The Interaction of Dark Traits with the Perceptions of Apprehension

Joana Gaia
Department of Management Science and Systems
University at Buffalo
joanaalu@buffalo.edu

David Murray
Department of Management Science and Systems
University at Buffalo
djmurray@buffalo.edu

G. Lawrence Sanders
Department of Management Science and Systems
University at Buffalo
mgtsand@buffalo.edu

Sean Patrick Sanders
Department of Computer Science and Engineering
University at Buffalo
spsander@buffalo.edu

Shambhu Upadhyaya
Department of Computer Science and Engineering
University at Buffalo
shambhu@buffalo.edu

Xunyi Wang
Department of Information Systems & Business Analytics
Baylor University
Xunyi_Wang@baylor.edu

Chul Woo Yoo
Information Technology and Operations Management
Florida Atlantic University
yooc@fau.edu

Abstract

This paper integrates dark personality traits with the economics of crime and rational choice theories to identify the role that the Dark Triad and thrill-seeking have on the perceptions of being caught engaging in violating privacy laws.

Psychopathy and thrill-seeking had a moderate negative effect on the perceptions of the probability of being apprehended for distributing illegally obtained healthcare information. The implication is that individuals scoring high on the psychopathy and thrill-seeking scales will need less money or monetary incentives to violate HIPAA laws. We also found additional support that white hat hackers score high on the Machiavellian, psychopathy and thrill-seeking scales. We also validated a previous finding that a white hat hacker might drift towards grey hat and black hat hacking.

1. Introduction

It has been estimated that 70% of organizational security breaches are not reported [1]. Companies have several reasons for not reporting violations, including protecting the privacy of employees and customers, potential litigation, and the possibility that such revelations would harm the organization's reputation [2]. In fact, 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" [3]. Those reports and current situations strongly call for research on employees and violation intention. Against this backdrop of importance of the topic, this study investigates the role of dark personality traits and their influence on monetary incentives and how they relate to the economics of crime and the violation of healthcare regulations.

The COVID-19 pandemic has placed a lot of stress on individual employees and organizations. 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 and the ensuing push to remote work, employee feelings of job insecurity, and the ease of moving stolen company data because of cloud and the ease of transferring large amounts of data (Weston, 2020).

The psychological profiling of hackers has attracted substantial theoretical interest traits [4], but the empirical results on insider threats and behavioral traits are limited [5-10]. This research will examine the influence of the Dark Triad and thrill-seeking traits in lowering the perceptions of being apprehended when violating healthcare regulations.

URI: https://hdl.handle.net/10125/79612
978-0-9981331-5-7

2. Psychological Research on Hackers

As noted earlier, the psychological profiling of hackers has attracted substantial research interest recently, but the empirical results are limited [5-10]. One reason for the lack of information is that organizations are not eager to report insider attacks: an estimated 70% are not reported [1]. The paucity of reporting relates to privacy issues, and litigation, and that such revelations would harm the organization's reputation [2]. Another reason is that many breaches are undetected—but that does not mean organizations have not been compromised.

Previous literature has demonstrated several pertinent personal characteristics found in the areas of cybersecurity, hacking, etc. One study of 72 cybersecurity professionals found that cybersecurity specialists have significantly higher openness, assertiveness, extraversion, and adventurousness scores [11]. It was also found that motivations for participating in hacking behavior include revenge, ideology, fun, thrills, survival, notoriety, recreation, and profit [5, 12]. It is also argued that the Dark Triad personality traits, which this study is interested in, consist of *Machiavellianism* (manipulative, deceitful, and exploitive), *narcissism* (self-centered and attention-seeking), and *psychopathy* (lack of remorse, cynical, and insensitive) [13-15]. A survey of 768 Amazon Mechanical Turk (AMT) IT professionals found that Machiavellianism, narcissism, and psychopathy had statistically significant beta weights related to sympathy for an individual who posted salary information of higher-paid coworkers [16]. An earlier study of 235 AMT respondents found a correlation between narcissism and total computer crime of 0.26 ($r^2 = 0.07$) [17]. A recent study using 474 students found that white hat, grey hat, and black hat hackers score high on the Machiavellian and psychopathy scales [18]. They also found that white hatters tend to be narcissists and that thrill-seeking was moderately significant for white hat and black hat hacking.

3. Research on the Economics of Crime

Becker's seminal paper on the market for criminal activity suggests that potential criminals examine returns related to illegal activity as a function of the probability of getting caught and the severity of the punishment [19]. The market model for crime assumes that offenders, victims, and law enforcement engage in optimizing behavior related to their preferences, offenders' expectations about returns, the propensity for being caught, and the resulting punishment [20]. Potential offenders use a calculus of rational choice in determining whether to engage in criminal activity [19, 21]. A likely perpetrator will commit a crime if the inequality presented in Figure 1 holds [22, 23]. Game theory has been proposed as a mechanism to increase the negative returns and to decrease the positive returns to the perpetrator considering an illegal cybersecurity attack [24, 25].

There are ongoing discussions and controversies about utility theory and rational decision-making among traditional and behavioral economists. Behavioral economists do not abandon the notion that humans can be rational, but they think that there are situations where decision-making is less than rational and that more robust models are needed to understand human behavior (c.f. [26-30]). The purpose of this research stream is to determine the effectiveness of the rational model in predicting interest in violations of privacy laws.

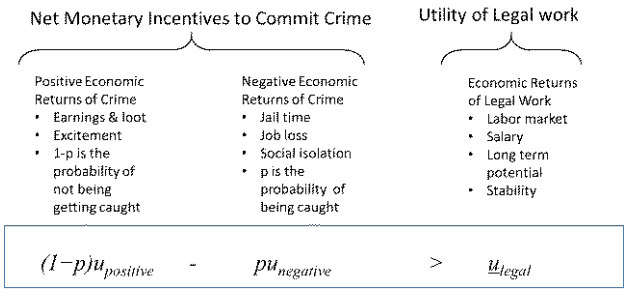

Figure 1. Becker crime Utility model

4. Research Questions and Hypotheses

Figure 2 presents an overview of the major questions examined in this paper. Engaging in illegal activity, such as selling health care information, involves choosing consequences and opportunities of those actions. However, individuals perceive these choices differently and can be deterred if there is a likelihood of punishment and that the penalty is severe [20]. The market model assumes that offenders are rational economic actors with expectations about the expected returns, the propensity for being caught, and the resulting punishment [20, 23]. The first research question will examine if our study and survey sample support the economics of crime literature regarding the need for higher monetary incentives when an individual perceives a high probability of being caught. Individuals perceiving a high likelihood of being apprehended (e.g., 75%) will require higher monetary incentives than individuals perceiving a lower probability of apprehension (e.g., 25%). Therefore, we propose the following hypothesis:

H1: Higher perceptions of being apprehended violating HIPAA regulations are positively related to higher requirements for monetary incentives.

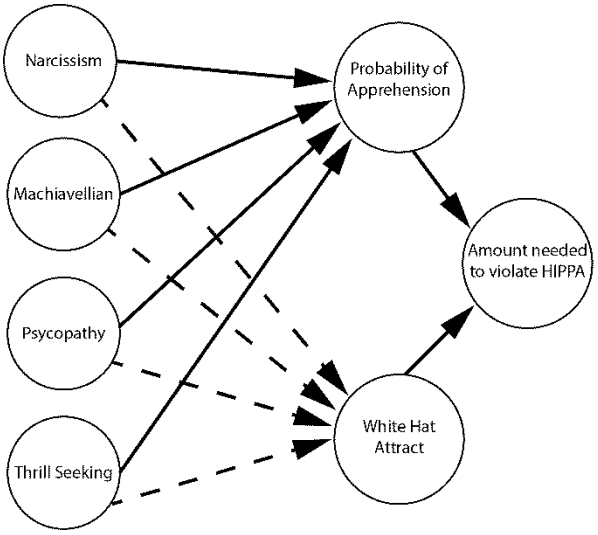

Figure 2. Research Model

Our second research question examines the role of psychological traits in the perceived probability of being apprehended in violating HIPAA laws. In essence, we are interested in whether an increase in certain traits is related to reducing the probability of apprehension when considering violating privacy laws. The dark triad traits are often viewed as being undesirable. However, research suggests that these traits have a dark side and a positive side [31]. 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 hacking and violation of healthcare laws and the level of psychopathy.

Thrill-seeking behavior is consistently touted as a motivation for hacking [32, 33]. Thrill-seekers derive pleasure from the excitement of hacking [34]. Many believe that the days of the hacker as a thrill-seeker have morphed into the larger role of state-sponsored hackers [35]. We included a thrill-seeking scale because this trait describes many individuals are attracted to hacking [17]. And many hackers are motivated by a combination of fun, thrill-seeking, excitement, and curiosity [36]. Based on this argument, we propose the following hypothesis:

H2: Higher levels of the Dark Triad and thrill-seeking are related to lower perceptions of being apprehended violating healthcare regulations.

Our third research question considers the role that interest in white hat hacking plays. We wanted to use this to validate the research model since earlier work found a statistically significant relationship between the Dark triad and thrill-seeking and interest in white hat hacking [18]. We also draw on several prior studies investigating the relationship between computer abuse and crime as influenced by narcissism, Machiavellianism, and psychopathy as additional justification [16, 17, 37] Based on the argument above, we propose the following hypothesis:

H3: The dark triad, Machiavellianism, narcissism, and psychopathy and thrill-seeking are positively related with interest in white hat hacking.

5. Research Methodology

Appendix 1 provides an overview of the scales used in the study. We chose the Dark Triad Dirty Dozen for this study because this set of measurements provides four concise items and was extensively validated by previous studies. In addition, it has reasonable psychometric properties and has been adapted for several cultures [38-41]. Next, we used a set of items to examine computer crime and abuse to measure the thrill-seeking trait [17]. The *probability of being apprehended* construct was initially developed as a part of another comprehensive study involving 523 subjects and was focused on the economics of crime [23]. 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 adapted the following COVID-19 scenario 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 computer abuse component of the scenario is the securing of private information on a famous patient. The amount of money that the subject would accept to commit the crime is the net monetary incentive to commit the crime. The likelihood of getting caught is the perceived probability of sanctions. We used a Covid-19 scenario as the backdrop of the study because we felt it would be timely and relatable to the students, thus

increasing active participation in the survey. See Appendix 1 for the online presentation of the question that was presented to the participants.

> *Suppose you are a computer technical support specialist at a hospital, and you earn $50,000 per year. You have just received a notice that you will be laid off next month because of the COVID-19 pandemic. You have a mortgage to pay and tuition due at a private school. A friend asks you to get them some information on a very famous patient at the hospital. ... 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?*

An important consideration in designing the survey was obtaining information from the subjects on the probability of getting caught if they violated a privacy regulation. The questionnaire items were anchored using numerical probabilities and verbal labels because this approach has been found to be a very effective method for eliciting probabilities [42], and it counters some of the measurement problems encountered in measuring perceived arrest rates involved in studies of rational choice theory [43].

The white hat scale was adapted from an existing validated scale [18]. The scale was developed by surveying the academic and professional literature and discussing security and privacy research with experts. The scale attempts to measure the attraction to both technical and social engineering hacking behaviors. The social engineering items measure interest in exploiting people and systems through the social manipulation of people, involving interactions that use disguises, ploys, and psychological tricks to achieve intrusion [44, 45]. This contrasts with the technical items in the scale that require sophisticated knowledge to attack a system. The questions form the white hat construct because we told the subject they would work for a government agency and that they would not be prosecuted for participating in these activities.

6. Data Collection and Analysis

We recruited 303 subjects from junior and senior undergraduates enrolled in a management information systems class at a state research institution in the northeastern United States to take an online Qualtrics survey. The study was approved by the Institutional Review Board (IRB). The total number of possible surveys from the course was 488. The number of individuals agreeing to participate in the survey was 325. 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 [46].

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. Studying management students provides a solid foundation for researching and investigating other populations since they will be entering the workforce in the immediate future. From our experience, they are less concerned with social desirability issues.

Conducting research involving undesirable behavior is challenging from an organizational and subject's perspective. Organizations do not want to risk reputation damage even if the study is performed anonymously and the results are reported anonymously. In addition, the personality data gathered from employees is usually biased and unreliable because of social desirability issues. The *social desirability bias* enters into the picture when studies involve abilities, personality, and illegal activities. Subjects are less prone to answer questions truthfully because they do not want to diminish their social prestige [47, 48]. In contrast to individuals from organizations and individuals with high-status jobs, we have found that students are less prone to over-report "good behavior" and under-report "bad behavior." As our results will show, rather than not engaging in illegal acts, approximately 66% of the subjects indicated they would receive money in times of monetary stress, such as the COVID-19 pandemic.

We used SmartPLS 3.0 to perform partial least squares (PLS) analysis because PLS is robust, resistant to statistical inadequacies, and effective in handling complex multidimensional constructs [49]. SmartPLS 3.0 was also used because our research model includes reflective sub-latent variables, and we were also interested in prediction [50]. We report only the significant paths to make the exposition and explanation clearer. The p values were generated using 1,000 bootstrapped samples.

6.1. Measurement Assessment

We examined individual loadings and internal consistency to test for item reliability. Loadings for all measurement items were above 0.7. Table 1 illustrates that Cronbach's alpha for every construct was greater than 0.7, indicating internal reliability [51]. 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 1. Latent Variable Statistics

Variables			
	Cronbach's Alpha	Composite Reliability	Average Variance Extracted
Machiavellian	0.818	0.875	0.638
Narcissistic	0.805	0.863	0.661
Psychopathy	0.821	0.882	0.653
Thrill seeking	0.899	0.882	0.768
White hat	0.943	0.954	0.747

6.2. Research Model Assessment

The essence of the first research question is to test the relationship that higher perceptions of being apprehended for violating HIPAA regulations are related to higher requirements for monetary incentives. A statistically significant correlation between the probability of being apprehended and the amount of money necessary for the individual to violate a healthcare privacy law is all that is required to support the research question. The correlation between the probability of getting caught and the amount of money that the subjects would accept to provide the information was 0.32 for the COVID-19 scenario. The correlation results are modest, but they are in the right direction. Therefore, H1 is supported. Table 2 presents the cross-tabs for the findings, and Figure 3 illustrates a pictorial overview. They both provide additional visual support for this hypothesis.

It should be noted from Table 2 that there is a price for violating privacy laws. Approximately 46% of the subject's participating in the study would take money ranging from under $10,000 to over a $1,000,000 dollars to turn over the data.

Table 2. The Amount of Money Willing to Receive and the Perceived Probability of Getting Caught

Covid Scenario		Perceived probability of getting caught				
		0% & 7%	25% - 75%	93% & 100%	Total	Percent
Amount of money willing to receive	<$10,000	3	21	1	25	8%
	$10,000 - $99,999	10	33	10	53	10%
	$100,000 - $999,999	8	40	13	61	12%
	Over $1,000,000	14	29	19	62	16%
	No amount of mone	10	33	59	102	54%
	Total	45	156	102	303	100%
	Percentage	14%	55%	30%	100%	

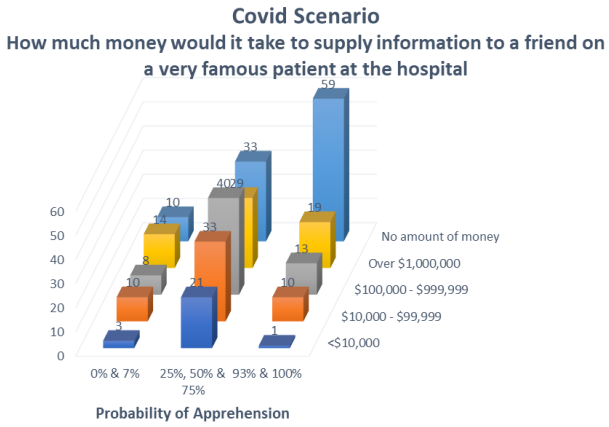

Figure 3. The Amount of Money Willing to Receive and the Perceived Probability of Getting Caught

Hypotheses H2 and H3 were examined using the SmartPLS package. Partial least squares (PLS) analysis is robust, resistant to statistical inadequacies, and effective in handling complex multidimensional constructs [49]. We were also interested in prediction, and PLS is suitable where latent variables involve prediction [50]. We report only the significant paths to make the exposition and explanation clearer. The *p* values were generated using 1000 bootstrapped samples.

The r^2 for the probability of being apprehended was 0.095 (see Figure 4). Thus, psychopathy and thrill-seeking had a modest and negative influence on the perceptions of the probability of being apprehended. As a result, H2 is supported. The implication is that individuals who are high on the psychopathy and thrill-seeking scales will perceive the likelihood of being caught as lower.

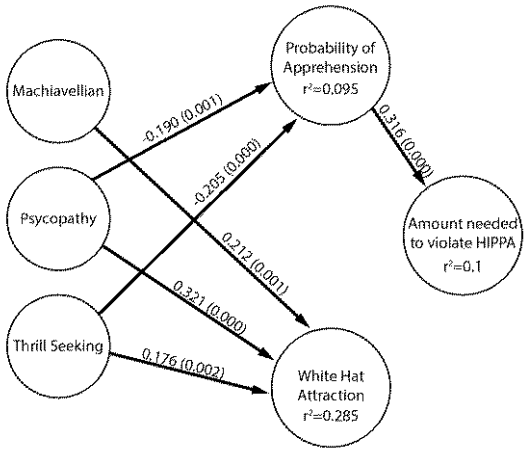

Figure 4. Results for Dark Triad Influence on Apprehension and Monetary Requirements

The r^2 for the white hat model was 0.285. Machiavellianism, psychopathy, and thrill-seeking were predictors of individuals attracted to white hat hacking. As a result, H3 is moderately supported. Psychopathy and Machiavellianism were moderate predictors of individuals attracted to white hat hacking.

6.3. Does an interest in white hat hacking influence the perception of the probability of apprehension?

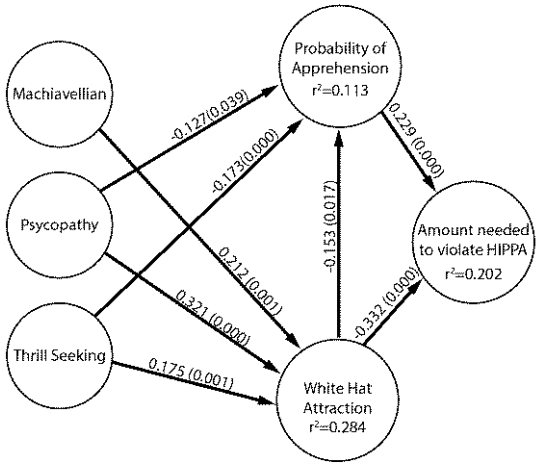

Figure 5. Results for Relationship of White Hat Influencing Apprehension and Monetary Incentives

One interesting question is whether white hat hacking can contribute to illegal hacking. A famous example of this drift to the dark side can be found in *American Kingpin* [52], a story of Ross Ulbricht, the developer of the darknet website called Silk Road. One of the government agents investigating Ross Ulbricht became enamored with the excitement and monetary attraction and eventually was lured into committing criminal activities. As illustrated in Figure 5, the perceptions of the probability of being apprehended and the amount of money needed to violate HIPAA are diminished, increasing the desirability of becoming a white hat hacker.

We also validated a previous finding related to whether white hat hackers might drift towards being black hat and grey hat hackers [53]. As illustrated in Figure 6, the paths from white hat hacking to black and grey hat hacking were strong. The r^2 for the grey hat construct was 0.474, and the r^2 for the black hat construct was 0.496. The implication is that, given the right situation, a white hat hacker might drift toward the dark side. The items used to measure the black hat and grey hat constructs can be viewed in the appendix.

The coefficients for the probability of apprehension were negative and significant for both black hat and grey hat hacking, thus supporting the deterrence effect of the perceived probability of being caught.

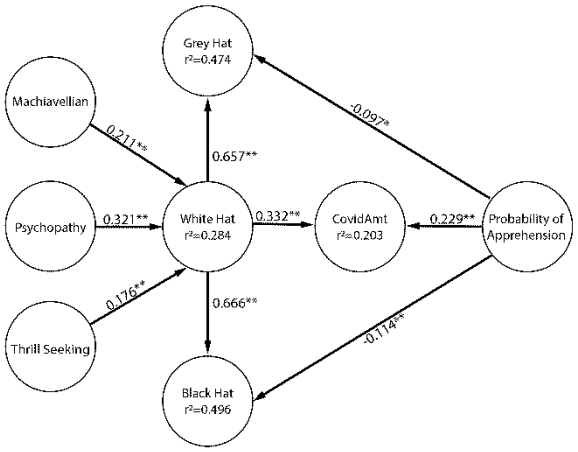

Figure 6. Drift Model for Grey Hat and Black Hat

7. Conclusion

We have found modest support that the potential abusers of computer systems use a rational choice calculus that wrongdoers use in the context of whether to engage in the violation of privacy laws [19, 21, 54]. We found that thrill-seeking, Machiavellianism, and psychopathy personality traits are modestly related to this calculus.

Using the dark triad personality traits to evaluate new employees as security threats may be possible [4], but this strategy should be approached cautiously for practical, ethical, and privacy reasons. For example, we found that white hat hackers have Machiavellian, psychopathy, and thrill-seeking traits. That does not mean they will migrate to become black hats, but they may be needed to counter black hat and grey hat attacks.

The Software Engineering Institute (SEI) institute at Carnegie Mellon University has identified strategies for countering insider threats [55]. These strategies include the development of monitoring systems, hiring practices, privileged access guidelines, and addressing behavioral issues. They note that positive incentives are effective in achieving higher levels of security and reducing insider misbehavior. However, as noted by CISA, detecting and dealing with insider threats is a complex behavioral issue.

One limitation of the study is that the sample was drawn from a student population. Further validation of

the research discussed here is in order. It would also be desirable to obtain a sample from various organizations and industries, even though employees will be guarded when they are asked if they would participate in illegal activities. Trust and social desirability issues loom large with individuals already in the workforce. However, real-world validation is the next step in examining the viability of the research stream.

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 [9]. These theories have the potential to assist an organization in developing behavioral approaches to curb insider threats.

This paper and previous research have shown that higher perceptions of being apprehended can deter committing cyber-crime. However, there is a significant problem when deterrence relies on the perceptions of being apprehended and charged. The probability of being charged and convicted is exceedingly tiny [23]. For example, between April 2003 and July 2018, 186,453 health information privacy complaints were submitted to the US Department of Health and Human Services. The sanctions were very few, and 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 receive a warning [56].

Our findings suggest that psychopathy, Machiavellianism, and thrill-seeking thrill influence potential hackers' rational decision-making process. In that context, countering deception using sophisticated technologies and advanced tactics plays a crucial role in influencing the attacker's behaviors. The application of game theory and artificial intelligence algorithms has the potential to reduce the risks and increase the costs of attacker [24], which is the goal of the deterrence theory and the economics of crime model. The key to future prevention of privacy breaches will be a concerted effort of enforcement, monitoring, and education to quell what will undoubtedly be the continuing assault on privacy.

8. Acknowledgement

This material is based upon work supported by the NSF under Grant No. DGE-1754085.

9. References

[1] "WRIT 2018," Overview Topics Steeringt Commitee, 2018. [Online]. Available: https://www.ieee-security.org/TC/SPW2018/WRIT/.

[2] C. Soh, S. C. Yu, A. Narayanan, S. Duraisamy, and L. H. Chen, "Employee profiling via aspect-based sentiment and network for insider threats detection," (in English), *Expert Syst Appl,* vol. 135, pp. 351-361, Nov 30 2019, doi: 10.1016/j.eswa.2019.05.043.

[3] CISA. "Insider Threat Mitigation Guide.", Cybersecurity and Infrastrucure Agency, November, 2014, pp. 1-133.

[4] 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, doi: 10.1109/Hicss.2015.423.

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

[6] G. Dhillon, S. Samonas, and U. Etudo, "Developing a Human Activity Model for Insider IS Security Breaches Using Action Design Research," (in English), *Ifip Adv Inf Comm Te,* vol. 471, pp. 49-61, 2016, doi: 10.1007/978-3-319-33630-5_4.

[7] 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), *P Ann Hicss,* pp. 3169-3177, 2014, doi: 10.1109/Hicss.2014.393.

[8] 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, doi: https://doi.org/10.1016/j.istr.2010.11.002.

[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), *J Inf Secur Appl,* vol. 40, pp. 247-257, Jun 2018, doi: 10.1016/j.jisa.2017.11.001.

[10] M. Warkentin, A. Vance, and A. C. Johnston, "Introduction to the HICSS-49 Minitrack on Innovative Behavioral IS Security and Privacy Research," (in English), *Proceedings of the 49th Annual Hawaii International Conference on System Sciences (Hicss 2016),* pp. 3635-3635, 2016, doi: 10.1109/Hicss.2016.454.

[11] S. E. Freed, "Examination of personality characteristics among cybersecurity and information technology professionals," Masters Thesis, Psychology, The University of Tennessee at Chattanooga, 2014.

[12] R. Seebruck, "A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model," (in English), *Digit Invest,* vol. 14, pp. 36-45, Sep 2015, doi: 10.1016/j.diin.2015.07.002.

[13] P. K. Jonason and G. D. Webster, "The Dirty Dozen: A Concise Measure of the Dark Triad," (in English),

Psychol Assessment, vol. 22, no. 2, pp. 420-432, Jun 2010, doi: 10.1037/a0019265.

[14] D. N. Jones and D. L. Paulhus, "Duplicity Among the Dark Triad: Three Faces of Deceit," (in English), *J Pers Soc Psychol,* vol. 113, no. 2, pp. 329-342, Aug 2017, doi: 10.1037/pspp0000139.

[15] D. L. Paulhus and K. M. Williams, "The Dark Triad of personality: Narcissism, Machiavellianism, and psychopathy," (in English), *J Res Pers,* vol. 36, no. 6, pp. 556-563, Dec 2002, doi: Pii S0092-6566(02)00505-6
Doi 10.1016/S0092-6566(02)00505-6.

[16] M. Maasberg, Van Slyke Crag, Ellis, Selwyn, Beebe, Nicole, "The dark triad and insider threats in cyber security," *Commun Acm,* vol. 63, no. 12, pp. 64-80, 2020/11/17 2020.

[17] K. C. Seigfried-Spellar, N. Villacis-Vukadinovic, and D. R. Lynam, "Computer criminal behavior is related to psychopathy and other antisocial behavior," (in English), *J Crim Just,* vol. 51, pp. 67-73, Jul-Aug 2017, doi: 10.1016/j.jcrimjus.2017.06.003.

[18] J. Gaia, Ramamurthy, B., Sanders, G.L., Sanders, S.P., Upadhyaya, S., Wang, X, Yoo, C.W., "Psychological Profiling of Hacking Potential," in *Hawaii International Conference on Systems Sciences*, Maui, Hawaii, 2020, vol. Proceedings of the 53rd Hawaii International Conference on System Sciences. [Online]. Available: https://scholarspace.manoa.hawaii.edu/handle/10125/64014. [Online].

[19] G. S. Becker, "Crime and Punishment - Economic Approach," (in English), *J Polit Econ,* vol. 76, no. 2, pp. 169-217, 1968, doi: Doi 10.1086/259394.

[20] S. L. Myers, "Estimating the Economic-Model of Crime - Employment Versus Punishment Effects," (in English), *Q J Econ,* vol. 98, no. 1, pp. 157-166, 1983, doi: Doi 10.2307/1885572.

[21] 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, doi: 10.1111/1745-9125.12097.

[22] M. Draca and S. Machin, "Crime and Economic Incentives," (in English), *Annu Rev Econ,* vol. 7, pp. 389-408, 2015, doi: 10.1146/annurev-economics-080614-115808.

[23] J. Gaia, X. Y. Wang, C. W. Yoo, and G. L. Sanders, "Good News and Bad News About Incentives to Violate the Health Insurance Portability and Accountability Act (HIPAA): Scenario-Based Questionnaire Study," (in English), *Jmir Med Inf,* vol. 8, no. 7, Jul 2020.

[24] S. Fugate and K. Ferguson-Walter, "Artificial Intelligence and Game Theory Models for Defending Critical Networks with Cyber Deception," (in English), *Ai Mag,* vol. 40, no. 1, pp. 49-62, Spr 2019, doi: DOI 10.1609/aimag.v40i1.2849.

[25] M. Bilinski, K. Ferguson-Walter, S. Fugate, R. Gabrys, J. Mauger, and B. Souza, "You only Lie Twice: A Multi-round Cyber Deception Game of Questionable Veracity," (in English), *Decision and Game Theory for Security,* vol. 11836, pp. 65-84, 2019..

[26] C. Jolls, C. R. Sunstein, and R. Thaler, "A behavioral approach to law and economics," (in English), *Stanford Law Rev,* vol. 50, no. 5, pp. 1471-1550, May 1998, doi: Doi 10.2307/1229304.

[27] R. H. Thaler, "Misbehaving: The Making of Behavioral Economics," (in English), *Int J Appl Behav Eco,* vol. 6, no. 1, pp. 77-81, Jan-Mar 2017. [Online]. Available: <Go to ISI>://WOS:000396638000005.

[28] R. H. Thaler, "Mental accounting and consumer choice," (in English), *Market Sci,* vol. 27, no. 1, pp. 15-25, Jan-Feb 2008, doi: 10.1287/mksc.1070.0330.

[29] D. Kahneman and A. Tversky, "Prospect Theory - Analysis of Decision under Risk," (in English), *Econometrica,* vol. 47, no. 2, pp. 263-291, 1979, doi: Doi 10.2307/1914185.

[30] A. Tversky and D. Kahneman, "Advances in Prospect-Theory - Cumulative Representation of Uncertainty," (in English), *J Risk Uncertainty,* vol. 5, no. 4, pp. 297-323, Oct 1992, doi: Doi 10.1007/Bf00122574.

[31] 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," (in English), *Pers Indiv Differ,* vol. 101, pp. 413-418, Oct 2016, doi: 10.1016/j.paid.2016.06.046.

[32] M. K. Rogers, K. Seigfried, and K. Tidke, "Self-reported computer criminal behavior: A psychological analysis," (in English), *Digit Invest,* pp. S116-S120, Sep 2006, doi: 10.1016/j.diin.2006.06.002.

[33] M. K. Rogers, "A two-dimensional circumplex approach to the development of a hacker taxonomy," (in English), *Digit Invest,* vol. 3, no. 2, pp. 97-102, Jun 2006, doi: 10.1016/j.diin.2006.03.001.

[34] M. Bachmann, "The Risk Propensity and Rationality of Computer Hackers," (in English), *Int J Cyber Criminol,* vol. 4, no. 1-2, pp. 643-656, 2010. [Online]. Available: <Go to ISI>://WOS:000437609000005.

[35] M. M. Waldrop, "How to hack the hackers: The human side of cybercrime," *Nature,* vol. 533, no. 7602, pp. 164-7, May 12 2016, doi: 10.1038/533164a.

[36] R. Madarie, "Hackers' Motivations: Testing Schwartz's Theory of Motivational Types of Values in a Sample of Hackers," (in English), *Int J Cyber Criminol,* vol. 11, no. 1, pp. 78-97, Jan-Jun 2017, doi: 10.5281/zenodo.495773.

[37] A. D. Nevin, "Cyber-Psychopathy: Examining the Relationship between Dark E-Personality and Online Misconduct," The School of Graduate and Postdoctoral Studies, The University of Western Ontario 2015.

[38] 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), *Front Psychol,* vol. 7, Mar 30 2016..

[39] P. K. Jonason and V. X. Luevano, "Walking the thin line between efficiency and accuracy: Validity and structural properties of the Dirty Dozen," (in English), *Pers Indiv Differ,* vol. 55, no. 1, pp. 76-81, Jul 2013, doi: 10.1016/j.paid.2013.02.010.

[40] 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), *Pers Indiv Differ,* vol. 117, pp. 11-14, Oct 15 2017.

[41] C. Savard, C. Simard, and P. K. Jonason, "Psychometric properties of the French-Canadian version of the Dark Triad Dirty Dozen," (in English), *Pers Indiv Differ,* vol. 119, pp. 122-128, Dec 1 2017.
[42] M. S. McGlone and A. B. Reed, "Anchoring in the interpretation of probability expressions," (in English), *J Pragmatics,* vol. 30, no. 6, pp. 723-733, Dec 1998, doi: Doi 10.1016/S0378-2166(98)00011-3.
[43] G. Pogarsky, S. P. Roche, and J. T. Pickett, "Heuristics and Biases, Rational Choice, and Sanction Perceptions," (in English), *Criminology,* vol. 55, no. 1, pp. 85-111, Feb 2017, doi: 10.1111/1745-9125.12129.
[44] 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.
[45] S. D. Applegate, "Social Engineering: Hacking the Wetware!," (in English), *Inf Secur J,* vol. 18, no. 1, pp. 40-46, 2009, doi: 10.1080/19393550802623214.
[46] R. Greszki, M. Meyer, and H. Schoen, "Exploring the Effects of Removing "Too Fast" Responses and Respondents from Web Surveys," (in English), *Public Opin Quart,* vol. 79, no. 2, pp. 471-503, Sum 2015, doi: 10.1093/poq/nfu058.
[47] 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, doi: 10.1016/j.chb.2017.02.043.
[48] D. Dodou and J. C. F. de Winter, "Social desirability is the same in offline, online, and paper surveys: A meta-analysis," (in English), *Comput Hum Behav,* vol. 36, pp. 487-495, Jul 2014.
[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), *Struct Equ Modeling,* vol. 17, no. 1, pp. 82-109, 2010.
[50] J. Henseler, "Partial least squares path modeling: Quo vadis?," (in English), *Qual Quant,* vol. 52, no. 1, pp. 1-8, Jan 2018, doi: 10.1007/s11135-018-0689-6.
[51] C. E. Werts, R. L. Linn, and K. G. Joreskog, "Intraclass Reliability Estimates - Testing Structural Assumptions," (in English), *Educ Psychol Meas,* vol. 34, no. 1, pp. 25-33, 1974, doi: Doi 10.1177/001316447403400104.
[52] N. Bilton, *American kingpin : the epic hunt for the criminal mastermind behind the Silk Road*. New York: Portfolio/Penguin, 2017, pp. xv, 329 pages, 8 unnumbered pages of plates.
[53] J. Gaia, Sanders, G. L., Sanders, S. P., Upadhyaya, S., Wang, X., & Yoo, C. W. , "Dark Traits and Hacking Potential," *Journal of Organizational Psychology,* vol. 21(3), 2021.
[54] J. Gaia, X. Y. Wang, C. W. Yoo, and G. L. Sanders, "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)," (in English), *Jmir Med Inf,* vol. 8, no. 9, Sep 2020.
[55] 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.
[56] R. Grimes. "Why It's So Hard to Prosecute Cyber Criminals " https://www.csoonline.com/article/3147398/why-its-so-hard-to-prosecute-cyber-criminals.html (accessed.

Appendix 1. Research Variable Items

Covid Scenario for economics of crime

Suppose you are a computer technical support specialist at a hospital, and you earn $60,000 per year. You have just received a notice that you will be laid-off next month because of the COVID-19 pandemic. You have a mortgage to pay and tuition due at a private school. A friend asks you to get them some information on a very famous patient at the hospital.

What amount of money would you receive to make this acceptable?

- Less than $999
- $1,000 - $4,999
- $5,000 – $9,000
- $10,000 – $49,999
- $50,000 - $99,999
- $100,000 - $249,999
- $250,000 - $499,999
- $500,000 – $999,999
- $1 M -$10 M
- Over $10 M
- No amount of $

What do you think is the probability of getting caught, if you accept the money?

- Extremely unlikely (0%)
- Moderately unlikely (7%)
- Slightly Unlikely (25%)
- Neither likely nor unlikely (50%)
- Slightly unlikely (75%)
- Moderately likely (93%)
- Extremely likely (100%)

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**
I would like to pretend I am an authority figure to obtain a password.	.854
I would like to observe a person's behavioral patterns over a week and use that as a way to obtain their personal information.	.829
I would like to use manipulative emails to obtain private information or install malware on computers.	.871
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.	.832
I would like to use password crackers to break into computer accounts.	.919
I would like to set up a website that looks like a real website to trick people into entering their personal information.	.871
I would like to be able to capture information that people use in wireless networks.	.871

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?**	**Loadings**
I could see myself engaging in hacking attacks if I needed money to purchase a $400,000 house for my family.	.915
I could see myself engaging in hacking attacks if I needed money to purchase a new $60,000 car that I could not afford.	.867
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.	.900

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?**	**Loadings**
I could see myself engaging in hacking attacks against a company that was supporting a political candidate that I did not like.	.914
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.	.912
I could see myself engaging in hacking attacks against a government agency that was engaging in an activity that I felt was wrong.	.877
I could see myself engaging in hacking attacks against an individual that was bullying me during an online game.	.846

	Dark Triad and Thrill Seeking Items **Seven-item scales ranging from *strongly disagree* to *strongly agree***	Loadings
Machiavellian	I have used deceit or lied to get my way.	.730
Machiavellian	I tend to manipulate others to get my way.	.891
Machiavellian	I have used flattery to get my way.	.714
Machiavellian	I tend to exploit others towards my own end.	.846
Narcissism	I tend to want others to admire me.	.751
Narcissism	I tend to want others to pay attention to me.	.802
Narcissism	I tend to expect special favors from others.	.822
Narcissism	I tend to seek prestige or status.	.751
Psychopathy	I tend to lack remorse.	.852
Psychopathy	I tend to be callous or insensitive.	.857
Psychopathy	I tend to be unconcerned with the morality of my actions.	.796
Psychopathy	I tend to be cynical.	.720
Thrill seeking	I will try almost anything to get my "thrills.	.822
Thrill seeking	I am a bit of a daredevil.	.901
Thrill seeking	I would risk injury to do something exciting.	.883
Thrill seeking	I like doing things that are risky or dangerous.	.896