The Effects of Dark Triad Traits and Perceived Law Enforcement Competence in Responding to Ransomware Attacks

Truong (Jack) Luu
University of Cincinnati
luutp@mail.uc.edu

Michael Jones
University of Cincinnati
m.jones@uc.edu

Binny M. Samuel
University of Cincinnati
samuelby@uc.edu

Abstract

This research investigates a largely unexamined psychological element in ransomware attacks, a prevalent form of cybercrime, focusing on how Dark Triad personality traits (narcissism, Machiavellianism, and psychopathy) influence victim responses. Traditional responses to ransomware include paying the ransom, abandoning the data/files, and/or reporting the issue to law enforcement. We look at the interaction between these traits and responses. Using a scenario-based survey, we have collected data from 287 participants so far to unearth the relationship between these factors and individual responses to this cybercrime. Such understanding can potentially inform personalized cyber threat prevention strategies, ultimately enhancing cybersecurity research. The paper also examines the implications of its findings for both research and practice.

Keywords: dark triad, cybercrime, ransomware attack, government agency competency, cryptocurrency payment

1. Introduction

Ransomware attacks, a prevalent form of cybercrime, have become an increasingly concerning problem in recent years, with 37 percent of all businesses and organizations hit by ransomware in 2021, costing the world $20 billion (Ferraro, 2021). These attacks have sparked widespread concern globally. Despite its significance, the psychological elements within these cyber threats, specifically individual responses to ransomware attacks, remain largely unexplored. Existing research has primarily focused on the technical aspects of this type of cybercrime, such as prevention mechanisms, security measures, and system vulnerabilities (Masuch et al., 2021). This focus leaves a scarcity in our understanding of human psychological factors, particularly how individual personality traits influence responses to ransomware attacks.

Given that studies have shown individual differences significantly contribute to variations in cybersecurity behavior (Crossler et al., 2013), this research aims to dive deeper into the relationship between specific personality traits, namely the Dark Triad, and responses to cyber threats. The Dark Triad traits, encompassing narcissism, Machiavellianism, and psychopathy, have been associated with risk-prone and manipulative behaviors (Harrison et al., 2018; Paulhus & Williams, 2002). The current literature, however, offers limited insights into how these traits influence responses to cybercrimes like ransomware attacks. Individuals possessing these traits might demonstrate unusual reactions to such threats, potentially impacting decisions about personal data disclosure, ransom payment, and the involvement of law enforcement authorities.

Additionally, this paper examines the role of perceived competency of government agencies, such as the FBI, in shaping individual responses to cyberattacks. Trust in an agency's ability to effectively handle such crises might inspire individuals to report these incidents (Kääriäinen & Sirén, 2011). Yet, the specific interaction between Dark Triad traits and perceived government competency has been unexplored in previous research, even though this interaction could significantly affect decision-making during a cybercrime incident like a ransomware attack. By addressing this paucity in current research, this paper investigates how the Dark Triad influences an individual's reaction to ransomware attacks. The research question guiding this investigation is, *how are the Dark Triad traits associated with victim responses during a ransomware attack?*

To answer the question, we developed a model based on the Dark Triad (Paulhus & Williams, 2002) and perceived competency towards government organizations (Grimmelikhuijsen & Knies, 2017). The

URI: https://hdl.handle.net/10125/106893
978-0-9981331-7-1

model has been tested using data from 287 participants to date and analyzed through structural equation modeling. This work aims to contribute to the evolving research landscape in the domain of cybercrime (Harviainen et al., 2023). More personalized strategies for cyber threat prevention and response can be developed by thoroughly understanding these individual differences, thus enhancing the overall cybersecurity research. We conclude the paper by discussing our findings and implications for research and practice.

2. Theoretical foundations

2.1. Ransomware attack

Ransomware attacks, a common form of cybercrime, involve malicious software encrypting or locking users out of their systems or data and demanding ransom, usually in cryptocurrency. The swift evolution of these attacks presents substantial challenges to businesses, governments, and individuals. The various ransomware types, including crypto-ransomware and locker-ransomware, each with distinct tactics and damage potential, make them attractive to cybercriminals. Current research emphasizes the need for a deeper understanding of ransomware attacks, such as attackers' motives, victims' reactions, and broader socio-technical systems. An interdisciplinary approach, merging technical defenses with human-centric interventions, is necessary. Researchers have highlighted the need for an interdisciplinary approach involving technical defenses and human-centric interventions to cope with the menace of ransomware (Crossler et al., 2013). The dynamics of decision-making during a ransomware attack, the impact of personality traits on responses to such cyber-attacks, and the role of trust in government agencies' competency are emerging themes in the field (Hadlington, 2017). As ransomware attacks continue to increase, it is crucial for ongoing research to stay one step ahead, contributing to the development of robust prevention, response, and recovery strategies.

2.2. Ransomware response

Gaining a comprehensive understanding of responses to ransomware attacks is crucial for effective cybersecurity policymaking. How individuals react to such sophisticated digital attacks can be swayed by various factors, among which risk perception, perceived benefits, and one's level of technical efficacy are prominent (Philip et al., 2023). Academic discourse has also highlighted the intriguing relationship between an individual's perceived susceptibility to ransomware attacks and their subsequent actions. Detailed analyses show that when individuals perceive an escalated threat level, they are more inclined to adopt preventive measures. These might include routine data backups, advanced encryption techniques, updated antivirus software, and engagement with cybersecurity awareness programs. Even though preventive actions such as security compliance and the intention to secure have been extensively covered in the literature (Philip et al., 2023), individual responses during cyberattacks, such as ransomware and phishing, have not been thoroughly studied. Ransomware victims often exhibit various responses, ranging from paying the demanded ransom, an act usually discouraged by cybersecurity experts, to completely abandoning their data. Intriguingly, the response spectrum extends beyond rational calculation and can be influenced by personality traits. For instance, the impact of the Dark Triad – a set of three negative personality traits: narcissism, Machiavellianism, and psychopathy – on individual response behaviors can have significant implications. Research suggests that individuals high in these traits may exhibit less compliance with recommended cybersecurity behaviors, making them more prone to becoming victims of such attacks and responding to them in a sub-optimal manner (Maasberg et al., 2020). This link underscores the necessity to consider psychological factors in designing and implementing effective cybersecurity strategies.

2.3. The dark triad

Understanding the role of personality traits becomes crucial when discussing individual response behavior. While the Big Five (i.e., Openness, Conscientiousness, Extraversion, Agreeableness, and Neuroticism) is a comprehensive model that covers a broad spectrum of personality traits, the Dark Triad is particularly relevant to our research due to its correlation with manipulative and exploitative behaviors, which we believe are particularly relevant in the context of ransomware attacks. Ransomware attacks often involve deception, coercion, and manipulation, traits that can be well-represented within the Dark Triad framework. Therefore, our focus on the Dark Triad was an extension to investigate these specific traits that are more likely to influence an individual's response to such malicious attacks. The Dark Triad, composed of narcissism, Machiavellianism, and psychopathy, offers a perspective in this regard (Paulhus & Williams, 2002). Narcissistic individuals, characterized by grandiosity

and entitlement, may be prone to handle cyber threats independently due to their overconfidence, possibly letting go of their data or trying to resolve the issue themselves. On the other hand, individuals exhibiting Machiavellian traits, known for their manipulative tendencies and self-interest, may perform a cost-benefit analysis and choose to pay the ransom if deemed less costly (Hadlington, 2017). Psychopathy, characterized by impulsivity and thrill-seeking (Harrison et al., 2018; Morgan et al., 2011), can yield unpredictable responses, including perceiving the attack as challenging and deciding to fight back or report it.

2.4. Perceived competency toward government agencies

As we investigate deeper into the factors influencing individuals' responses, the role of perceived competency of government agencies becomes apparent. McKnight et al. (2002) highlight the importance of trusting beliefs, including perceived competency, in shaping behavioral intentions. If individuals perceive institutions like the FBI as competent, they are more likely to report ransom attacks and comply with the guidelines. On the contrary, perceived incompetency can lead individuals to ignore institutional advice and handle the situation independently, often worsening the issue. In essence, the interaction between individual personality traits, their perception of risk, and their trust in the competence of government agencies shape the response to ransom attacks. Understanding these relationships is a steppingstone toward better ransom attack prevention and response strategies.

3. Research model

Literature on cybersecurity behavior suggests a strong relationship between the Dark Triad personality traits and cybercrime. For instance, studies found that personality traits, including the Dark Triad, significantly influence behavior in cybersecurity threats (Maasberg et al., 2020) and unethical behavior (Harrison et al., 2018). Specifically, studies observed a correlation between Dark Triad traits and malicious cyber threats behaviors, such as abandoning control over personal data. Other studies supported these findings in which scholars found a significant link between Dark Triad traits, particularly psychopathy and Machiavellianism, and a disregard for secure cyber practices (Padayachee, 2020). This might suggest that individuals with these traits are more likely to give up their personal data during a cyber-attack. When examined individually, each Dark Triad trait provides further insight into this relationship. Narcissistic individuals may underestimate risks due to their overconfidence; Machiavellian individuals might disregard secure practices in pursuit of personal gain; and individuals with psychopathic traits may impulsively give up their data due to their thrill-seeking nature (Paulhus & Williams, 2002). Existing literature finds that these individuals often engage in risky actions driven by a desire for personal gain or thrill (Crysel et al., 2013). In the context of a ransom attack, this predisposition towards risk, antisocial, and impulsiveness (Book et al., 2015) could manifest as a willingness to abandon personal data. The potential benefits, such as avoiding the ransom payment, may be perceived by these individuals as outweighing the potential costs, such as losing personal data. Moreover, people with Dark Triad traits often fail to empathize with others (Jonason & Krause, 2013), which could extend to a lack of concern for the potential harm caused by losing their personal data. Impulsivity is another characteristic often associated with the Dark Triad, as studies found these individuals tend to make quick, rash decisions without fully considering the potential consequences (Jones & Paulhus, 2011). In a high-pressure situation like a ransom attack, this impulsivity could lead to hasty decisions, such as abandoning data or quickly paying the ransom. Though the decision to abandon personal data during a ransom attack is not solely a function of personality traits, existing literature suggests that individuals often underestimate the value of their personal data and the potential harm that could result from its loss (Acquisti et al., 2015). This underestimation could further contribute to the likelihood of individuals with Dark Triad traits abandoning their data during a ransom attack, as individuals with the Dark Triad tendency seem to lead to antisocial behavior, impaired empathy, and lack of remorse. Therefore, the combination of risk-taking behavior, lack of empathy, impulsivity, and underestimation of the value of personal data makes it plausible to hypothesize that individuals with higher levels of Dark Triad traits are more likely to abandon their personal data during a ransom attack. Taken together, these insights form the basis for our first hypothesis:

Hypothesis 1: *Individuals with higher levels of Dark Triad traits are more likely to abandon their personal data during a ransom attack.*

Those who have Dark Triad traits also have a range of their manifestation. Drilling down into the nature of Dark Triad personality traits allows us to understand why such individuals might be more inclined to pay ransom during cyber-attacks. For

instance, the Machiavellian tendency to focus on self-interest and manipulate others for personal gain (Paulhus & Williams, 2002) could inform their decision-making during a ransom attack. Evaluating the situation through a utilitarian lens, these individuals might weigh the costs and benefits and decide that paying the ransom is the quickest, least damaging way to recover their data (Jones & Paulhus, 2017). Narcissistic individuals, meanwhile, might be driven to pay the ransom due to their inflated self-perception. The loss of control they experience during a ransom attack could be intolerable for these individuals, and paying the ransom could be a means for them to regain control quickly (Bushman & Baumeister, 2002).

Finally, the impulsive characteristic of psychopathy might lead individuals with this trait to act quickly without considering the long-term implications (Harrison et al., 2018; Morgan et al., 2011). Their need for an immediate solution could lead to a willingness to pay the ransom. These tendencies are underpinned by the observation that Dark Triad traits are often associated with risky behavior in the face of cybersecurity threats (Crossler et al., 2014). This provides further reason to believe that individuals with these traits would be more inclined to pay the ransom, despite the risk of doing so. Based on these insights, we propose:

Hypothesis 2: *Individuals with higher levels of Dark Triad traits are more likely to pay the ransom demanded by the attackers.*

Additionally, there are reasons to believe that individuals with high levels of Dark Triad traits might be less likely to report ransom attacks to authorities like the FBI. For instance, narcissistic individuals might feel capable of handling the situation independently due to their grandiosity and sense of superiority. Those with high Machiavellianism might fear the negative consequences of making the attack public, such as reputational damage, and so might avoid reporting the attack (Hadlington, 2017). Lastly, those with psychopathy might deem the reporting process tedious and unimportant due to their impulsivity and lack of empathy, thus potentially being less likely to report the attack. This leads us to propose,

Hypothesis 3: *Individuals with higher levels of Dark Triad traits are less likely to report the situation to the FBI during a ransom attack.*

The role of trust in institutions, particularly cybersecurity, is a critical factor that can significantly shape individuals' responses to ransom attacks. This trust is often influenced by the perceived competence of government agencies, such as the FBI. As articulated by McKnight and Choudhury (McKnight et al., 2002), the concept of trusting beliefs provides a theoretical framework for understanding this relationship. In this context, the perceived competence of the FBI is defined as the belief in the agency's skills, expertise, and ability to handle cybersecurity threats effectively. A positive perception of the FBI's competence can engender high trust in the institution. This trust, in turn, can influence individual behavior during a cybersecurity threat. If individuals perceive the FBI as competent, they are more likely to trust the agency's advice and guidance in the event of a ransom attack. This trust can foster a greater willingness to report cyber incidents, as individuals may believe that the FBI has the necessary expertise to respond to the threat and mitigate its impact effectively. This argument is supported by empirical research in the field of information systems, which states that trust in an institution, which is influenced by the perceived competence of the institution, can significantly impact individuals' behavior in the context of cybersecurity (Ifinedo, 2012). Specifically, individuals who trust an institution and perceive it as competent are more likely to follow the institution's advice and report cyber incidents. Trust in an institution's competence can encourage individuals to take recommended actions, such as reporting a ransom attack, which can help mitigate the attack's impact and contribute to overall cybersecurity. Therefore, we can propose the following hypothesis:

Hypothesis 4: *Individuals who perceive the FBI as highly competent are more likely to report a ransom attack to the FBI.*

The Dark Triad personality traits have been recognized for their influence on an individual's behavior across various contexts, including cybersecurity. These traits can result in riskier cybersecurity behaviors (Hadlington, 2017) and might increase the likelihood of an individual surrendering personal data during a ransomware attack. Meanwhile, the perceived competency of law enforcement organizations, such as the FBI, can greatly influence an individual's response during cybersecurity incidents. A study found that the perceived competency of these entities can either serve as a deterrent for illegal activities or as a risk modifier that influences an individual's decision-making process (Ifinedo, 2012). In other words, if the FBI is perceived as highly competent, individuals with Dark Triad traits might assess the situation as risky. They might not want the police to discover more about them, potentially leading them to abandon data during a ransomware attack due to increased perceived risk.

Moreover, cognitive dissonance theory may shed light on the underlying psychological processes. When Dark Triad individuals perceive the FBI to be highly

competent, they may experience cognitive dissonance due to the conflict between their self-perceived freedom, as research found that ego threat is highly associated with the Dark Triad (Crysel et al., 2013). They may abandon their data during ransomware attacks as a coping mechanism, viewing it as a more risky and impulsive choice than the prospect of tangling with a highly skilled FBI agent. And more importantly, individuals with higher Dark Triad traits are more likely to develop antisocial behaviors and highly likely unethical behavior (Harrison et al., 2018), which might prevent them from acting according to the social norms (Book et al., 2015), as they fear that the FBI might find something wrong or unethical about them. Given these points, the interaction of Dark Triad traits and the perceived competency of the FBI seems to be an essential factor influencing the decision-making process during a ransomware attack. Hence, we propose,

Hypothesis 5: *The perceived competency of the FBI moderates the relationship between Dark Triad traits and the likelihood of abandoning an individual's personal data, such that the relationship is stronger among those who have a higher perception of competency toward the FBI.*

As for ransom payment, individuals with Dark Triad traits may be more inclined to resolve the situation swiftly by paying the ransom (Crossler et al., 2014). This propensity could be exacerbated if the FBI is perceived as highly competent. If individuals believe that the FBI can effectively trace the ransom payment and apprehend the attacker, they may perceive the entire investigation process as an impediment and lengthy. Thus, they tend to accept the immediate resolution offered by the attackers by paying the ransom. More importantly, the Dark Triad has been associated with unethical behavior [5], indicating that people with these traits do not want the FBI to get involved in the investigation because they fear that the Bureau might find some unethical behaviors that make them vulnerable. Hence, we propose,

Hypothesis 6: *The perceived competency of the FBI moderates the relationship between Dark Triad traits and the likelihood of paying the ransom to the attacker, such that the relationship is stronger among those who have a higher perception of competency toward the FBI.*

In sum, both the Dark Triad traits and the perceived competence of government agencies might shape individuals' decision-making and behaviors during ransom attacks. Significantly, Dark Triad traits might magnify risk-taking behaviors, potentially overpowering the influence of perceived government competency and resulting in potentially detrimental choices such as surrendering personal data or paying the ransom. The situation might be different when reporting the ransom attack to the FBI. As discussed earlier, Dark Triad traits could potentially reduce the likelihood of reporting the attack to the FBI. If the FBI is perceived as highly competent, individuals with Dark Triad traits may feel their self-interest could be jeopardized through potential legal repercussions or public exposure. Therefore, they may be less likely to report the attack, even when recognizing the FBI's competence. To enhance our understanding, we further investigate the combined effects of Dark Triad traits and the perceived competency of the FBI. Narcissistic individuals, due to their inflated sense of self-importance and entitlement, might feel that their skills alone can resolve the situation, irrespective of the FBI's competence (Bushman & Baumeister, 2002).

Similarly, Machiavellian individuals, given their tendency to manipulate situations for personal gain, might perceive collaboration with competent authorities as potentially exposing their manipulative tactics and causing harm to their personal interests (Jones & Paulhus, 2017). Lastly, individuals with psychopathic traits, characterized by impulsivity, might view reporting to the authorities as a prolonged process and instead prefer immediate actions, regardless of the competency of the FBI (Crysel et al., 2013). This leads to,

Hypothesis 7: *The perceived competency of the FBI moderates the relationship between Dark Triad traits and the likelihood of reporting the ransom attack to the FBI. Specifically, the negative relationship is magnified among those who have a higher perception of competency toward the FBI.*

These hypotheses, as briefly depicted in Figure 1, underscore that individual personality traits and perceptions about institutional competence play pivotal roles in shaping responses to ransom attacks. Moreover, they highlight the need for a more nuanced understanding of how these factors interact in shaping such behaviors. With the development of these hypotheses, we aim to uncover complex dynamics that influence an individual's response to a ransom attack.

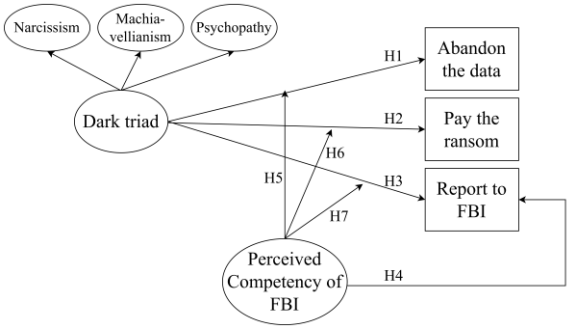

Figure 1. Proposed research model

4. Methodology

4.1. Participants

Using the *pwrSEM* package in R, we determined that a sample size of 230 is required to achieve a power of 0.80 at a 0.05 significance level for detecting a small-to-medium effect size in our structural equation model (SEM). To achieve this, we surveyed 318 workers from the U.S. using the Prolific.co platform, offering a small monetary incentive. Prolific is favored in social science research due to its generalizability over traditional methods such as student samples (Palan & Schitter, 2018). Out of the participants, four failed attention checks and 27 did not complete tasks satisfactorily, leaving 287 usable responses. The age of the sample ranged from 19 to 80 (mean = 37.30, SD = 13.42). 40.1% identified as female, 73.9% identified as White, and their educational backgrounds ranged from less than high school to graduate or professional degrees.

4.2. Measures

The online study commenced with a demographic questionnaire and a clear definition of ransomware. The survey then utilized the Dark Triad measure developed by Jonason and Webster (2010) to measure participants' levels of these personality traits. We subsequently assessed perceptions of the FBI's competence using a scale adapted from Grimmelikhuijsen and Knies (2017), derived initially from McKnight et al. (2002). Table 1 below provides the measurement items and their statistics.

Table 1. Measurement items and statistics

Items	Mean	SD	Loading
Perceived competence of the FBI (Grimmelikhuijsen & Knies, 2017)			
If there is a ransomware attack, the FBI is capable of helping me getting my data back.	4.46	1.391	0.933
If there is a ransomware attack, the FBI is an expert in helping me deal with the problem.	4.34	1.432	0.928
If there is a ransomware attack, the FBI carries out its duty very well.	4.33	1.334	0.919
Machiavellianism (Jonason & Webster, 2010)			
I tend to manipulate others to get my way.	2.38	1.752	0.924
I have used deceit or lied to get my way.	3.23	1.993	0.853
I have use flattery to get my way.	3.53	2.067	0.813
I tend to exploit others towards my own end.	2.13	1.632	0.904
Psychopathy (Jonason & Webster, 2010)			
I tend to lack remorse.	2.07	1.658	0.909
I tend to be unconcerned with the morality of my actions.	2.12	1.667	0.902
I tend to be callous or insensitive.	2.52	1.855	0.921
I tend to be cynical.	3.63	2.151	0.706
Narcissism (Jonason & Webster, 2010)			
I tend to want others to admire me.	3.51	2.062	0.872
I tend to want others to pay attention to me.	3.19	2.025	0.910
I tend to seek prestige or status.	2.98	1.992	0.893
I tend to expect special favors from others.	2.46	1.789	0.870
Victim responses (self-developed)			
How likely would you be to make the ransomware payment to the attacker in order to recover access to your files?	2.53	1.657	-
How likely would you be to report the attack to the FBI?	4.92	1.941	-
How likely would you be to let go of the data/files on your computer and do nothing?	3.33	2.010	-

4.3. Procedures

Following these steps, we presented participants with a hypothetical ransomware attack scenario to understand their potential responses in a real-life situation. The scenario was as follows:
"*Imagine that you have fallen victim to a ransomware attack and can no longer access any of your files, including critical personal and financial data such as important photos and videos, tax documents (including your social security number), healthcare records, and your online banking account passwords saved in your browser. Furthermore, you do not have any backups of these files on another device or in a cloud storage platform such as Google Drive. The attacker is demanding a ransom of $1,000 USD, to be paid in a cryptocurrency like Bitcoin, in order to restore access to your files.*" This scenario offered a

realistic context for participants to demonstrate potential actions, thereby providing a rich basis for analyzing the relationships posited in our hypotheses.

5. Data analyses and results

5.1. Measurement model assessment

To assess the factor structure of our measurement items, we used the *lavaan* package of R with a covariance-based maximum likelihood estimation. The measurement model exhibited an adequate fit to the data with the following fit indices recommended cutoff. Indicators of good fit include a Comparative Fit Index (CFI) and Tucker-Lewis Index (TLI) above .90, Standardized Root Mean Square Residual (SRMR), and Root Mean Square Error of Approximation (RMSEA) below .08 (Hair Jr et al., 2017). The model exhibited a good fit, Chi-square 245.891 with 84 degrees of freedom (df); therefore, Chi-square/df = 2.927. CFI = 0.947, TLI = 0.933. SRMR = 0.055, RMSEA = 0.080. All factor loadings, both first and second-order constructs, were significant ($p < 0.05$), indicating that all the observed variables were valid measures of their respective latent constructs. As shown in Table 2, all constructs' composite reliability and Cronbach's alpha values exceeded 0.7, indicating good internal consistency. The Average Variance Extracted (AVE) for all constructs surpassed 0.5, confirming convergent validity. For discriminant validity, in each case, the square root of the AVE was greater than the inter-construct correlations, confirming that each construct shared more variance with its own measures than with any other construct (see table A1 in the appendix for details). This indicates acceptable discriminant validity for all constructs in our model.

Table 2. Latent constructs' statistics

Construct	AVE	CR	Alpha
FBI competence	0.859	0.919	0.918
Machiavellianism	0.765	0.906	0.897
Psychopathy	0.746	0.901	0.883
Narcissism	0.785	0.914	0.909

Note: AVE = Average variance extracted; CR = Composite reliability; Alpha = Cronbach's alpha

5.2. Structural model assessment

Transitioning from evaluating the measurement model, we moved on to assess our proposed hypotheses. The findings of this study confirm several important hypotheses. We start with hypothesis 1, which suggests that individuals with higher levels of Dark Triad traits are more likely to abandon their personal data during a ransom attack. Our results support this premise, demonstrating a positive relationship between Dark Triad traits and the likelihood of abandoning personal data (effect size = 0.293, $p < 0.001$, 95% CI [0.173, 0.436]). Following this, we examined hypothesis 2, positing that these individuals - those higher in Dark Triad traits - are more likely to accept the attackers' demands and pay the ransom. Our data provided further support for this hypothesis, again highlighting a positive relationship (effect size = 0.193, $p < 0.001$, 95% CI [0.033, 0.348]).

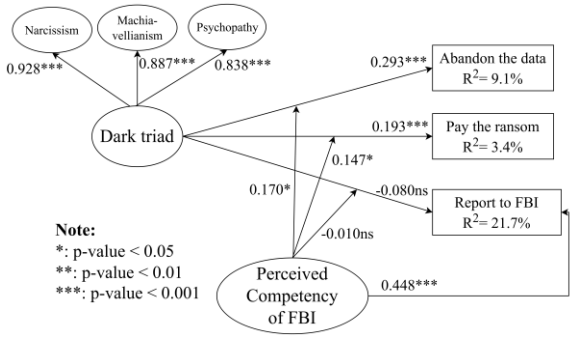

Figure 2. Initial results

These findings show a concerning pattern of individuals with pronounced Dark Triad traits demonstrating potentially risky behaviors in response to ransom attacks. However, the results did not support all hypotheses. For instance, hypothesis 3, which proposed that individuals with higher levels of Dark Triad traits would be less likely to report a ransom attack to the FBI, did not find support in our data (effect size = -0.080, $p = 0.195$, 95% CI [-0.198, 0.047]). This suggests that Dark Triad traits do not necessarily discourage the willingness to involve law enforcement in such situations.

In contrast, we found statistical support for hypothesis 4, suggesting that those individuals who perceive the FBI as highly competent are more inclined to report a ransom attack to the Bureau (effect size = 0.448, $p < 0.001$, 95% CI [0.341, 0.546]). This highlights the significance of the perceived competency of law enforcement in influencing individuals' decisions about reporting cyberattacks.

Moreover, the analysis shed light on how the perceived competency of the FBI might interact with Dark Triad traits. Hypothesis 5 proposed that a higher perceived competency of the FBI strengthens the relationship between Dark Triad traits and the likelihood of abandoning personal data. Our results confirmed this moderating effect (effect size = 0.170, $p = 0.022$, 95% CI [0.034, 0.321]). Subsequently, hypothesis 6 extended this idea to the likelihood of paying the ransom, suggesting a stronger relationship

among those who view the FBI as highly competent. The findings supported this hypothesis (Effect size = 0.147, p = 0.036, 95% CI [0.009, 0.271]). These outcomes underscore the complex interaction between individual personality traits and attitudes toward law enforcement in shaping responses to cyber threats. Finally, we considered hypothesis 7, which extended this moderation effect to the likelihood of reporting the ransom attack to the FBI.

Interestingly, unlike the previous hypotheses, this one did not find support in our data (effect size = -0.010, p = 0.881, 95% CI [-0.136, 0.125]). Overall, our findings reveal a picture of how individual psychological factors and perceptions of law enforcement competence interrelate in the context of ransom attacks. Most notably, we observed that all hypotheses were supported except for hypotheses 3 and 7, suggesting areas for future investigation. Figure 2 reports the initial results from our hypotheses testing.

5.3. Additional analysis for hypotheses 1 and 2

The coexistence of hypotheses 1 and 2 can be understood by considering how each dimension of the Dark Triad might affect an individual differently based on the intensity of that dimension. To ensure the robustness of these findings, we conducted t-tests on each dimension of the Dark Triad split by the mean of our scale to separate high vs low, and each response (i.e., abandoning, paying the ransom amount, and reporting to the FBI). The likelihood of abandoning the data was analyzed by an independent samples t-test. There was a statistically significant difference in the scores for the low narcissism group (M = 3.02, SD = 2.121) and high narcissism group (M = 3.55, SD = 1.889); t(287) = -2.486, p = 0.013, d = 2.004. There was also a statistically significant difference in the scores for the low psychopathy group (M = 2.84, SD = 2.018) and the high psychopathy group (M = 3.83, SD = 1.889); t(287) = -4.772, p < 0.001, d = 1.960. The results indicate that the likelihood of abandoning the data is associated with both psychopathy and narcissism, where the effect size magnitude appears larger for individuals with higher psychopathy traits.
Similarly, for the likelihood of paying the ransomware amount, there was a statistically significant difference in the scores for the low narcissism group (M = 2.17, SD = 1.537) and the high narcissism group (M = 2.74, SD = 1.718), t(287) = -3.275, p = 0.001, d = 1.633. There was no significant difference in the scores for the low psychopathy group (M = 2.32, SD = 1.612) and the high psychopathy group (M = 2.64, SD = 1.693); t(287) = -1.825, p = 0.069. The results indicate that the likelihood of paying the ransom is mainly associated with narcissism traits.

The results showed no statistically significant differences in behaviors across different Machiavellianism levels. Specifically, there was no statistically significant difference in abandoning the data between the low Machiavellianism group (M = 3.26, SD = 2.131) and the high Machiavellianism group (M = 3.52, SD = 1.843); t(287) = -1.097, p = 0.274. Similarly, there was no significant difference in paying the ransom between the low Machiavellianism group (M = 2.33, SD = 1.583) and the high Machiavellianism group (M = 2.58, SD = 1.637); t(287) = -1.316, p = 0.189.

Based on the t-tests, the results suggest that victims with higher psychopathy traits are more likely to abandon their data, while those with higher narcissism traits are more likely to either pay the ransom or abandon their data. Machiavellianism does not seem to be a factor driving these two responses.

6. Discussion

We found that individuals with higher levels of Dark Triad traits are more likely to abandon their personal data and pay the ransom demanded by attackers during a ransom attack (i.e., hypotheses 1 and 2). These findings underscore the need to explore the motivations and decision-making processes of individuals with these personality traits when faced with cyber threats. For more comprehensive insights, future research should manipulate the ransom amount as this would facilitate a deeper understanding of the thresholds at which individuals decide to pay or abandon the data, particularly when faced with exorbitantly high demands. In the present study, we did not manipulate the requested ransom amount.

On the other hand, the data did not support that individuals with higher levels of Dark Triad traits are less likely to report a ransom attack to the FBI (i.e., hypothesis 3). Future research should explore the factors influencing individuals' decisions to report cyberattacks, including their perception of the potential benefits, risks, and efficacy of involving law enforcement agencies. Interestingly, individuals who perceive the FBI as highly competent are more likely to report a ransom attack to the Bureau (hypothesis 4). This emphasizes the importance of public perception of law enforcement agencies in influencing individuals' willingness to seek help and report cyber incidents. Moreover, the study explored the moderating effect of perceived FBI competency on the relationship between Dark Triad traits and individuals' responses to ransom attacks (i.e., hypotheses 5, 6, and 7). The results supported that a higher perceived competency of the FBI strengthens the relationship between Dark Triad traits and the likelihood of

abandoning personal data and paying the ransom (hypotheses 5 and 6). These findings highlight the nuanced interplay between individual personality traits, perceptions of law enforcement competency, and cybersecurity decision-making. However, the data did not support the moderation effect of the likelihood of reporting the ransom attack to the FBI (hypothesis 7).

6.1. Theoretical implications

This research adds depth to our knowledge of individual responses to ransom attacks, a significant form of cybercrime, particularly regarding Dark Triad personality traits and perceptions of law enforcement competency. It confirms Dark Triad traits significantly influence reactions to these cybercrime instances. Future studies should explore these traits' motivations to enhance risk mitigation strategies. Counterintuitively, Dark Triad traits did not hinder ransom attack reporting to the FBI, implying even individuals with these traits might cooperate with law enforcement. This unexpected finding merits further examination. The research also emphasizes the role of the FBI's perceived competence in reporting attacks, underlining the importance of public trust in law enforcement and the potential for increased reporting through improved public perception.

Additionally, we found the interaction effects between Dark Triad traits and the perceived competency of the FBI. Our data showed that the impact of Dark Triad traits on individuals' responses to ransom attacks could be moderated by their views of the FBI's competency. However, intriguingly, this interaction effect did not hold regarding the likelihood of reporting the attack. This discrepancy presents a valuable opportunity for future research to investigate why this interaction effect does not extend to reporting behaviors. Overall, this study has augmented our understanding of the factors influencing individual responses to cybercrime, specifically ransom attacks.

6.2. Practical implications

This study's implications highlight the need for strategic interventions to lessen ransom attack impacts. Recognizing that Dark Triad traits may lead to riskier behavior during such attacks underscores the importance of self-awareness and education about these traits. Programs that help individuals identify their personality traits and potential response to cyber-attacks can be effective. The findings also have relevance for corporate practices, alerting companies to the risks posed by employees with Dark Triad traits during cyber-attacks. On a broader scale, the results emphasize the importance of law enforcement's reputation, especially the FBI's, in influencing the public's likelihood to report ransom attacks. It necessitates law enforcement agencies to focus on enhancing their public image through measures like community outreach, public awareness drives, or showcasing cybercrime resolution successes to boost public trust and reporting of cyber-attacks.

6.3. Limitations

This study offers key insights into the impact of Dark Triad traits and law enforcement competency perceptions on responses to ransom attacks, yet some limitations exist. Using an online survey may not fully represent decision-making complexities during an actual ransom attack due to its hypothetical nature. In terms of study manipulation, we encourage future research to manipulate the nature of the data, for instance, utilitarian versus hedonic or personal versus work. The predominantly White sample constrains the findings' applicability across varied cultures and demographics. Social desirability bias could skew self-reported responses regarding Dark Triad traits, potentially leading to an underestimation of these traits. Individuals may be reluctant to admit or might even lack self-awareness about possessing these traits due to the associated stigma. People often wish to present themselves in a favorable light, especially when the information could be shared or viewed by others. Additionally, given the important role of trust in government agencies, future research could potentially examine a model in which perceived competency mediates between the Dark Triad and responses to ransomware attacks. Future studies should strive to address these issues.

7. Conclusion

In conclusion, we found support for the association between higher levels of Dark Triad traits and a propensity to abandon personal data and acquiesce to attackers' demands during ransom attacks. We also discovered interaction effects between the Dark Triad traits and perceived competency of government agencies, i.e., the FBI. These findings underscore the complexity of individual behaviors in cybercrime contexts (Harviainen et al., 2023), highlighting the crucial role of personality traits and perceptions of law enforcement competency.

8. References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509-514.

Book, A., Visser, B. A., & Volk, A. A. (2015). Unpacking "evil": Claiming the core of the Dark Triad. *Personality and Individual Differences*, *73*, 29-38.

Bushman, B. J., & Baumeister, R. F. (2002). Does self-love or self-hate lead to violence? *Journal of Research in Personality*, *36*(6), 543-545.

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.

Crossler, R. E., Long, J. H., Loraas, T. M., & Trinkle, B. S. (2014). Understanding compliance with bring your own device policies utilizing protection motivation theory: Bridging the intention-behavior gap. *Journal of Information Systems*, *28*(1), 209-226.

Crysel, L. C., Crosier, B. S., & Webster, G. D. (2013). The Dark Triad and risk behavior. *Personality and Individual Differences*, *54*(1), 35-40.

Ferraro, M. F. (2021). Ransomware attacks are about to get worse. But there are ways to stop them. CNN Business.

Grimmelikhuijsen, S., & Knies, E. (2017). Validating a scale for citizen trust in government organizations. *International Review of Administrative Sciences*, *83*(3), 583-601.

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, *3*(7), e00346.

Hair Jr, J. F., Babin, B. J., & Krey, N. (2017). Covariance-based structural equation modeling in the Journal of Advertising: Review and recommendations. *Journal of Advertising*, *46*(1), 163-177.

Harrison, A., Summers, J., & Mennecke, B. (2018). The effects of the dark triad on unethical behavior. *Journal of Business Ethics*, *153*, 53-77.

Harviainen, T., Hamari, J., Siuda, P., & Gehl, R. W. (2023, January). Understanding and Moving Forward Research on Online Crime: Introduction to Cybercrime Minitrack. *In Hawaii International Conference on System Sciences 2023* (pp. 3609-3610).

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83-95.

Jonason, P. K., & Krause, L. (2013). The emotional deficits associated with the Dark Triad traits: Cognitive empathy, affective empathy, and alexithymia. *Personality and Individual Differences*, *55*(5), 532-537.

Jonason, P. K., & Webster, G. D. (2010). The dirty dozen: a concise measure of the dark triad. *Psychological Assessment*, *22*(2), 420.

Jones, D. N., & Paulhus, D. L. (2011). The role of impulsivity in the Dark Triad of personality. *Personality and Individual Differences*, *51*(5), 679-682.

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.

Kääriäinen, J., & Sirén, R. (2011). Trust in the police, generalized trust and reporting crime. *European Journal of Criminology*, *8*(1), 65-81.

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.

Masuch, K., Hengstler, S., Schulze, L., & Trang, S. (2021). The Impact of Threat and Efficacy on Information Security Behavior: Applying an Extended Parallel Process Model to the Fear of Ransomware. *Proceedings of the 54th Hawaii International Conference on System Sciences.*

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research*, *13*(3), 334-359.

Morgan, J. E., Gray, N. S., & Snowden, R. J. (2011). The relationship between psychopathy and impulsivity: A multi-impulsivity measurement approach. *Personality and Individual Differences*, *51*(4), 429-434.

Padayachee, K. (2020). Understanding the relationship between the dark triad of personality traits and neutralization techniques toward cybersecurity behaviour. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, *10*(4), 1-19.

Palan, S., & Schitter, C. (2018). Prolific. ac—A subject pool for online experiments. *Journal of Behavioral and Experimental Finance*, 17, 22-27.

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.

Philip, S. J., Luu, T. J., & Carte, T. (2023). There's No place like home: Understanding users' intentions toward securing internet-of-things (IoT) smart home networks. *Computers in Human Behavior*, *139*, 107551.

Appendix

Table A1. Correlation table and $\sqrt{AVE}$ (bolded)

	1	2	3	4	5	6	7
1	**0.927**						
2	-0.133*	**0.875**					
3	-0.171**	0.777**	**0.864**				
4	-0.069	0.674**	0.570**	**0.886**			
5	-0.159**	0.165**	0.250**	0.184**	-		
6	0.457**	-0.148**	-0.120**	-0.104	-0.182**	-	
7	0.052	0.129	0.033	0.005	-0.019	-0.015	-

1 - Perceived competence of the FBI.
2- Machiavellianism. 3 – Psychopathy. 4 – Narcissism. 5 - Abandon data. 6 - Report to the FBI. 7- Pay the ransom