics course in a management school and an undergraduate computer science course on data intensive computing. We believe studying these two populations, management and computer science students will provide a solid foundation for studying and investigating other populations.

We removed subjects from the analyses where the subjects had more than 10% missing values and where subjects took less than two minutes to complete the survey. The number of valid surveys was 439, for a participation rate of 92%. There were 246 students from the school of management course and 193 students from computer science in the study. Again, we chose this sample because they will be entering the workforce in the immediate future, and from our experience, they are less concerned with social desirability issues. It is very difficult to get participation using actual organizations in this kind of a study. We have found that organizations do not want to participate in this type of study because it might reflect on their reputation. Employees are also not good candidates for such a study because of social desirability bias.

In essence, personality data gathered from employees is usually biased and unreliable. Social desirability bias is a problem in studies involving abilities, personality, and illegal activities. Social desirability bias occurs when subjects are less prone to answer questions truthfully that could diminish their social prestige [47, 48]. Individuals will tend to over-report “good behavior and under-report “bad behavior.” Social desirability bias is a problem in studies involving abilities, personality, and illegal activities. Subjects often tend to deny Illegal acts. Our findings were illuminating, as the subjects in our study were very candid.

Seventy-two percent of the subjects were male, and 28% were female. The average age of the subjects was between 20 and 21. Thirty-eight percent were White, 1.6% Black, 2.1% Hispanic, 54% Asian and 4% other.

We used SmartPLS 3.0 for the analysis since PLS is very robust, resistant to statistical inadequacies, and effective in handling complex multidimensional constructs [49]. Because our research model includes six reflective sub-latent variables, we were also interested in prediction, and PLS is designed to maximize the prediction of dependent variables [50].

The five psychological traits, Opposition to Authority, Machiavellianism, Narcissism, Psychopathy, and Thrill-Seeking were used to predict the attraction to participate in White Hat, Grey Hat, and Black Hat behavior. We also included the perception of the potential of being apprehended in pursuing an illegal activity.

We tested the White Hat, Grey Hat, and Black Hat models separately to make the exposition and explanation clearer.

9. Measurement Assessment

Individual loadings and internal consistency were examined to test for item reliability. Loadings for all measurement items were above 0.7 except for one of the Narcissism items (Narc1 with an outer loading of 0.625) for the Grey Hat model. Table 1 illustrates that the Cronbach’s alpha for every construct was greater than 0.7, thus indicating internal reliability [51]. All of the items used in the study are available from the online supplementary material [2].

Discriminant validity was assessed using the average variance extracted (AVE). The square root of AVE should be greater than the correlations among the constructs. Table 1 shows Cronbach’s Alpha, the composite reliability, and the average variance extracted for the constructs.

Table 1- Latent Variable Statistics

Independent Variables			
	Cronbach Alpha	Composite Reliability	Average Variance Extracted
Machiavellian	0.877	0.915	0.729
Narcissistic	0.829	0.877	0.641
Opposition	0.867	0.909	0.715
Psychopathy	0.838	0.892	0.674
Thrill Seeking	0.877	0.913	0.725
Prob. Being apprehended	0.885	0.920	0.744
Dependent Variables			
	Cronbach Alpha	Composite Reliability	Average Variance Extracted
White Hat ($r^2 = 0.407$)	0.953	0.962	0.782
Black Hat ($r^2 = 0.372$)	0.903	0.933	0.778
Grey Hat ($r^2 = 0.297$)	0.895	0.934	0.826

10. Model Assessment

All of the r-squared values for the models were above 0.28. According to Cohen, a small r-square effect size is approximately less than 0.14, a medium effect size is between 0.14 and 0.26, and a large effect size is greater than 0.26 [52]. The essential criterion

[2] Https://onedrive.live.com/view.aspx?cid=a3660eed58d91ed9&page=view&resid=A3660EED58D91ED9!78125&parId=A3660EED58D91ED9!78124&app=Word

for evaluating PLS path models is the r-square or coefficient of determination.

10.1 White Hat Results

The r-squared for the White Hat model was 0.407. Machiavellianism, Narcissism, Psychopathy, and Thrill-Seeking were predictors of individuals attracted to White Hat hacking. Psychopathy and Machiavellianism were very strong predictors of individuals attracted to White Hat hacking (Figure 2). The p-values for the model coefficients are in parentheses. They were generated using 500 bootstrapped samples.

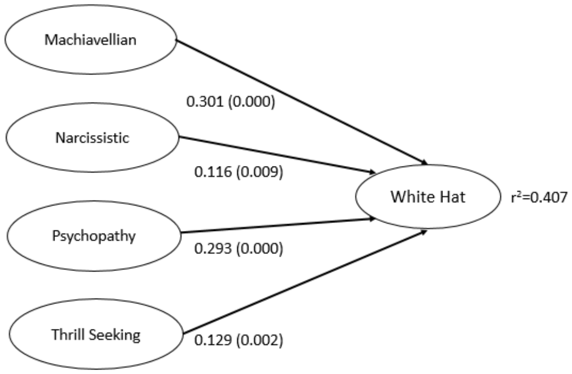

Figure 2 -White Hat Model Results

10.2 Grey Hat Results

The r-squared for the Grey Hat model was 0.297. Opposition to Authority, Machiavellianism and Psychopathy were statistically significant predictors of individuals attracted to Grey Hat hacking (Figure3).

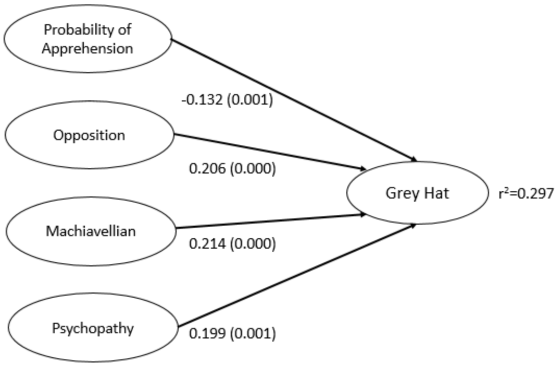

Figure 3 - Grey Hat Model Results

We had anticipated that individuals attracted to Grey Hat hacking would be higher on the Opposition to Authority scale because these individuals would have ideological motivations that translate to actions against political figures, company policies and even nation-states. We were not sure that opposition to authority would be statistically significant for White Hats and Black Hats.

10.3 Black Hat Results

The r-squared for the Black Hat model was 0.372. Thrill Seeking, Machiavellianism, and Psychopathy were statistically significant predictors of individuals attracted to Black Hat hacking (Figure 4). We were not surprised that individuals interested in Black Hat hacking would be in it for the thrills because Black Hat hacking is illegal and thrill-seeking is often a factor in all types of crime, particularly in younger people [53]. Thrill-seeking relates to curiosity and the desire for knowledge [35]. A Black Hat is primarily motivated by the personal gain to breach computer systems illegally, and they might also be mischief-makers that are in it for the thrill of the attack, and to seek notoriety.

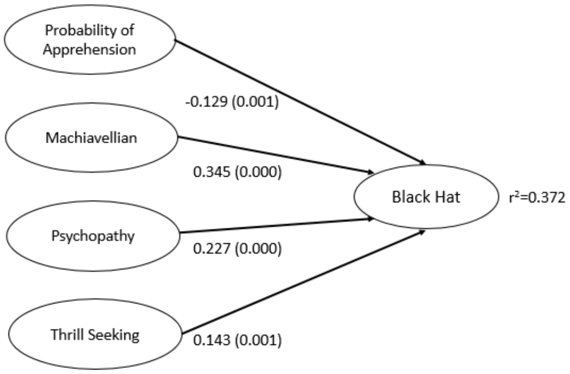

Figure 4 - Black Hat Model Results

11. Conclusion

The results of this study and other studies suggest that security compliance will continue to be a problem. Organizations can engage in several activities that reduce the impact and even prevent security breaches. For example, preventive controls including sophisticated monitoring technologies and multi-factor authentication can be used to prevent unauthorized access to buildings, software, and databases. Organizations can often turn to monitoring and recording privileged user’s activity sessions as they access files, folders, databases, servers, applications, hardware, and buildings.

Organizations typically focus on technical preventives because they are relatively easy to implement, and they are under the control of the organization. It takes a significant commitment of resources to employ deterrent strategies that focus on the apprehension and punishment of perpetrators as well as on education, legal campaigns, and fear appeals.

Using the Dark Triad personality traits to evaluate new employees as security threats, is possible [17]. However, this strategy will be approached cautiously for practical, ethical, and privacy reasons.

We found that White Hat hackers have Machiavellian, Narcissistic Psychopathy and Thrill-Seeking traits. But that does not mean they will migrate to being Black Hats. And more importantly, they are needed to counter Black Hat and Grey Hat attacks.

Even if surveys like the Dark Triad are administered to potential employees, the results will undoubtedly be biased. Potential employees may not answer such questions truthfully because they will not want to diminish their social prestige [47, 48]. People tend to over-report "good behavior and under-report "bad behavior." Being deceitful, manipulative, lacking remorse, and being unconcerned with the morality of one's actions certainly diminishes social prestige. Indeed, we were very surprised that so many of the subjects were so candid in their responses to the survey questions.

Since it is unlikely that potential employees would be very candid in answering the Dark Triad questions, the only way organizations could obtain this type of information is to conduct a 360-degree analysis of each employee's personality. This would, of course, present numerous, social, legal, and ethical issues.

The Software Engineering Institute of Carnegie Mellon University has identified very detailed procedures, in their guide for countering insider threats [7]. These guidelines are extensive, and they include policymaking, the development of organizational control and monitoring systems, hiring practices, privileged access guidelines, and addressing behavioral issues as well. An important take-away from the SEI insider report is the use of positive incentives such as connecting, engaging and supporting with employees along with negative incentives in the form of restrictions, monitoring, sanctions, and punishments. Security through positive incentives can be accomplished more effectively using small teams. The net result is that the frequency of insider misbehavior might be reduced with the use of positive incentives.

Hacking knowledge is a two-edged sword that can be used for mischief as well as to counter illegal attacks against individuals, organizations, and society. The key is constant organizational attention to security issues and the development of educational and training programs. Developing security education, training, and awareness (SETA) is always a challenge. It is not enough to have employees complete an online or even an in-person security training class. Employees need to be immersed in security training, receive feedback, and have social interaction with other employees on security issues if the training is to be successful [54].

Two theories, with significant potential, include Social Bond Theory and Situational Crime Prevention Theory, are being applied to address insider threats. The idea is to reduce the rewards, remove excuses, increase negative attitudes towards misbehavior, and generate social bonds that lead to commitment towards organizational security policies [9].

Wrongdoers use a calculus of rational choice in determining whether to engage in criminal activity [55] [31]. This calculus is affected by an individual's personality traits, which in turn is related to the probability of being caught. Improvements in technology and attention to organizational processes for addressing and preventing security breaches are the key to reducing insider threats.

12. Future Research

Because this is an exploratory study. There are many areas for future study. Further validation of the White Hat, Grey Hat, and Black constructs is the first step. Our sample used 246 management students and 193 computer science students in the study. It would be desirable to obtain a sample from a variety of organizations in several industries, but as noted before that data will be highly circumspect because the trust and social desirability issues loom large with individuals already in the workforce. A future study could replicate the findings in a more age-diverse sample, as such findings would have greater generalizability across a multi-generational workforce. We chose an undergraduate sample because they are more computer proficient, they will be entering the workforce in the immediate future, and they are less concerned with social desirability issues. Furthermore, cross-cultural (collectivism vs. individualism) Behavioral InfoSec research on hacking potential would be very interesting for future research to explore [56].

Finally, we have identified a potential target population which caters to the hacker culture. However, several issues need to be addressed, including how to reduce the chance that the survey team is not targeted by hackers.

12. References

[1] D. Reinsel, Gantz, J., Rydning, J., "The Digitization of the World From Edge to Core," *IDC,* p. 27, 2018.

[2] (2005, 6/12/2019). *Data Breaches*. Available: https://www.privacyrights.org/data-breaches

[3] J. HIPAA, "Largest Healthcare Data Breaches of 2018," *HIPAA,* Dec 27, 2018.

[4] P. B. L. Robert Willison, and Raymond Paternoster, "A Tale of Two Deterrents: Considering the Role of Absolute and Restrictive Deterrence to Inspire New Directions in Behavioral and Organizational Security Research," *Journal of the Association for Information Systems* 2018.

[5] R. E. Crossler, A. C. Johnston, P. B. Lowry, Q. Hu, M. Warkentin, and R. Baskerville, "Future directions for behavioral information security research," *computers & security,* vol. 32, pp. 90-101, 2013.

[6] E. Chickowoski. (2018, 6/12/2019). *The 6 Worst Insider Attacks of 2018 – So Far*. Available: https://www.darkreading.com/the-6-worst-insider-attacks-of-2018---so-far/d/d-id/1332183?image_number=7

[7] T. Michael *et al.*, "Common Sense Guide to Mitigating Insider Threats, Sixth Edition," Software Engineering Institute, Carnegie Mellon University, Pittsburgh, Pennsylvania, Technical Report CMU/SEI-2018-TR-010, 2019.

[8] S. L. Myers, "Estimating the Economic-Model of Crime - Employment Versus Punishment Effects," (in English), *Quarterly Journal of Economics,* vol. 98, no. 1, pp. 157-166, 1983.

[9] N. S. Safa, C. Maple, T. Watson, and R. Von Solms, "Motivation and opportunity based model to reduce information security insider threats in organisations," (in English), *Journal of Information Security and Applications,* vol. 40, pp. 247-257, Jun 2018.

[10] G. Dhillon, S. Samonas, and U. Etudo, "Developing a Human Activity Model for Insider IS Security Breaches Using Action Design Research," (in English), *Ict Systems Security and Privacy Protection, Sec 2016,* vol. 471, pp. 49-61, 2016.

[11] M. Kajtazi, B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Assessing Sunk Cost Effect on Employees' Intentions to Violate Information Security Policies in Organizations," (in English), *2014 47th Hawaii International Conference on System Sciences (Hicss),* pp. 3169-3177, 2014.

[12] K. Roy Sarkar, "Assessing insider threats to information security using technical, behavioural and organisational measures," *Information Security Technical Report,* vol. 15, no. 3, pp. 112-133, 2010/08/01/ 2010.

[13] M. Warkentin, A. Vance, and A. C. Johnston, "Introduction to the Minitrack on Innovative Behavioral IS Security and Privacy Research," in *2016 49th Hawaii International Conference on System Sciences (HICSS)*, 2016, pp. 3635-3635: IEEE.

[14] R. Seebruck, "A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model," (in English), *Digital Investigation,* vol. 14, pp. 36-45, Sep 2015.

[15] H. Thackray, C. Richardson, H. Dogan, J. Taylor, and J. McAlaney, "Surveying the Hackers: The Challenges of Data Collection From a Secluded Community," in *European Conference on Cyber Warfare and Security*, 2017, pp. 745-748: Academic Conferences International Limited.

[16] R. Madarie, "Hackers' Motivations: Testing Schwartz's Theory of Motivational Types of Values in a Sample of Hackers," (in English), *International Journal of Cyber Criminology,* vol. 11, no. 1, pp. 78-97, Jan-Jun 2017.

[17] 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 English), *2015 48th Hawaii International Conference on System Sciences (Hicss),* pp. 3518-3526, 2015.

[18] E. E. Schultz, "A framework for understanding and predicting insider attacks," *Computers & Security,* vol. 21, no. 6, pp. 526-531, 2002.

[19] D. L. Paulhus and K. M. Williams, "The Dark Triad of personality: Narcissism, Machiavellianism, and psychopathy," (in English), *Journal of Research in Personality,* vol. 36, no. 6, pp. 556-563, Dec 2002.

[20] D. N. Jones and D. L. Paulhus, "Duplicity Among the Dark Triad: Three Faces of Deceit," (in English), *Journal of Personality and Social Psychology,* vol. 113, no. 2, pp. 329-342, Aug 2017.

[21] P. K. Jonason and G. D. Webster, "The Dirty Dozen: A Concise Measure of the Dark Triad," (in English), *Psychological Assessment,* vol. 22, no. 2, pp. 420-432, Jun 2010.

[22] D. N. Jones and D. L. Paulhus, "Introducing the Short Dark Triad (SD3): A Brief Measure of Dark Personality Traits," (in English), *Assessment,* vol. 21, no. 1, pp. 28-41, Feb 2014.

[23] K. C. Seigfried-Spellar, N. Villacis-Vukadinovic, and D. R. Lynam, "Computer criminal behavior is related to psychopathy and other antisocial behavior," (in English), *Journal of Criminal Justice,* vol. 51, pp. 67-73, Jul-Aug 2017.

[24] T. J. Holt, "Examining the Role of Technology in the Formation of Deviant Subcultures," (in English), *Social Science Computer Review,* vol. 28, no. 4, pp. 466-481, Nov 2010.

[25] M. A. Mahmood, M. Siponen, D. Straub, H. R. Rao, and T. S. Raghu, "Moving toward Black Hat Research in Information Systems Security: An Editorial Introduction to the Special Issue," (in English), *Mis Quarterly,* vol. 34, no. 3, pp. 431-433, Sep 2010.

[26] J.-H. Lee, "Black Hat: Knowledge Resource for Cybersecurity [Society News]," *IEEE Consumer Electronics Magazine,* vol. 6, no. 1, pp. 16-19, 2017.

[27] S. Farooqi *et al.*, "Characterizing key stakeholders in an online black-hat marketplace," in *2017 APWG Symposium on Electronic Crime Research (eCrime)*, 2017, pp. 17-27: IEEE.

[28] C. Hoffman. (2017, 6/12/2019). *Hacker Hat Colors Explained: Black Hats, White Hats, and Gray Hats.*

Available: https://www.howtogeek.com/157460/hacker-hat-colors-explained-black-hats-white-hats-and-gray-hats/

[29] C. C. Palmer, "Ethical hacking," (in English), *IBM Systems Journal,* vol. 40, no. 3, pp. 769-780, 2001.

[30] K. L. Hui, S. H. Kim, and Q. H. Wang, "Cybercrime Deterrence and International Legislation: Evidence from Distributed Denial of Service Attacks," (in English), *Mis Quarterly,* vol. 41, no. 2, pp. 497-+, Jun 2017.

[31] G. S. Becker, "Crime and Punishment - Economic Approach," (in English), *Journal of Political Economy,* vol. 76, no. 2, pp. 169-217, 1968.

[32] S. D. Levitt, "The Economics of Crime," *Journal of Political Economy,* vol. 125, no. 6, pp. 1920-1925, 2017.

[33] J. Gaia, X. Wang, C. W. Yoo, and G. L. Sanders, "The Good News and Bad News about Incentives to Violate HIPAA:It depends on the context, and it's mostly bad news," *Working Paper.,* 2019.

[34] M. K. Rogers, K. Seigfried, and K. Tidke, "Self-reported computer criminal behavior: A psychological analysis," (in English), *Digital Investigation,* pp. S116-S120, Sep 2006.

[35] M. K. Rogers, "A two-dimensional circumplex approach to the development of a hacker taxonomy," (in English), *Digital Investigation,* vol. 3, no. 2, pp. 97-102, Jun 2006.

[36] M. M. Waldrop, "How to hack the hackers: The human side of cybercrime," *Nature,* vol. 533, no. 7602, pp. 164-7, May 12 2016.

[37] M. Sauter, *The coming swarm : DDoS actions, hacktivism, and civil disobedience on the Internet*. New York ; London: Bloomsbury Academic, 2014, pp. xv, 168 pages.

[38] (6/12/2019). *Internet troll*. Available: https://en.wikipedia.org/wiki/Internet_troll

[39] P. Shachaf and N. Hara, "Beyond vandalism: Wikipedia trolls," (in English), *Journal of Information Science,* vol. 36, no. 3, pp. 357-370, Jun 2010.

[40] M. Erbschloe, *Trojans, worms, and spyware : a computer security professional's guide to malicious code*. Amsterdam ; Boston: Elsevier Butterworth Heinemann, 2005, pp. xix, 212 p.

[41] R. Agarwal and J. Prasad, "A conceptual and operational definition of personal innovativeness in the domain of information technology," *Information systems research,* vol. 9, no. 2, pp. 204-215, 1998.

[42] C. Savard, C. Simard, and P. K. Jonason, "Psychometric properties of the French-Canadian version of the Dark Triad Dirty Dozen," (in English), *Personality and Individual Differences,* vol. 119, pp. 122-128, Dec 1 2017.

[43] E. Ozsoy, J. F. Rauthmann, P. K. Jonason, and K. Ardic, "Reliability and validity of the Turkish versions of Dark Triad Dirty Dozen (DTDD-T), Short Dark Triad (SD3-T), and Single Item Narcissism Scale (SINS-T)," (in English), *Personality and Individual Differences,* vol. 117, pp. 11-14, Oct 15 2017.

[44] A. Z. Czarna, P. K. Jonason, M. Dufner, and M. Kossowska, "The Dirty Dozen Scale: Validation of a Polish Version and Extension of the Nomological Net," (in English), *Frontiers in Psychology,* vol. 7, Mar 30 2016.

[45] P. K. Jonason and V. X. Luévano, "Walking the thin line between efficiency and accuracy: Validity and structural properties of the Dirty Dozen," *Personality and Individual Differences,* vol. 55, no. 1, pp. 76-81, 2013.

[46] J. Volmer, I. K. Koch, and A. S. Goritz, "The bright and dark sides of leaders' Dark Triad traits: Effects on subordinates' career success and well-being (vol 101, pg 413, 2016)," (in English), *Personality and Individual Differences,* vol. 108, pp. 226-226, Apr 1 2017.

[47] D. Dodou and J. C. F. de Winter, "Social desirability is the same in offline, online, and paper surveys: A meta-analysis," (in English), *Computers in Human Behavior,* vol. 36, pp. 487-495, Jul 2014.

[48] Y. Akbulut, A. Donmez, and O. O. Dursun, "Cyberloafing and social desirability bias among students and employees," (in English), *Computers in Human Behavior,* vol. 72, pp. 87-95, Jul 2017.

[49] J. Henseler and W. W. Chin, "A Comparison of Approaches for the Analysis of Interaction Effects Between Latent Variables Using Partial Least Squares Path Modeling," (in English), *Structural Equation Modeling-a Multidisciplinary Journal,* vol. 17, no. 1, pp. 82-109, 2010.

[50] D. Gefen, E. E. Rigdon, and D. Straub, "Editor's comments: an update and extension to SEM guidelines for administrative and social science research," *Mis Quarterly,* pp. iii-xiv, 2011.

[51] C. E. Werts, R. L. Linn, and K. G. Joreskog, "Intraclass Reliability Estimates - Testing Structural Assumptions," (in English), *Educational and Psychological Measurement,* vol. 34, no. 1, pp. 25-33, 1974.

[52] J. Cohen, "A Power Primer," (in English), *Psychological Bulletin,* vol. 112, no. 1, pp. 155-159, Jul 1992.

[53] T. Hirschi and M. Gottfredson, "Age and the Explanation of Crime," (in English), *American Journal of Sociology,* vol. 89, no. 3, pp. 552-584, 1983.

[54] C. W. Yoo, G. L. Sanders, and R. P. Cerveny, "Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance," (in English), *Decision Support Systems,* vol. 108, pp. 107-118, Apr 2018.

[55] T. A. Loughran, R. Paternoster, A. Chalfin, and T. Wilson, "Can Rational Choice Be Considered a General Theory of Crime? Evidence from Individual-Level Panel Data," (in English), *Criminology,* vol. 54, no. 1, pp. 86-112, Feb 2016.

[56] R.E. Crossler, A. C. Johnston, P. B. Lowry, Q., Hu, M. Warkentin, and R. Baskerville. Future directions for behavioral information security research. Computers & Security, 32, pp. 90-101, 2013.