Dark Traits and Hacking Potential

Joana Gaia
University at Buffalo

G. Lawrence Sanders
University at Buffalo

Sean Patrick Sanders
University at Buffalo

Shambhu Upadhyaya
University at Buffalo

Xunyi Wang
Baylor University

Chul Woo Yoo
Florida Atlantic University

This paper investigates the psychological traits of individuals' attraction to engaging in hacking behaviors (both ethical and illegal/unethical) upon entering the workforce. A new set of scales have been developed to assist in the delineation of the three hat categories. We have also developed a scale to measure each subject's perception of the probability of being apprehended for violating privacy laws. The results suggest that 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 in the thrill-seeking dimension, and white hatters, the good guys, tend to be narcissists. Thrill-seeking was moderately important for white hat and black hat hacking, and opposition to authority was significant for grey hat hacking. Narcissism was not statistically significant in any of the models. A perceived probability of being apprehended had a negative effect on both grey hat and black hat hacking. Additional models were explored to examine the relationships among the research variables.

Keywords: hacking, psychology, dark triad, economics of crime

INTRODUCTION

The International Data Corporation (Reinsel, 2018) estimates that the amount of stored data will grow from 33 zettabytes to 175 zettabytes by 2025 (a *zettabyte* is one trillion gigabytes). The ongoing protection

of this batholith of organizational and personal information is a significant challenge because substantial data has monetary and informational 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 ("Data Breaches," 2005). Now that number is over 11.7 billion records. The 18 largest breaches in 2018 involved more than 10.3 million individuals (HIPAA, 2018; Reinsel, 2018).

The dark side of the abundance of personal information is that even legally protected information can be compromised by trusted insiders and external hackers. A substantial portion of privacy violations, including embezzlement of funds, pilfering of trade secrets, theft of customer information, theft of competitive information, and related fraudulent activities, can be traced to insiders (Robert Willison, 2018), and there are many types of insiders that can pose a threat. The United States Cybersecurity and Infrastructure Secularity Agency (CISA) defines an *insider* as "any person who has or had authorized access to or knowledge of an organization's resources, including personnel, facilities, information, equipment, networks, and systems" (Chickowoski, 2018). In addition to employees, organizations' virtual nature has expanded insiders to include contractors, consultants, board members, outsourced business activities such as network engineers, software developers, product designers, logistics, sales, vendors, and maintenance services. It is challenging to ascertain the boundaries of insider versus an external threat.

The recent Solar Winds Solara breach highlights the problem of who or what is an insider threat. Solar Winds Orion software platform is used to monitor, analyze, and manage IT services. The password for their update server was *solarwinds123,* which hackers easily guessed (Canales, 2020). The attackers then installed malware into the Orion production software, and the compromised software was distributed to around 18,000 clients.

Losses from insider attacks can be significant (Crossler et al., 2013), and the average cost of an insider attack can exceed $8 million (Chickowoski, 2018). The collateral damage from a breach can lead to long-term customer loss, lawsuits, and severely damaged reputations. Despite the importance of insiders in security management, understanding how their hacking intentions are motivated, based on personal traits, is still lacking. This study addresses the gap in the literature by bringing attention to the dark triad, opposition to authority, and thrill-seeking traits and their influence on the white hat, black hat, and grey hat hacking intentions.

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?*

This research makes several contributions to the information security literature. Our study's first significant contribution is a set of dependent variable scales to measure behavioral intentions to engage in white hat, black hat, and grey hat hacking. The second significant contribution is integrating psychological variables with the economics of crime and rational choice theory frameworks. We included a construct for determining if the probability of being apprehended along with the dark triad, opposition to authority, and thrill-seeking traits influence an individual's propensity to engage in hacking activities.

RESEARCH ON CYBERSECURITY AND HACKING MOTIVATION

A rich tradition surrounds the hacking persona and the accompanying stereotype. Eric S. Raymond presented a portrait of the so-called random hacker that resonates today (Raymond, 2004). He described the typical hacker as curious, introverted, and intelligent anti-conformists who had trouble with emotions. He noted that typical hackers wore Birkenstocks or went barefoot, wore tie-dyed t-shirts, and were primarily scruffy hairy males with libertarian political inclinations. Raymond also suggested they had higher rates of attention-deficit syndrome and detested Smurfs, Ewoks, Microsoft, COBOL, and BASIC.

A modern-day candidate for the prototypical hacker is Elliot Alderson in the Mr. Robot television series. Mr. Robot is anti-establishment and anti-capitalism, with a dissociative identity disorder (Volmar,

2017) (Herzog, 2015; Smith, 2019). Elliot is essentially an amalgam of the grey hat and white hat hacker, whereas his nemesis is a psychopathic black hat. Mr. Robot has been touted in the popular press as a breath of fresh air, different from earlier portrayals of hackers in film and television.

> "But the show nails the anthropology of hacking, which is fascinating as all get-out. The way hackers decide what they're going to do, and how they're going to do it, is unprecedented in social history, because they make up an underground movement that, unlike every other underground in the past, has excellent, continuous, global communications. They also have intense power struggles, technical and tactical debates, and ethical conundrums—the kind of things found in any typical *Mr. Robot* episode. "(Doctorow, 2017)

The *Mr. Robot* description sounds a lot like the description of the hacker that Raymond put forth many years earlier. One of the goals of this research is to understand the psychological underpinnings that lead to being attracted to hacking.

Prior Research

There are few studies involving insider threat behavior (M. Maasberg, Warren, & Beebe, 2015). The psychological profiling of hackers has attracted substantial recent research interest, but the empirical results are limited (Crossler et al., 2013; Dhillon, Samonas, & Etudo, 2016; Kajtazi, Bulgurcu, Cavusoglu, & Benbasat, 2014; Roy Sarkar, 2010; Safa, Maple, Watson, & Von Solms, 2018; Warkentin, Vance, & Johnston, 2016). There are two reasons for the limited empirical research on insider threats. One reason for the lack of insider information is that organizations are not eager to report insider attacks: an estimated 70% are not reported ("WRIT 2018," 2018). This lack of reporting relates to concerns about privacy issues, litigation, and the possibility that such revelations would harm the organization's reputation (Soh, Yu, Narayanan, Duraisamy, & Chen, 2019).

Another reason for the paucity of data is that many breaches are undetected—but that does not mean organizations have not been compromised. As noted by the United States Cybersecurity and Infrastructure Security Agency (CISA), there are two types of organizations: "those whose members have already stolen intellectual property, and those who simply do not know it yet" (CISA, 2020). CISA has identified a list of predisposition attributes and stressors that could impact an insider to become a threat (see Table 1). These characteristics have not been validated using conventional research and empirical methods.

TABLE 1
VARIABLES THAT ARE RELATED TO INSIDER THREAT

Characteristics of Insiders at Risk of Becoming a Threat (CISA, 2020)	
• Alcoholism • History of rules violations • History of criminal conduct • Convictions • History of aggression and violence • Self-injury	• Lack of social skills • Inability to get along with others • Compulsive behavior • Psychopathy • Narcissism

Psychological Research on Hackers

Freed (Freed, 2014) found that cybersecurity specialists differ from IT professionals. She compared 72 cybersecurity professionals and 46 information technology employees and found that cybersecurity specialists have significantly higher Openness, Assertiveness, Extraversion, and Adventurousness scores and significantly lower Agreeableness, Sympathy, Trust, Vulnerability, and Self-Consciousness scores.

Many hackers are motivated by what they dislike, rather than what they do like (Madarie, 2017). This may account for the discrepancies between what "experts" believe motivates hackers and what motivates them. Hacking frequency is driven by peer recognition, respect, and the opportunity to engage in team play, not by intellectual challenge, curiosity, or even the pursuit of justice. Motivations identified for participating in hacking behavior include revenge, ideology, fun, thrills, survival, notoriety, recreation, and profit (Crossler et al., 2013; Seebruck, 2015).

There has been an increased interest in using the dark triad to understand the motivation to participate in hacking. The *dark triad* refers to a group of three personality traits that are considered socially undesirable. They include *Machiavellianism* (manipulative, deceitful, and exploitive), *narcissism* (self-centered and attention-seeking), and *psychopathy* (lack of remorse, cynical, and insensitive) (Jonason & Webster, 2010; Jones & Paulhus, 2017; Paulhus & Williams, 2002). These measures are related, but they are nevertheless distinct constructs (Jones & Paulhus, 2014; Paulhus & Williams, 2002). Many of the dark triad personality traits are used by the press and by security experts to describe criminal activity by insiders. They have been postulated as important psychological traits contributing to interests in hacking and other inappropriate cyber activities. In a study of 324 adolescents between 14 and 18, cyber-aggression was related to psychopathy. *Cyber-aggression* included spreading rumors, insulting, damaging personal reputations, and hacking Facebook accounts. However, narcissism and Machiavellianism were not associated with cyber-aggression (Lopes & Yu, 2017; Pabian, De Backer, & Vandebosch, 2015). Antisocial trolling has been associated with high scores on the dark triad (Lopes & Yu, 2017).

A survey of 768 Amazon Mechanical Turk (AMT) IT professionals found that Machiavellianism, narcissism, and psychopathy were related to sympathy for an individual who posted salary information of higher-paid coworkers (M. Maasberg, Van Slyke Crag, Ellis, Selwyn, Beebe, Nicole, 2020). However, that study reported limited statistical results; they only reported beta weights for the dark triad and did not include any correlations or model fit indices.

Another recent study investigated the relationships between computer abuse, narcissism, psychopathy, and other personality variables (Seigfried-Spellar, Villacis-Vukadinovic, & Lynam, 2017). In the study, 235 AMT respondents participated an extensive survey containing 200 items. Emotional stability had a 0.08 correlation with total computer crime (r^2 = 0.01), disinhibition had a 0.37 correlation with total computer crime (r^2 = 0.14), and the correlation between narcissism and total computer crime was 0.26 (r^2 = 0.07).

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 in hacking communities (Holt, 2010), academic communities (Farooqi et al., 2017; Lee, 2017; Mahmood, Siponen, Straub, Rao, & Raghu, 2010), and the popular press (Hoffman, 2017). Conceptual clarity is essential for theory development (Weber, 2012), so we developed a scale to structure and clarified the meanings of the white hat, grey hat, and black hat constructs. *White hat hackers*, sometimes referred to as *ethical hackers* (Palmer, 2001), assist system owners in detecting and fixing security system vulnerabilities. They are referred to as ethical hackers because they do not violate laws, even though they use many of the same tools as black hat and grey hat hackers.

Black hat hackers, sometimes called *crackers*, are typically motivated by personal gains from illegally breaching computer systems (Krit & Haimoud, 2016). However, they might also be social mischief-makers seeking the thrill of the attack, revenge, or notoriety. *Grey hats* tend to have ideological motivations that translate to hacking attacks against an adversarial political position, a company policy, or nation-state. The grey hat hacker lies somewhere between the extremes of black hat and white hat hacking by operating on the fringe of criminal and civil liability (Kirsch, 2104). Grey hats are sometimes referred to as *hacktivists*. They can be white hats by day and help their companies to detect and mitigate flaws in systems and, at night, engage in ideological hacking activities to correct perceived wrongs.

Economics of Crime Literature

Engaging in criminal activity involves choices of consequences and opportunities, and individuals perceive them differently. Becker's paper on the market for criminal activity posits that potential criminals examine returns on an illegal activity as a function of the probability of being apprehended and the severity of the punishment. Individuals can be deterred, despite possible monetary gains, if the probability and severity of punishment are sufficiently high (Becker, 1968; Levitt, 2017). The market model assumes that offenders have expectations about returns, the potential for being caught, and the resulting punishment (Gaia et al. 2020).

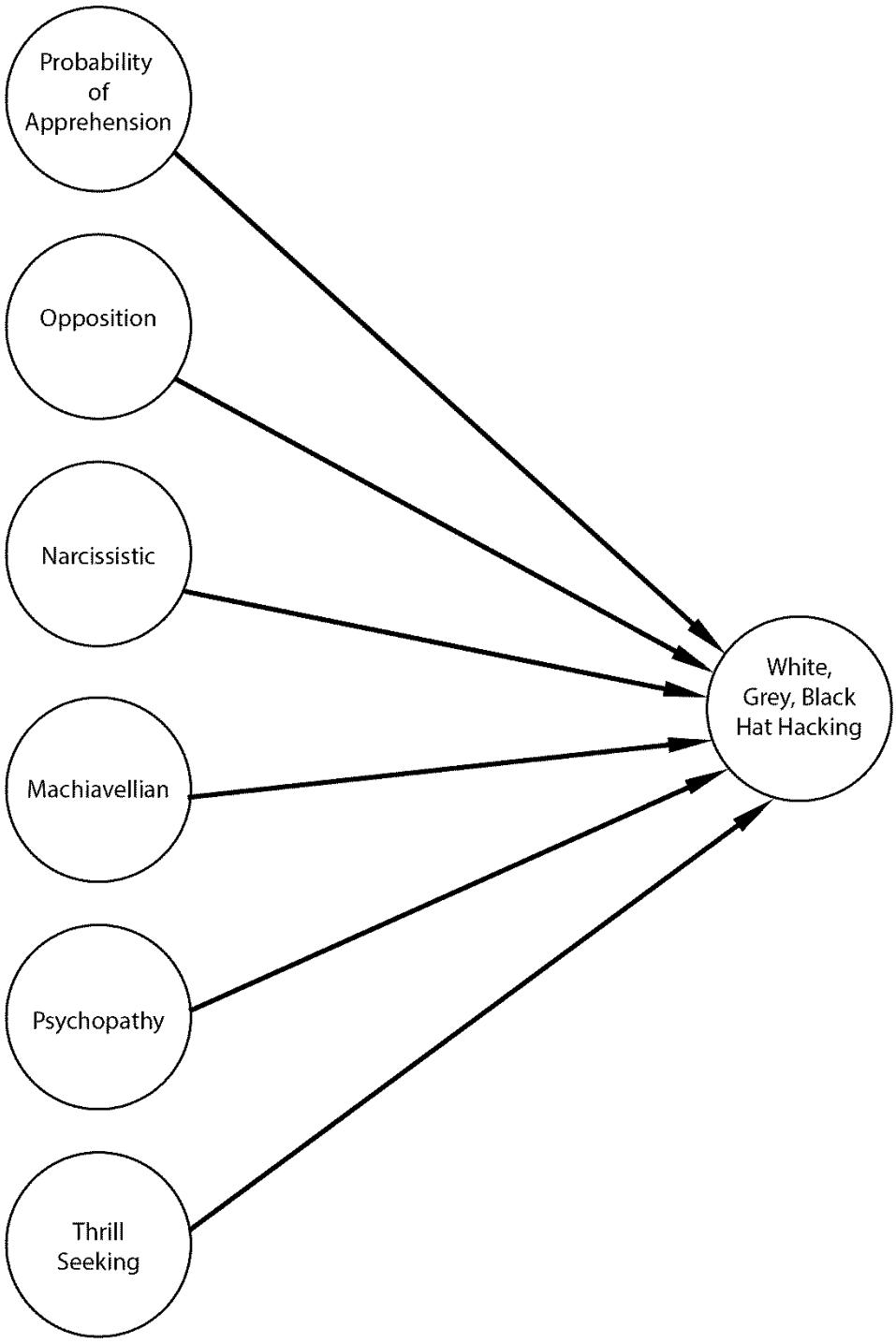
The economics of crime literature assumes that wrongdoers use a calculus of rational choice in determining whether to engage in criminal activity (Becker, 1968; Loughran, Paternoster, Chalfin, & Wilson, 2016). There are ongoing discussions by behavioral economists concerning rational decision-making. Behavioral economists do not abandon the notion that humans can be rationale, but they think that there are situations in which decision-making is less than rational and that more robust models are needed to understand the vagaries of human behavior (Jolls, Sunstein, & Thaler, 1998; Kahneman & Tversky, 1979; Thaler, 2008, 2017; Tversky & Kahneman, 1992). In this study, we will draw on a combination of traditional economics, behavioral economics, and psychological motivation to model choice behavior related to hacking behavior and criminal activity.

RESEARCH MODEL AND HYPOTHESIS

We intend to understand the role of five psychological variables and the probability of being apprehended, in relation to the attractiveness to participate in white hat, grey hat, and black hat hacking. Figure 1 presents the conceptual model depicting relationships between hacking motivations, personal traits, and three types of hacking intentions. We argue that five individual factors influence the three types of hacking intentions differently, moderated by different probabilities of being apprehended in different situations.

Our first hypothesis is related to the psychology of hackers. For example, Maasberg et al. (M. Maasberg et al., 2015) proposed a research model that integrated the dark triad and the capability, motive, and opportunity (CMO) framework. We also draw on several research studies investigating the relationship between computer abuse and crime as influenced by narcissism, Machiavellianism, and psychopathy as additional justification (M. Maasberg, Van Slyke Crag, Ellis, Selwyn, Beebe, Nicole, 2020; Nevin, 2015; Pabian et al., 2015; Seigfried-Spellar et al., 2017).

FIGURE 1
RESEARCH MODEL



H1: *The dark triad, Machiavellianism, narcissism, and psychopathy are essential predictors of interest in white hat, grey hat, and black hat hacking.*

Thrill-seeking behavior has been consistently touted as a motivation for hacking (Rogers, 2006; Rogers, Seigfried, & Tidke, 2006). Thrill-seekers derive pleasure from the excitement of hacking (Bachmann,

2010). Indeed, some believe that the days of the hacker as a thrill-seeker have morphed into the larger role of state-sponsored hackers (Waldrop, 2016). We included a thrill-seeking scale because it is used to describe many individuals who are attracted to hacking (Seigfried-Spellar et al., 2017) because many hackers are motivated by a combination of fun, thrill-seeking, excitement, and curiosity (Madarie, 2017).

H2: *Interest in thrill seeking is an essential predictor of interest in white hat, grey hat, and black hat hacking.*

In the form of hacktivism, civil disobedience has emerged as a go-to strategy for disrupting organizational and even national activities (Sauter, 2014). Trolls and hackers have much in common (Lopes & Yu, 2017). There is some evidence that boredom, attention-seeking, and revenge motivate both trolls and hackers. However, hackers seem to be driven by freedom of expression and an anti-bureaucracy orientation and a mistrust of authority (Shachaf & Hara, 2010). We included a scale for *opposition to authority* to determine if this construct influenced engagement in one of the three hat activities (Seigfried-Spellar et al., 2017).

H3: *Opposition to authority is an essential predictor of interest in white hat, grey hat, and black hat hacking.*

Engaging in criminal activity involves a choice involving opportunities and consequences, and individuals perceive them differently. Our intention is to integrate the economics of the crime model with key psychological variables. The issue is whether individuals can be deterred if there is a high perceived likelihood of being apprehended (Myers, 1983). As noted earlier, the market model for crime assumes that offenders, victims, and law enforcement engage in optimizing behaviors related to their preferences and that offenders have expectations about returns, and individual sensitivity for being caught and the resulting punishment (Levitt, 2017). Thus, we include a construct to determine if the probability of being apprehended moderates the tendency to engage in black hat and grey hat hacking activities. White hat hacking is not illegal, and therefore it will not have an effect on the propensity to engage in that type of hacking.

H4: *The probability of being apprehended moderates interest in grey hat, and black hat hacking, but not white hat hacking.*

Scale Development for the Hacking Typology

Scales were developed by surveying the academic and professional literature and having discussions with experts in security and privacy research. The six white hat items include technical and social engineering hacking behaviors. Social engineering hackers exploit people and systems through the social manipulation of people, involving interactions that use disguises, ploys, and psychological tricks to achieve intrusion (Applegate, 2009; Erbschloe, 2005). This is in contrast to technical attacks that require sophisticated knowledge to attack a system. The four black hat items involve financial attacks that are motivated by personal gains for breaching computer systems. These activities are typically illegal. The three grey hat items are in the middle ground. They are ideological activities engaged in correcting a perceived wrong, and they might be unlawful.

The study follows the criteria recommended by Agarwal and Prasad (Agarwal & Prasad, 1998) for choosing survey items, removing items that are not relevant to the specific innovation examined in the study, and deleting items that are similar to other items. By using these criteria, the selected items ensure complete coverage of the constructs at hand. The various hat items represent behavioral intentions to engage in white hat, grey hat, and black hat hacking. We initially identified 18 items for the hat typology and then reduced them down to 16 items based on item analyses. We removed two items from the grey hat scale because of the overlapping coverage manifested by the variance inflation factor being above five. The wording for the scales and the item loadings for all of the scales can be found in Appendix 1.

The Dark Triad, Thrill Seeking, and Opposition to Authority Constructs

We chose the Dark Triad Dirty Dozen for this study because these concise scales contain only four items for Machiavellianism, narcissism, and psychopathy (Jonason & Webster, 2010). These scales also have been used extensively, have reasonable psychometric properties with acceptable convergent and discriminate validity, and have been adapted for several cultures (Czarna, Jonason, Dufner, & Kossowska, 2016; Jonason & Luevano, 2013; Ozsoy, Rauthmann, Jonason, & Ardic, 2017; Savard, Simard, & Jonason, 2017).

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 (Volmer, Koch, & Goritz, 2016). A German study found that leaders with Machiavellianism and psychopathy personality traits were detrimental to employee well-being. In contrast, subordinates rating leaders 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 that we are not trying to detect whether the respondents are, for example, psychopaths; instead, we are investigating the association between the propensity to engage in white, black, or grey hacking behavior and the level of psychopathy.

As noted earlier, it is often assumed that hackers are thrill-seekers. Many hackers are motivated by fun, thrill-seeking, excitement, and curiosity (Madarie, 2017). This study uses a thrill-seeking scale that Seigfried-Spellar et al. (Seigfried-Spellar et al., 2017) used to examine computer crime and abuse. Hackers are often viewed as being anti-bureaucratic and mistrusting authority (Rogers et al., 2006). We, therefore, included an *opposition to authority* scale to determine if this construct influenced engagement in one of the three hat activities (Seigfried-Spellar et al., 2017).

Probability of Being Apprehended

The *probability of being apprehended* construct was initially developed as part of another large study involving 523 subjects and was focused on the economics of crime (Gaia et al. 2020). That study's objective was to identify the role of monetary incentives in violating HIPAA regulations and privacy laws in the next generation of employees. The research model was developed using the economics of crime and rational choice theory frameworks to identify situations in which employees might engage in illegal breach behaviors.

We developed four scenarios to determine if the probability of being apprehended increases the level of monetary incentives necessary to encourage people to violate HIPAA laws through obtaining health care information illegally and releasing that information to individuals and media outlets. The four scenarios were used to construct a latent variable labeled the *probability of being apprehended* and measure each subject's perceived likelihood 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 take to make this acceptable? … What do you think is the likelihood of getting caught if you accept the money?*

DATA COLLECTION AND ANALYSIS

We recruited subjects from sophomore and junior undergraduates majoring in management and computer science enrolled at a state research institution in the northeastern United States. All subjects participated in the survey voluntarily; they were advised that they could withdraw from participation at any time without penalty. All 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 that studying these two populations, management, and computer science students, provides a solid

foundation for researching and investigating other populations. They will be entering the workforce in the immediate future, and from our experience, they are less concerned with issues of social desirability.

It is challenging to get actual organizations to participate in this kind of study. That is, organizations do not want to risk reputation damage and social desirability bias, and therefore, organization employees would serve as poor candidates for this type of study. Personality data gathered from employees is usually biased and unreliable. *Social desirability bias* is a problem in studies involving abilities, personality, and illegal activities. It occurs when subjects are less prone to answer questions truthfully to diminish their social prestige (Akbulut, Donmez, & Dursun, 2017; Dodou & de Winter, 2014). Individuals tend to over-report "good behavior" and under-report "bad behavior." Subjects often tend to deny Illegal acts.

We removed from the analysis any subjects who were missing more than 10% of the values or took less than two minutes to complete the survey because speedy responses tend to introduce noise into the results (Greszki, Meyer, & Schoen, 2015). The number of valid surveys was 439, with a participation rate of 92%. There were 246 students from the school of management and 193 students from computer science in the study. 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. Partial least squares (PLS) analysis is robust, resistant to statistical inadequacies, and effective in handling complex multidimensional constructs (Henseler & Chin, 2010). Because our research model includes six reflective sub-latent variables and we were also interested in prediction, PLS deems suitable for this research (Henseler, 2018). We tested the white hat, grey hat, and black hat models separately; we report only the significant paths to make the exposition and explanation clearer. The *p* values were generated using 500 bootstrapped samples.

Measurement Assessment

We examined individual loadings and internal consistency to test for item reliability. Loadings for all measurement items were above 0.7, except for one of the narcissism items for the grey hat model (Narc1 with an outer loading of 0.625). Table 2 illustrates that Cronbach's alpha for every construct was greater than 0.7, thus indicating internal reliability (Werts, Linn, & Joreskog, 1974). We assessed discriminant validity using the average variance extracted (AVE). The square root of the AVE should be higher than the correlations among the constructs. Table 2 shows Cronbach's alpha, the composite reliability, and the average variance extracted for the constructs.

TABLE 2
LATENT VARIABLE STATISTICS

Independent Variables			
	Cronbach's 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	0.912	0.723
Probability of being apprehended	0.885	0.920	0.743
Dependent Variables			
	Cronbach's Alpha	Composite Reliability	Average Variance Extracted
White hat	0.953	0.962	0.782
Black hat	0.903	0.933	0.778
Grey hat	0.895	0.934	0.826

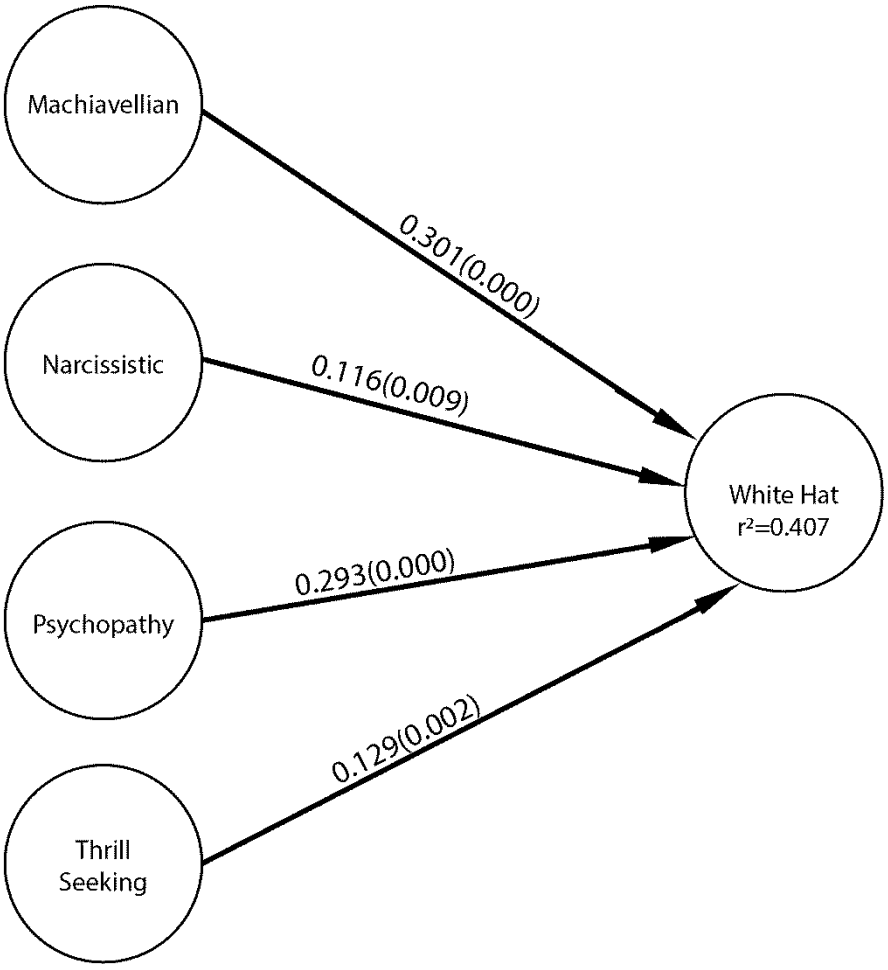
Model Assessment

The essential criterion for evaluating PLS path models is the r^2, or the *coefficient of determination*. All of the r^2 values for the models were above 0.29. According to Cohen (Cohen, 1992), a small r^2 effect size is less than approximately 0.14, a medium effect size is between 0.14 and 0.26, and a large effect size is greater than 0.26. All the effect sizes were greater than the threshold of the medium effect size.

White Hat Results

The r^2 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 strong predictors of individuals attracted to white hat hacking (see Figure 2). The *p* values for the model coefficients are in parentheses. As anticipated, the probability of apprehension was not a significant predictor of white hat hacking because white hat hacking is not illegal. Recall that we are not showing paths with non-significant *p* values to simplify the presentation of the results.

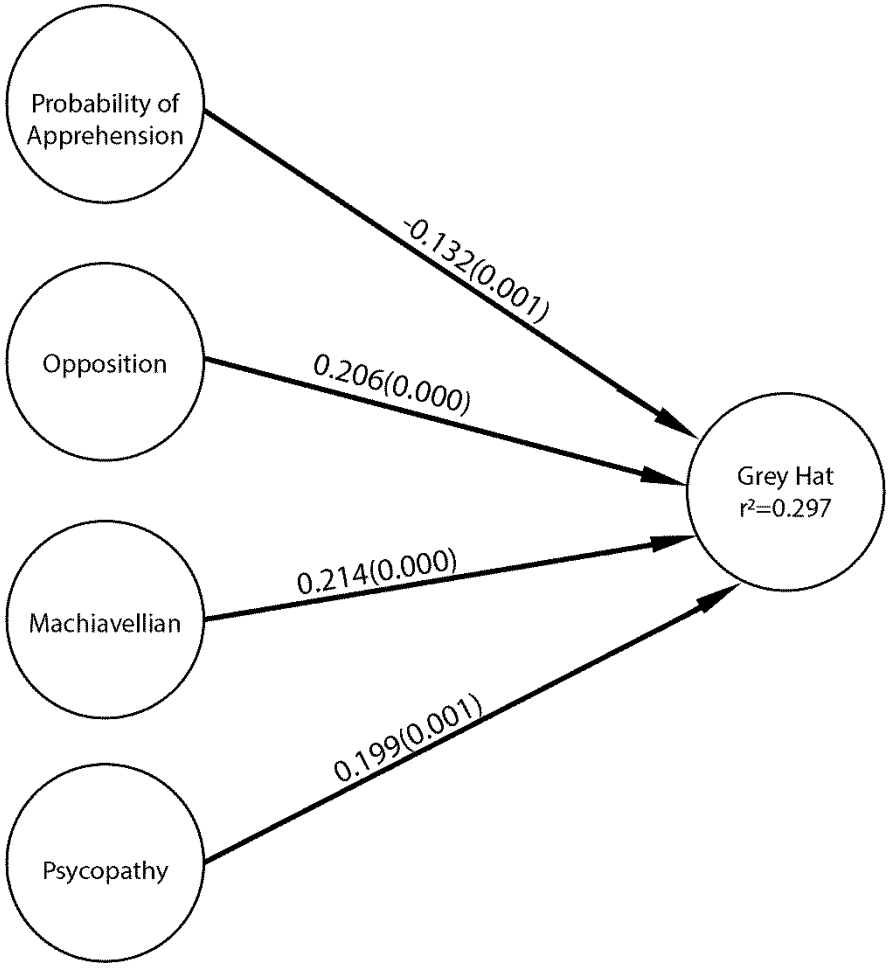
FIGURE 2
WHITE HAT MODEL RESULTS



Grey Hat Results

The r^2 for the grey hat model was 0.297. Opposition to authority, Machiavellianism, and psychopathy were statistically significant predictors of attraction to grey hat hacking (see Figure 3). The *p* values for the model coefficients are in parentheses.

FIGURE 3
GREY HAT MODEL RESULTS

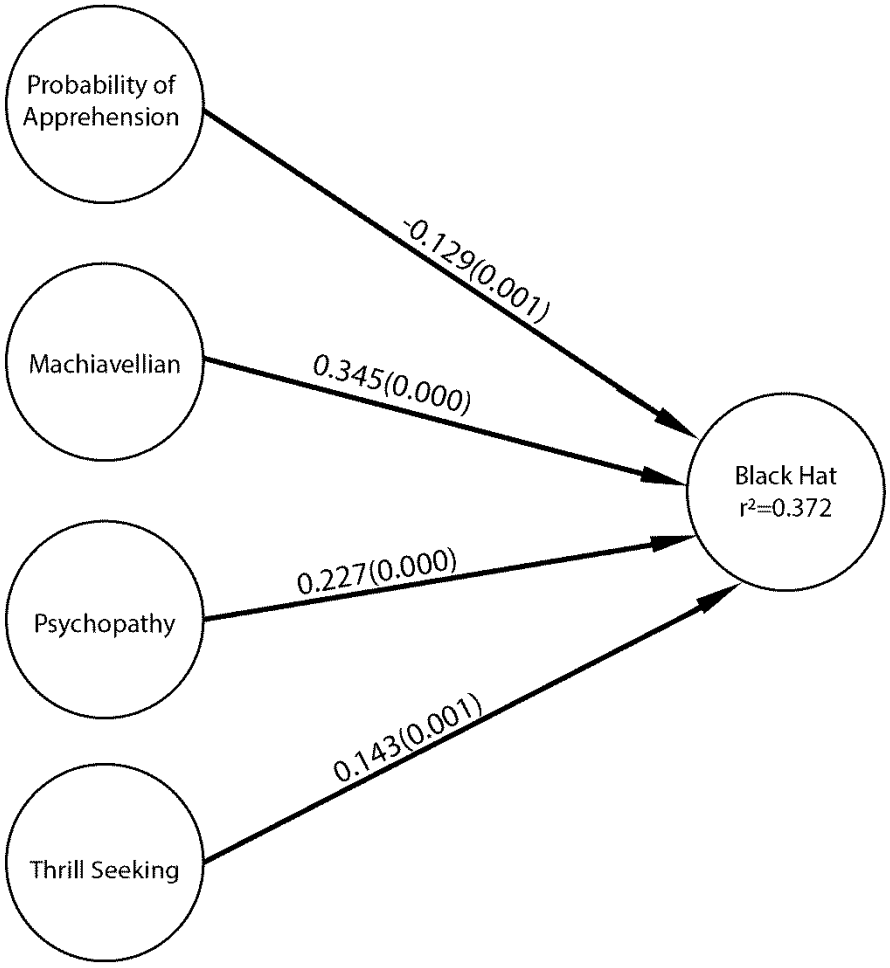


We anticipated that individuals attracted to grey hat hacking would be higher on the opposition to authority scale because they would have ideological motivations that translate to actions against political figures, company policies, or even nations. A priori, we were not sure that opposition to authority would be statistically significant for white hats and black hats. Opposition to authority was not a significant predictor of attraction to white hat and grey hat hacking. The coefficient for the probability of apprehension was negative and statistically significant. This result supports the deterrence effect of the perceived probability of being caught.

Black Hat Results

The r^2 for the black hat model was 0.372. Thrill-seeking, Machiavellianism, psychopathy, and the probability of apprehension were statistically significant predictors of attraction to black hat hacking (see Figure 4). The *p* values for the model coefficients are in parentheses.

FIGURE 4
BLACK HAT MODEL RESULTS



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 any type of crime, particularly for younger people (Hirschi & Gottfredson, 1983). Thrill-seeking relates to curiosity, the desire for knowledge, and adaptation (Reio, Petrosko, Wiswell, & Thongsukmag, 2006). A black hat is primarily motivated by personal gains from breaching computer systems illegally and might also be mischief-makers who are in it for the thrill of the attack and for notoriety. The coefficient for the probability of apprehension was negative and statistically significant, thus supporting the deterrence effect of the perceived probability of being caught in black hat hacking.

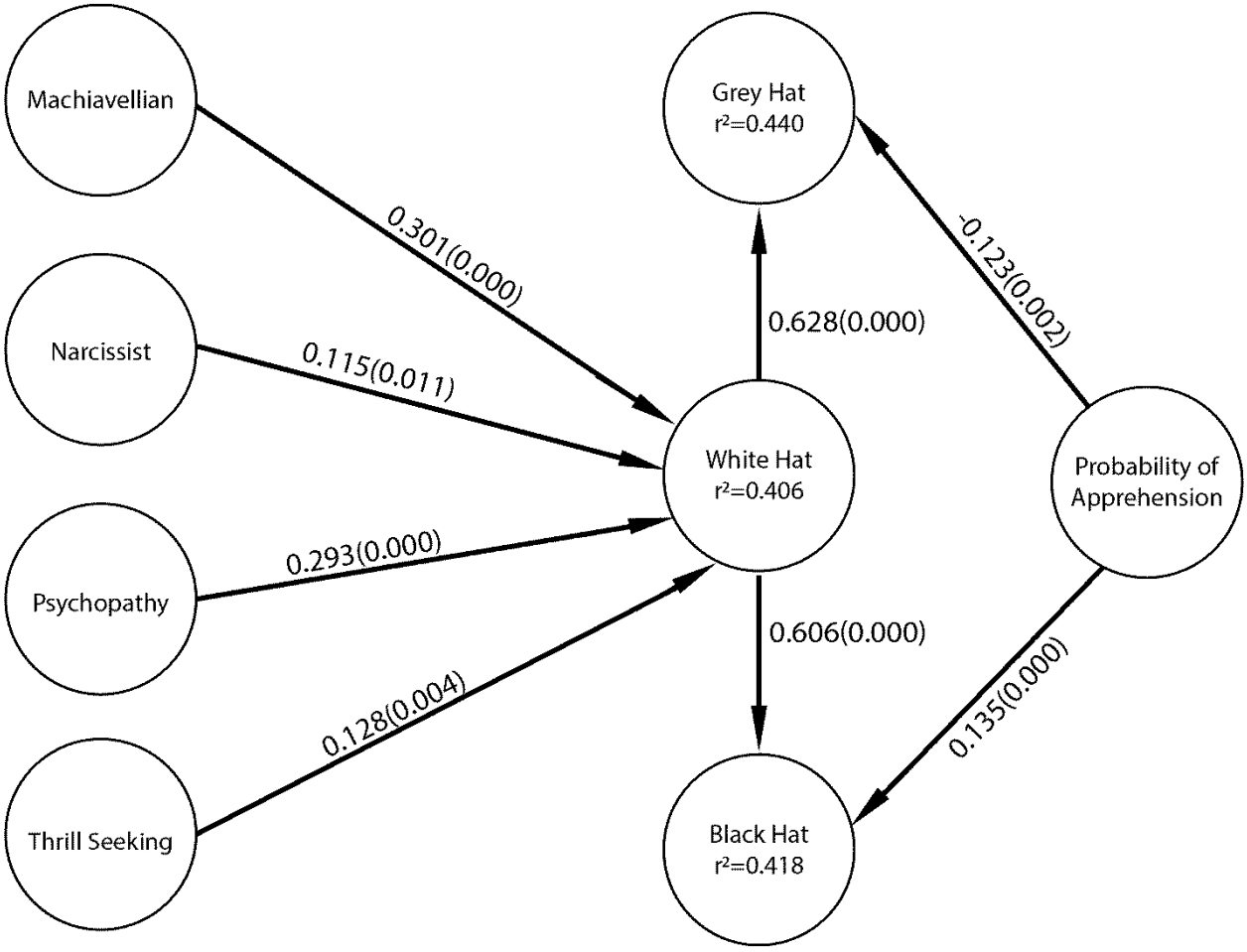
Will White Hat Hacking Lead to Grey Hat and Black Hat Hacking?

A natural question is whether white hat hackers would drift to becoming grey hat or even black hat hackers. A famous example of this drift to the dark side can be found in *American Kingpin* (Bilton, 2017). It is the story of Ross Ulbricht, who developed the darknet market website called Silk Road. One of the government agents investigating him was subsequently lured to the criminal side because of the monetary attraction. Recent research suggests that monetary incentives can play an essential role in the next generation of employees' propensity to violate privacy laws.

Machiavellianism, narcissism, psychopathy, and thrill-seeking again predicted attraction to white hat hacking. Psychopathy and Machiavellianism were especially strong predictors of attraction to white hat

hacking (see Figure 5). The r^2 for the white hat construct was 0.406. The r^2 for the grey hat construct was 0.440, and for the black hat, the construct was 0.418. The coefficients for the probability of apprehension were negative and statistically significant for both black hat and grey hat hacking, thus supporting the deterrence effect of the perceived probability of being caught for both. The implication is that, given the right situation, a white hat hacker would drift toward the dark side.

FIGURE 5
WHITE HAT HACKING AS AN ANTECEDENT TO BLACK HAT AND GREY HAT HACKING



Comparing Management and Computer Science Students

Our original research model did not include a comparison because we were unsure if the two groups would differ in terms of how the independent variables would affect the propensity to participate in hacking. Figure 6 shows the trimmed significant paths for the 246 management students. The probability of apprehension, Machiavellianism, narcissism, psychopathy, and thrill-seeking again predicted attraction to white hat hacking; Machiavellianism was the strongest predictor. The r^2 for the white hat construct was 0.395. The r^2 for the grey hat construct was 0.387, and for the black hat, the construct was 0.321.

FIGURE 6
MANAGEMENT MODEL

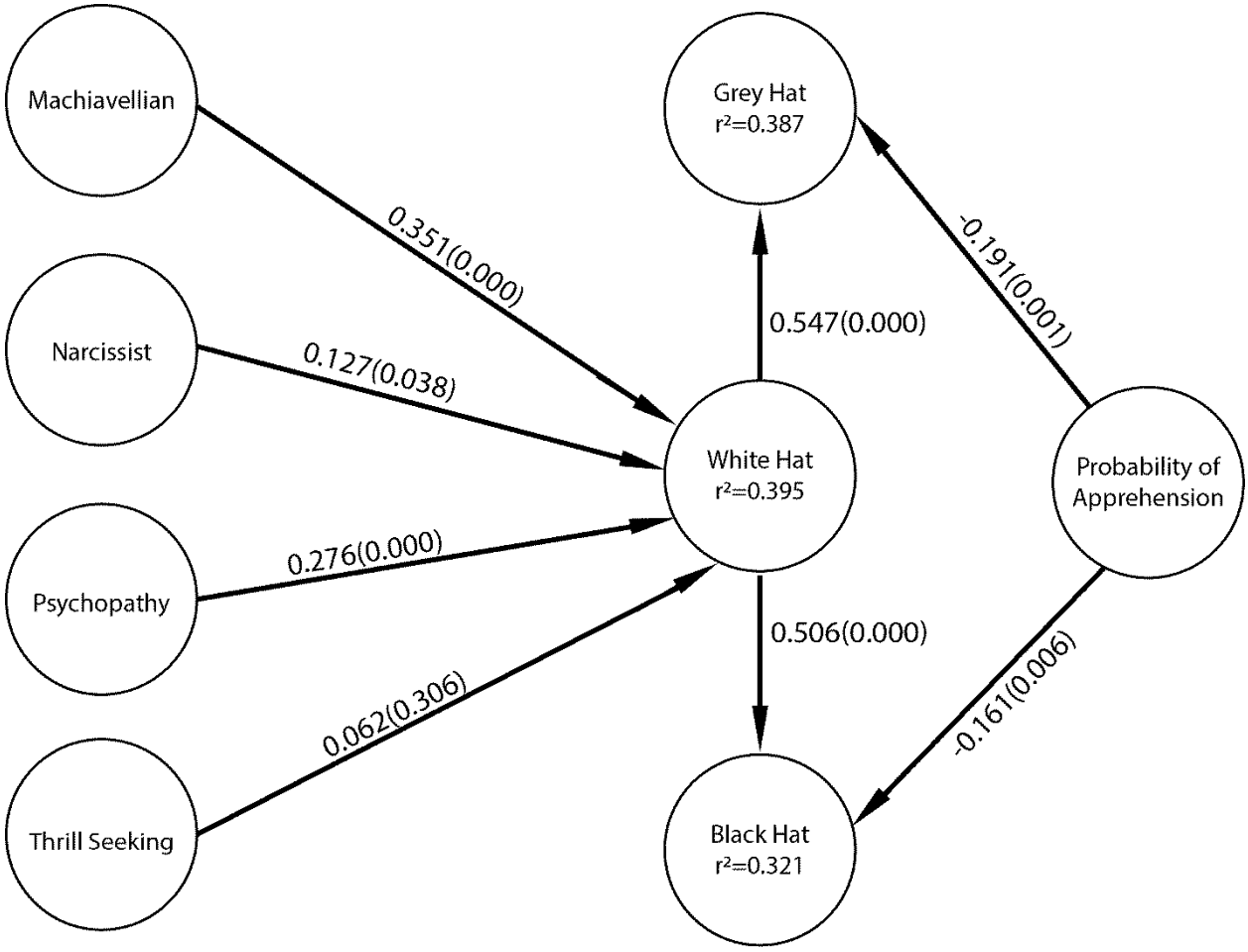
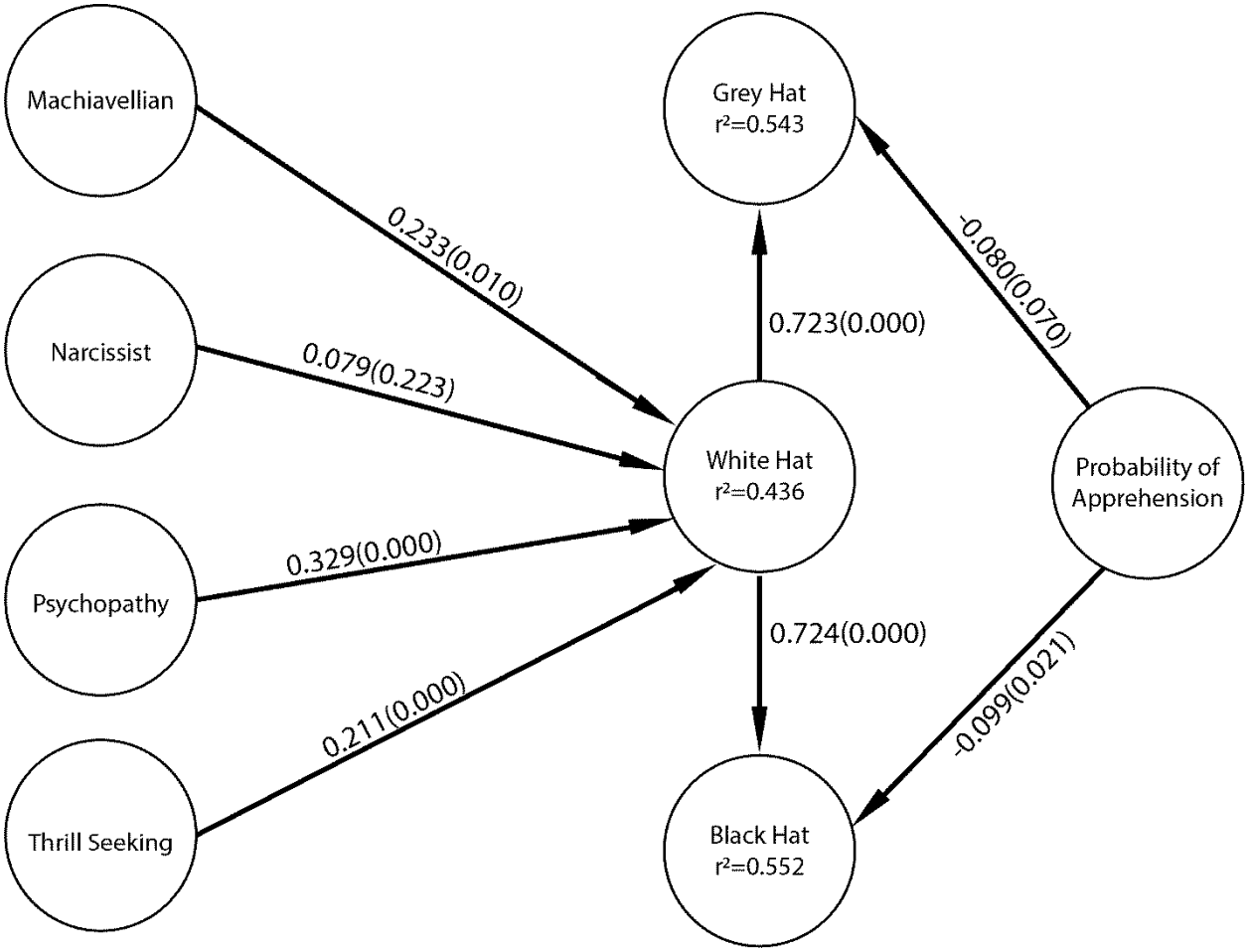


Figure 7 shows the trimmed results of the significant paths for the 193 computer science students. Machiavellianism, psychopathy, and thrill-seeking were predictors of attraction to white hat hacking; psychopathy was the strongest predictor. The r^2 for the white hat construct was 0.436. The r^2 for the grey hat construct was 0.543. For the black hat construct, it was 0.552. Interestingly, unlike the management students, the probability of being apprehended did not statistically influence the model. The coefficients for the perceived probability of being caught were lower for computer science students than for management students and were not significant for grey hat hacking. The implication is that a perceived higher probability of being caught will deter management students from black hat and grey hat hacking more than computer science students.

FIGURE 7
COMPUTER SCIENCE MODEL



CONCLUSION

Organizations can engage in several activities to prevent or reduce the impact of security breaches. For example, preventive measures like sophisticated monitoring technologies and multi-factor authentication can be used to preclude unauthorized access to buildings, software, and databases. Organizations can monitor and record privileged activity sessions as users access files, folders, databases, servers, applications, hardware, and buildings. Organizations typically focus on technical preventives because they are 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 and education, legal campaigns, and fear appeals.

Using the dark triad personality traits to evaluate new employees as security threats is possible (M. Maasberg et al., 2015). However, this strategy should be approached cautiously for practical, ethical, and privacy reasons. We found that white hat hackers have Machiavellian, narcissism, psychopathy, and thrill-seeking traits. However, that does not mean they will migrate to become black hats. More importantly, they are needed to counter black hat and grey hat attacks.

Even if surveys like the Dark Triad Dirty Dozen are administered to potential employees, the results will undoubtedly be biased. Prospective employees may not answer such questions truthfully because they will not want to diminish their social prestige (Akbulut et al., 2017; Dodou & de Winter, 2014). People tend to over-report "good behavior" and under-report "bad behavior." Being deceitful and manipulative, lacking

remorse, and being unconcerned with the morality of one's actions certainly diminish one's social prestige. Indeed, we were 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. Such a tactic would, of course, present numerous social, legal, and ethical issues.

The Carnegie Mellon University Software Engineering Institute (SEI) has identified detailed procedures in its guide for countering insider threats (T. Michael et al., , 2019). These guidelines are extensive, including policymaking, the development of organizational control and monitoring systems, hiring practices, privileged access guidelines, and addressing behavioral issues. An important takeaway from the SEI insider report is the use of positive incentives such as connecting, engaging, and supporting employees along with negative incentives in the form of restrictions, monitoring, sanctions, and punishments. Positive incentives are more effective in achieving security when using small teams. The net result is that positive incentives might reduce the frequency of insider misbehavior. However, as noted by CISA, detecting and dealing with insider threats is a complex issue. Table 3 presents an overview of the issues involved in developing a successful mitigation strategy to counter insider threats (CISA, 2020).

TABLE 3
KEY POINTS FROM CISA (2020) RELATED TO INSIDER THREATS

- A successful program will recognize that the **insider threat evolves over time and exhibits multiple overlapping detectable and observable behaviors.**
- **Behavior is what matters most**, not the motivation, whether it is political, religious, ideological, financial gain, or revenge.
- **Confirmation of any threat indicator requires a solid understanding of context**; recognizing that people often display behaviors representative of an individual point in their life that may not result in a direct expression of a threat.
- **Exhibiting no indicators does not guarantee that a person will not pose an insider threat**.
- **Professional stressors have the additional effect of creating potential grievances** against an employer, organization, or agency.
- **Behavioral indicators reflect patterns of activity over time**, based on the way the insider interacts within the organization. These indicators are directly observable by peers, HR personnel, supervisors, managers, and technological systems.
- **Technical indicators are those that require direct application of IT systems and tools to detect.** UAM is the most frequently used application for the detection of technical insider threat indicators.
- **Violence carries specific behaviors or collections of behaviors** that instill fear or generate a concern that a person might act out violently.
- **People are key sensors for the detection and identification of an insider threat.** People may have an awareness of the predispositions, stressors, and behaviors of insiders who may be considering taking violent actions toward an organization.
- **Those who perpetrate violence or steal data or secrets often leak their plans or grievances.** It is well established that a person of concern will tell others of their intent or plan at a much greater rate than they will tell the target of their plan.
- As part of an organization's or business' obligation to provide a safe environment, the **insider threat policies and programs should always consider a commitment to support domestic violence victims** and to take protective steps when such violence threatens to intrude on the workplace or organization.

Hacking knowledge is a two-edged sword that can be used for mischief and to counter 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 a security training class online or even in person. Employees need to be immersed in security training, receive feedback, and interact with other employees on security issues (Yoo, Sanders, & Cerveny, 2018).

As noted earlier, wrongdoers use a calculus of rational choice in determining whether to engage in criminal activity (Becker, 1968; Gaia, Wang, Yoo, & Sanders, 2020; Loughran et al., 2016). This calculus is affected by an individual's personality traits 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. Research has shown that higher perceptions of getting caught can be a deterrent to committing cybercrime. In this study, this relationship was only held for the management students. This relationship did not hold for computer science students in the study. The real dilemma is that the probability of being apprehended and convicted is exceedingly small (Gaia et al., 2020). Between April 2003 and July 2018, 186,453 health information privacy complaints were submitted to the US Department of Health and Human Services. However, the Department of Justice levied very few fines and jail sentences during that period. One security expert estimated that for every individual who gets caught, 10,000 people go free and for every individual prosecuted successfully, 100 go free or just receive a warning (Gaia et al., 2020).

FUTURE RESEARCH

The COVID-19 pandemic has placed additional stress on society, companies, and individuals. Forrester estimates that one in three data breaches in 2021 will come from insiders and that the number of insider incidents will increase by 25% because of the COVID-19 pandemic because of the rapid push to remote work, employee feelings of job insecurity, and the ease of moving stolen company data because of the nature of the cloud and the availability of large data pipelines (Weston, 2020).

Further validation of the white hat, grey hat, and black hat constructs is the next step. It would also be desirable to obtain a sample from a variety of organizations and industries. Caution is needed because data from organizations where employees will be guarded when they are asked if they would participate in grey hat and black hat activities because trust and social desirability issues loom large with individuals already in the workforce.

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 organizational security policies (Safa et al., 2018). These theories have the potential to assist an organization in developing behavioral approaches to curb insider threats. The changing dynamics of societal systems and the stress it has placed on employees will need to be addressed. Future research will need to address and replicate the findings in a more age-diverse sample across a multi-generational workforce.

ACKNOWLEDGEMENT

This material is based upon work supported by the NSF under Grant No. DGE-1754085. An early version of this paper was presented at the 2020 Hawaii Conference on Systems Sciences.

REFERENCES

Agarwal, R., & Prasad, J. (1998). A conceptual and operational definition of personal innovativeness in the domain of information technology. *Information Systems Research*, *9*(2), 204-215. DOI 10.1287/isre.9.2.204

Akbulut, Y., Donmez, A., & Dursun, O.O. (2017). Cyberloafing and social desirability bias among students and employees. *Computers in Human Behavior*, *72*, 87-95. doi:10.1016/j.chb.2017.02.043

Applegate, S.D. (2009). Social Engineering: Hacking the Wetware! *Information Security Journal*, *18*(1), 40-46. doi:10.1080/19393550802623214

Bachmann, M. (2010). The Risk Propensity and Rationality of Computer Hackers. *International Journal of Cyber Criminology*, *4*(1-2), 643-656. Retrieved from <Go to ISI>://WOS:000437609000005

Becker, G.S. (1968). Crime and Punishment - Economic Approach. *Journal of Political Economy*, *76*(2), 169-217. doi:Doi 10.1086/259394

Bilton, N. (2017). *American kingpin: The epic hunt for the criminal mastermind behind the Silk Road*. New York: Portfolio/Penguin.

Canales, K. (2020). *A security expert reportedly warned SolarWinds in 2019 that anyone could access the company's update server with the password 'solarwinds123*'. Retrieved from https://www.businessinsider.com/solarwinds-warned-weak-123-password-could-expose-firm-report-2020-12

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

CISA. (2020, November). *Insider Threat Mitigation Guide.* Retrieved from https://www.publicpower.org/periodical/article/cisa-releases-insider-threat-mitigation-guide, https://www.cisa.gov/sites/default/files/publications/Insider%20Threat%20Mitigation%20Guide_Final_508.pdf

Cohen, J. (1992). A Power Primer. *Psychological Bulletin*, *112*(1), 155-159. doi:Doi 10.1037//0033-2909.112.1.155

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, *32*, 90-101. doi:10.1016/j.cose.2012.09.010

Czarna, A.Z., Jonason, P.K., Dufner, M., & Kossowska, M. (2016). The Dirty Dozen Scale: Validation of a Polish Version and Extension of the Nomological Net. *Frontiers in Psychology*, *7*. doi:ARTN 44510.3389/fpsyg.2016.00445

Data Breaches. (2019, June 12). Retrieved from https://www.privacyrights.org/data-breaches

Dhillon, G., Samonas, S., & Etudo, U. (2016). Developing a Human Activity Model for Insider IS Security Breaches Using Action Design Research. *Ict Systems Security and Privacy Protection, Sec 2016*, *471*, 49-61. doi:10.1007/978-3-319-33630-5_4

Doctorow, C. (2017). Mr. Robot Killed the Hollywood Hacker. *Technology Review*, *120*(1), 100-103. Retrieved from <Go to ISI>://WOS:000397833700024

Dodou, D., & de Winter, J.C.F. (2014). Social desirability is the same in offline, online, and paper surveys: A meta-analysis. *Computers in Human Behavior*, *36*, 487-495. doi:10.1016/j.chb.2014.04.005

Erbschloe, M. (2005). *Trojans, worms, and spyware: A computer security professional's guide to malicious code*. Amsterdam; Boston: Elsevier Butterworth Heinemann.

Farooqi, S., Ikram, M., De Cristofaro, E., Friedman, A., Jourjon, G., Kaafar, M.A., . . . Zaffar, F. (2017). Characterizing Key Stakeholders in an Online Black-Hat Marketplace. *Proceedings of the 2017 Apwg Symposium on Electronic Crime Research (Ecrime)*, pp. 17-27. Retrieved from <Go to ISI>://WOS:000408972400003

Freed, S.E. (2014). *Examination of personality characteristics among cybersecurity and information technology professionals* (Masters Thesis). The University of Tennessee at Chattanooga, Chattanooga, Tennessee, University of Tennessee at Chattanooga. Retrieved from https://scholar.utc.edu/theses/127/

Gaia, J., Wang, X.Y., Yoo, C.W., & Sanders, G.L. (2020). Good News and Bad News About Incentives to Violate the Health Insurance Portability and Accountability Act (HIPAA): Scenario-Based

Questionnaire Study (vol 8, e15880, 2020). *Jmir Medical Informatics*, *8*(9). doi:ARTNe2424310.2196/24243
Greszki, R., Meyer, M., & Schoen, H. (2015). Exploring the Effects of Removing "Too Fast" Responses and Respondents from Web Surveys. *Public Opinion Quarterly*, *79*(2), 471-503. doi:10.1093/poq/nfu058
Henseler, J. (2018). Partial least squares path modeling: Quo vadis? *Quality & Quantity*, *52*(1), 1-8. doi:10.1007/s11135-018-0689-6
Henseler, J., & Chin, W.W. (2010). A Comparison of Approaches for the Analysis of Interaction Effects Between Latent Variables Using Partial Least Squares Path Modeling. *Structural Equation Modeling-a Multidisciplinary Journal*, *17*(1), 82-109. doi:Pii 91853652110.1080/10705510903439003
Herzog, K. (2015). *A Psychiatrist Analyzes Mr. Robot's Elliot Alderson.* Retrieved from https://www.vulture.com/2015/08/mr-robot-elliot-alderson-psych-evaluation.html
HIPAA, J. (2018). Largest Healthcare Data Breaches of 2018. Retrieved from https://www.hipaajournal.com/largest-healthcare-data-breaches-of-2018/
Hoffman, C. (2017). *Hacker Hat Colors Explained: Black Hats, White Hats, and Gray Hats*. Retrieved from https://www.howtogeek.com/157460/hacker-hat-colors-explained-black-hats-white-hats-and-gray-hats/
Holt, T.J. (2010). Examining the Role of Technology in the Formation of Deviant Subcultures. *Social Science Computer Review*, *28*(4), 466-481. doi:10.1177/0894439309351344
Jolls, C., Sunstein, C.R., & Thaler, R. (1998). A behavioral approach to law and economics. *Stanford Law Review*, *50*(5), 1471-1550. doi:Doi 10.2307/1229304
Jonason, P.K., & Luevano, V.X. (2013). Walking the thin line between efficiency and accuracy: Validity and structural properties of the Dirty Dozen. *Personality and Individual Differences*, *55*(1), 76-81. doi:10.1016/j.paid.2013.02.010
Jonason, P.K., & Webster, G.D. (2010). The Dirty Dozen: A Concise Measure of the Dark Triad. *Psychological Assessment*, *22*(2), 420-432. doi:10.1037/a0019265
Jones, D.N., & Paulhus, D.L. (2014). Introducing the Short Dark Triad (SD3): A Brief Measure of Dark Personality Traits. *Assessment*, *21*(1), 28-41. doi:10.1177/1073191113514105
Jones, D.N., & Paulhus, D.L. (2017). Duplicity Among the Dark Triad: Three Faces of Deceit. *Journal of Personality and Social Psychology*, *113*(2), 329-342. doi:10.1037/pspp0000139
Kahneman, D., & Tversky, A. (1979). Prospect Theory - Analysis of Decision under Risk. *Econometrica*, *47*(2), 263-291. doi: 10.2307/1914185
Kajtazi, M., Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2014). Assessing Sunk Cost Effect on Employees' Intentions to Violate Information Security Policies in Organizations. *2014 47th Hawaii International Conference on System Sciences (Hicss)*, pp. 3169-3177. doi:10.1109/Hicss.2014.393
Kirsch, C. (2104). The Grey Hat Hacker: Reconciling Cyberspace Reality and the Law. *Northern Kentucky Law Review*, *41*(3), 383-404.
Krit, S.D., & Haimoud, E. (2016). Review On The IT Security Attack And Defense. *2016 International Conference on Engineering & Mis (Icemis)*. Retrieved from <Go to ISI>://WOS:000391535300095
Lee, J.H. (2017). Black Hat: Knowledge Resource for Cybersecurity. *Ieee Consumer Electronics Magazine*, *6*(1), 16-19. doi:10.1109/Mce.2016.2614644
Levitt, S.D. (2017). The Economics of Crime. *Journal of Political Economy*, *125*(6), 1920-1925. Retrieved from <Go to ISI>://WOS:000417579700028
Lopes, B., & Yu, H. (2017). Who do you troll and Why: An investigation into the relationship between the Dark Triad Personalities and online trolling behaviours towards popular and less popular Facebook profiles. *Computers in Human Behavior*, *77*, 69-76. doi:10.1016/j.chb.2017.08.036

Loughran, T.A., Paternoster, R., Chalfin, A., & Wilson, T. (2016). Can Rational Choice Be Considered a General Theory of Crime? Evidence from Individual-Level Panel Data. *Criminology*, *54*(1), 86-112. doi:10.1111/1745-9125.12097

Maasberg, M., Van Slyke, C., Ellis, S., & Beebe, N. (2020). The dark triad and insider threats in cyber security. *Communications of the ACM*, *63*(12), 64-80.

Maasberg, M., Warren, J., & Beebe, N.L. (2015). The Dark Side of the Insider: Detecting the Insider Threat Through Examination of Dark Triad Personality Traits. *2015 48th Hawaii International Conference on System Sciences (Hicss)*, pp. 3518-3526. doi:10.1109/Hicss.2015.423

Madarie, R. (2017). Hackers' Motivations: Testing Schwartz's Theory of Motivational Types of Values in a Sample of Hackers. *International Journal of Cyber Criminology*, *11*(1), 78-97. doi:10.5281/zenodo.495773

Mahmood, M.A., Siponen, M., Straub, D., Rao, H.R., & Raghu, T.S. (2010). Moving toward Black Hat Research in Information Systems Security: An Editorial Introduction to the Special Issue. *Mis Quarterly*, *34*(3), 431-433. Retrieved from <Go to ISI>://WOS:000281129800001

Myers, S.L. (1983). Estimating the Economic-Model of Crime - Employment Versus Punishment Effects. *Quarterly Journal of Economics*, *98*(1), 157-166. doi:Doi 10.2307/1885572

Nevin, A.D. (2015). *Cyber-Psychopathy: Examining the Relationship between Dark E-Personality and Online Misconduct.* The University of Western Ontario.

Ozsoy, E., Rauthmann, J.F., Jonason, P.K., & Ardic, K. (2017). 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). *Personality and Individual Differences*, *117*, 11-14. doi:10.1016/j.paid.2017.05.019

Pabian, S., De Backer, C.J.S., & Vandebosch, H. (2015). Dark Triad personality traits and adolescent cyber-aggression. *Personality and Individual Differences*, *75*, 41-46. doi:10.1016/j.paid.2014.11.015

Palmer, C.C. (2001). Ethical hacking. *Ibm Systems Journal*, *40*(3), 769-780. doi:DOI 10.1147/sj.403.0769

Paulhus, D.L., & Williams, K.M. (2002). The Dark Triad of personality: Narcissism, Machiavellianism, and psychopathy. *Journal of Research in Personality*, *36*(6), 556-563. doi:Pii S0092-6566(02)00505-6 Doi 10.1016/S0092-6566(02)00505-6

Raymond, E.S. (2004). *The Jargon File, version 4.4.8.* Retrieved from http://www.catb.org/jargon/

Reinsel, D., Gantz, J., Rydning, J. (2018). The Digitization of the World From Edge to Core. *IDC*, *27*. Retrieved from https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf

Reio, T.G., Petrosko, J.M., Wiswell, A.K., & Thongsukmag, J. (2006). The measurement and conceptualization of curiosity. *Journal of Genetic Psychology*, *167*(2), 117-135. Doi 10.3200/Gntp.167.2.117-135

Robert Willison, P.B.L., & Paternoster, R. (2018). 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*.

Rogers, M.K. (2006). A two-dimensional circumplex approach to the development of a hacker taxonomy. *Digital Investigation*, *3*(2), 97-102. doi:10.1016/j.diin.2006.03.001

Rogers, M.K., Seigfried, K., & Tidke, K. (2006). Self-reported computer criminal behavior: A psychological analysis. *Digital Investigation*, pp. S116-S120. doi:10.1016/j.diin.2006.06.002

Roy Sarkar, K. (2010). Assessing insider threats to information security using technical, behavioural and organisational measures. *Information Security Technical Report*, *15*(3), 112-133. https://doi.org/10.1016/j.istr.2010.11.002

Safa, N.S., Maple, C., Watson, T., & Von Solms, R. (2018). Motivation and opportunity based model to reduce information security insider threats in organisations. *Journal of Information Security and Applications*, *40*, 247-257. doi:10.1016/j.jisa.2017.11.001

Sauter, M. (2014). *The coming swarm: DDoS actions, hacktivism, and civil disobedience on the Internet*. New York; London: Bloomsbury Academic.

Savard, C., Simard, C., & Jonason, P.K. (2017). Psychometric properties of the French-Canadian version of the Dark Triad Dirty Dozen. *Personality and Individual Differences*, *119*, 122-128. doi:10.1016/j.paid.2017.06.044
Seebruck, R. (2015). A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model. *Digital Investigation*, *14*, 36-45. doi:10.1016/j.diin.2015.07.002
Seigfried-Spellar, K.C., Villacis-Vukadinovic, N., & Lynam, D.R. (2017). Computer criminal behavior is related to psychopathy and other antisocial behavior. *Journal of Criminal Justice*, *51*, 67-73. doi:10.1016/j.jcrimjus.2017.06.003
Shachaf, P., & Hara, N. (2010). Beyond vandalism: Wikipedia trolls. *Journal of Information Science*, *36*(3), 357-370. doi:10.1177/0165551510365390
Smith, A.N. (2019). Pursuing "Generation Snowflake": Mr. Robot and the USA Network's Mission for Millennials. *Television & New Media*, *20*(5), 443-459. doi:10.1177/1527476418789896
Soh, C., Yu, S.C., Narayanan, A., Duraisamy, S., & Chen, L.H. (2019). Employee profiling via aspect-based sentiment and network for insider threats detection. *Expert Systems With Applications*, *135*, 351-361. doi:10.1016/j.eswa.2019.05.043
Theis, M., Trzeciak, R., Costa, D., Moore, A., Miller, S., Cassidy, T., & Claycomb, W. (2019). *Common Sense Guide to Mitigating Insider Threats*, Sixth Edition. Pittsburgh, Pennsylvania.
Thaler, R.H. (2008). Mental accounting and consumer choice: Anatomy of a failure. *Marketing Science*, *27*(1), 12-14. doi:10.1287/mksc.1070.0348
Thaler, R.H. (2017). Misbehaving: The Making of Behavioral Economics. *International Journal of Applied Behavioral Economics*, *6*(1), 77-81. Retrieved from <Go toI SI>://WOS:000396638000005
Tversky, A., & Kahneman, D. (1992). Advances in Prospect-Theory - Cumulative Representation of Uncertainty. *Journal of Risk and Uncertainty*, *5*(4), 297-323. doi:Doi 10.1007/Bf00122574
Volmar, D. (2017). Far from the Lonely Crowd The Trenchant Techno-Cynicism of Mr. Robot. *Endeavour*, *41*(4), 208-210. doi:10.1016/j.endeavour.2017.05.002
Volmer, J., Koch, I.K., & Goritz, A.S. (2016). The bright and dark sides of leaders' dark triad traits: Effects on subordinates' career success and well-being. *Personality and Individual Differences*, *101*, 413-418. doi:10.1016/j.paid.2016.06.046
Waldrop, M.M. (2016). How to hack the hackers: The human side of cybercrime. *Nature*, *533*(7602), 164-167. doi:10.1038/533164a
Warkentin, M., Vance, A., & Johnston, A.C. (2016). Introduction to the HICSS-49 Minitrack on Innovative Behavioral IS Security and Privacy Research. *Proceedings of the 49th Annual Hawaii International Conference on System Sciences (Hicss 2016)*, pp. 3635-3635. doi:10.1109/Hicss.2016.454
Weber, R. (2012). Theory Building in the Information Systems Discipline: Some critical reflections. *Information Systems Foundations: Theory Building in Information Systems*, pp. 1-20. Retrieved from <Go to ISI>://WOS:000331997700001
Werts, C.E., Linn, R.L., & Joreskog, K.G. (1974). Intraclass Reliability Estimates - Testing Structural Assumptions. *Educational and Psychological Measurement*, *34*(1), 25-33. doi:Doi 10.1177/001316447403400104
Weston, S. (2020). *Insider data breaches set to increase due to remote work shift*. Retrieved from https://www.itpro.co.uk/security/data-breaches/357545/insider-data-breaches-third-2021
WRIT 2018. (2018). Retrieved from https://www.ieee-security.org/TC/SPW2018/WRIT/
Yoo, C.W., Sanders, G.L., & Cerveny, R.P. (2018). Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance. *Decision Support Systems*, *108*, 107-118. doi:10.1016/j.dss.2018.02.009

APPENDIX

Research Variables

Dependent Variables Seven-item scales ranging from *strongly disagree* to *strongly agree*		
Type of Question	**White Hat Items** **For the following questions, assume that you would be working for a government agency and that you would not be prosecuted for participating in these activities. Also, assume that you have the necessary technical skills to engage in these activities. Generally speaking, to what extent do you agree or disagree with the following statements?**	**Loadings**
Social engineering	I would like to pretend I am an authority figure to obtain a password.	.871
Social engineering	I would like to observe a person's behavioral patterns over a week and use that as a way to obtain their personal information.	.846
Social engineering	I would like to use manipulative emails to obtain private information or install malware on computers.	.898
Social engineering	I would like to sneak into buildings using a lock pick, by following someone else, or by using an electronic device to counter the lock system.	.886
Technical	I would like to use password crackers to break into computer accounts.	.910
Technical	I would like to set up a website that looks like a real website to trick people into entering their personal information.	.877
Technical	I would like to be able to capture information that people use in wireless networks.	.900

	Black Hat Items **For the following questions, assume that you would not get caught for participating in the following activities and that you have the necessary technical skills to engage in these activities. Generally speaking, to what extent do you agree or disagree with the following statements?**	
Financial	I could see myself engaging in hacking attacks if I needed money to help a family member pay $200,000 for medical treatment for a life-threatening medical procedure not covered by insurance.	.789
Financial	I could see myself engaging in hacking attacks if I needed money to purchase a $400,000 house for my family.	.931
Financial	I could see myself engaging in hacking attacks if I needed money to purchase a new $60,000 car that I could not afford.	.877
Financial	I could see myself engaging in hacking attacks if I needed money to pay off a credit card debt that had reached $100,000 and I was just fired from my job.	.924

	Grey Hat Items **For the following questions, assume that you would not get caught for participating in the following activities and that you have the necessary technical skills to engage in these activities. Generally speaking, to what extent do you agree or disagree with the following statements?**	
Hacktivist	I could see myself engaging in hacking attacks against a company that was supporting a political candidate that I did not like.	.918
Hacktivist	I could see myself engaging in hacking attacks against a Twitter account of a person that had extreme views that I did not believe in.	.920
Hacktivist	I could see myself engaging in hacking attacks against a government agency that was engaging in an activity that I felt was wrong.	.888

Independent Variables **Seven-item scale ranging from *strongly disagree* to *strongly agree* except for probability of apprehension**		
Construct	**Items**	**Loadings**
Machiavellian	I have used deceit or lied to get my way.	.820
Machiavellian	I tend to manipulate others to get my way.	.900
Machiavellian	I have used flattery to get my way.	.818
Machiavellian	I tend to exploit others towards my own end.	.876
Narcissism	I tend to want others to admire me.	.732
Narcissism	I tend to want others to pay attention to me.	.791
Narcissism	I tend to expect special favors from others.	.855
Narcissism	I tend to seek prestige or status.	.821
Psychopathy	I tend to lack remorse.	.849
Psychopathy	I tend to be callous or insensitive.	.866
Psychopathy	I tend to be unconcerned with the morality of my actions.	.818
Psychopathy	I tend to be cynical.	.748
Thrill seeking	I will try almost anything to get my "thrills."	.734
Thrill seeking	I am a bit of a daredevil.	.829
Thrill seeking	I would risk injury to do something exciting.	.906
Thrill seeking	I like doing things that are risky or dangerous.	.920
Opposition to authority	I get a kick out of challenging so-called authority figures.	.823
Opposition to authority	I am known as a bit of a rebel.	.885
Opposition to authority	Rules are made to be broken.	.866
Opposition to authority	I am not very good at following orders.	.807
Probability of apprehension	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 do you think is the likelihood of getting caught, if you accept the money?**	.853
Probability of apprehension	Suppose you work for an insurance company and make $60,000 per year. A relative asks you to get insurance data on a famous local celebrity from the organization you work for. **What do you think is the likelihood of getting caught, if you accept the money?**	.880

Probability of apprehension	Your mother has just been diagnosed with a rare condition that causes kidney failure and is fatal if untreated. This condition can be treated, but the treatment is still considered experimental and is therefore not covered by health insurance, nor is it eligible for any type of financial assistance. The treatment is available both nationally and internationally and costs $100,000. A media outlet approaches you to get information about a famous politician and offers to pay you $100,000 for that information. This money can save your mother's life. **What do you think is the likelihood of getting caught, if you accept the money?**	.849
Probability of apprehension	Your best friend has been in an all-terrain vehicle (ATV) accident in a rural area of Kansas. He/she has life-threatening injuries and needs air medical transportation to receive lifesaving medical care. The medical air evacuation is not covered by insurance and costs $100,000. Your best friend will not survive ground transportation or local medical care. A media outlet offers you $100,000 to obtain the health care records of a famous reality television star. This money can save your best friend's life. **What do you think is the likelihood of getting caught, if you accept the money?**	.865