Malicious Insider Behaviour in Cybersecurity Informed by the Fraud Triangle

Chelsea Idensohn and Stephen Flowerday
The University of Tulsa, Department of Cyber Studies
cji6709@utulsa.edu and stephen-flowerday@utulsa.edu

Abstract

The prevalence of cybersecurity insider threats is increasing rapidly. Whilst organisations deploy advanced inside threat detection technologies, the effectiveness of such measures remains questionable. The propensity for individuals with higher scores on the Dark Triad personality traits –Machiavellianism, narcissism, and psychopathy- to perceive themselves as more capable, motivated, and opportunistic in conducting malicious cybersecurity acts reveals a significant oversight. Such individuals are not only more likely to engage in harmful behaviours, but also to rationalise their actions. This discrepancy highlights the need for a deeper understanding of the psychological underpinnings of insider threats, beyond the scope of traditional cybersecurity measures. This study seeks to enrich the academic discourse by employing the Fraud Triangle Framework with the Dark Triad as an additional dimension to delve into the psychological drivers of insider cybersecurity breaches. By acknowledging the pivotal role of the human element in organisational security, linking specific personality traits to insider threat potential, our research addresses a notable gap in scholarly dialogue and organisational risk management models. The findings underscore the need for fraud risk models to incorporate personality influences and advocate for a multidisciplinary approach that combines technological and behavioural understandings of cybersecurity.

Keywords: Malicious Insider Cybersecurity Behaviour, Inside Threats, Fraud Triangle, Dark Triad

Introduction

Malicious insider threats in the cybersecurity realm have significantly increased in stealth, with the constant advancements in technology allowing for their actions to be more elusive (Harrison et al., 2018). The role of human behaviour emerges as a critical factor in the battle against organisational threats. As organisations grapple with the ominous threat of malicious insiders (Maasberg et al., 2015) it is increasingly imperative that underlying influences which drive individuals' malicious behaviour are deciphered (Burch et al., 2021).

Referred to as the "looming crisis" (Rauthmann & Kolar, 2012), organisations face a major challenge, which is the "widespread failure of organisations to recognise and respond decisively to insider threats" (Maasberg et al., 2020). Whilst organisations devote resources to the protection of their infrastructure against such potential inside threats, it is not always sufficient to stop the immense peril that insider threats intentionally cause (Maasberg et al., 2020a). This is because not enough is known about their insiders, the employees, especially regarding their personalities and situational factors, which play a key factor in determining malicious behaviour (Burch et al., 2021).

This research innovatively integrates dark personality traits within the Fraud Triangle's framework to examine malicious insider threats more comprehensively. Literature suggests that merging these elements with the Dark Triad traits could significantly increase the potential for risk identification of malicious insiders within organisations (Epstein & Ramamoorti, 2016; Harrison et al., 2018; Maasberg et al., 2020;

Sariçi̇çek, 2023). This study delves into the relationship between these psychological and situational factors. By enriching the Fraud Triangle with the Dark Triad, we seek to offer a more holistic understanding of the mechanisms driving malicious insider behaviour, thereby advancing our grasp of its underlying causes.

According to the Cost of Insider Risks global report by the Ponemon Institute and DTex, insider security risks are on the rise (BobSulli, 2023). In 2023, 73% of companies experienced between twenty-one and over forty insider security incidents. This is a 67% increase from the previous year. Malicious insiders accounted for an average of 6.2 of these incidents and cost an average of $701, 500 per incident (BobSulli, 2023). Insider threats emerge when trusted individuals, whether current or former members, engage in actions that compromise the organisation's security (Maasberg et al., 2015). The issue revolves around their capacity to misuse a privileged position for activities that are deemed inappropriate or harmful. Insiders constitute greater risks for organisations compared to external threats because of their access to organisational information systems (Maasberg et al., 2015). This risk is intensified by their extensive organisational knowledge and the trust vested in them (Maasberg et al., 2020).

The shared concern regarding insider threats revolves around the fundamental idea that humans represent the Achilles' heel of organisational cybersecurity (Burch et al., 2021; Maasberg et al., 2015, 2020). This emphasises the paramount importance of understanding and gaining critical insight into the traits that render individuals as significant vulnerabilities to an organisation. The challenge of insider threats stems from the subjective nature of an individual's underlying psychology and situational factors, indicating that the creation of effective insider threat detection cannot rely solely on objective technology (Maasberg et al., 2015).

Insider threat behaviour represents unethical actions and fraudulent behaviour within organisations (Whitty, 2021). Individuals act unethically and commit fraud for several reasons. The examination of influential psychological factors that impact an individual’s propensity to act unethically within organisations is a growing topic in literature (Harrison et al., 2018). Psychologists have identified three interrelated dark personality traits – Machiavellianism, narcissism, and psychopathy – collectively referred to as the Dark Triad (Jones & Paulhus, 2014). All three of these traits have been consistently associated with manipulative and maladaptive behaviours correlating with unethical decision-making, counterproductive workplace behaviour, and fraud (Carré et al., 2020; Harrison et al., 2018; Jones & Paulhus, 2014, 2014; Maasberg et al., 2020; Paulhus & Williams, 2002; Rauthmann & Kolar, 2012; Sariçi̇çek, 2023). These dark traits are predictive of self-serving and callous workplace behaviour and yet have been largely overlooked in existing behavioural models within organisations (Jones, 2014). While traditional security measures focus on technological defences, the influence of individual psychology, particularly the Dark Triad’s dark personality traits on cybersecurity threats, has also been less explored (Maasberg et al., 2020). The oversight represents a critical gap in current research, as these traits can offer predictive insights into malicious behaviours within organisations (Harrison et al., 2018).

The Fraud Triangle is a risk assessment model that provides an interactionist perspective on unethical decisions that emerge in fraud cases (Harrison et al., 2018). Its theory is popular among criminologists and accounting firms for pinpointing the risk factors associated with individuals who engage in fraud (Epstein & Ramamoorti, 2016). It encompasses the motivation behind an individual’s actions, the opportunity to exploit others, and the capacity to rationalise their actions within their own set of ethics (Cressey 1953). It has, however, been criticised for its simplicity and oversight of personality – a critical predictor (Epstein & Ramamoorti, 2016). The theory fails to consider how certain personality traits may lead individuals to perceive fraudulent opportunities that others might miss, extending beyond merely possessing the inclination to engage in fraudulent activities (Epstein & Ramamoorti, 2016). Research demonstrates that the traits of the Dark Triad jointly serve as significant predictors of fraudulent actions where each trait affects different parts of the unethical decision-making process (Harrison et al., 2018; Maasberg et al., 2020; Sariçi̇çek, 2023). Machiavellianism not only drives individuals towards unethical behaviour but also changes their view on available opportunities to mislead others. Narcissism influences individuals to behave unethically for their own gain and alters their capacity to execute fraud successfully. Psychopathy significantly influences individual’s rationalisation for their fraudulent actions (Harrison et al., 2018).

This study proposes the following problem statement:

The escalation of cybersecurity insider threats creates a pressing challenge in safeguarding organisational security and emphasises a critical demand for an adaptive perspective at identifying risks posed by malicious cybersecurity insiders.

There is a notable gap in understanding the impact of individual dispositions on behaviours within organisational security contexts (Maasberg et al., 2020; Whitty, 2021). This study addresses this gap by applying the Fraud Triangle to explore how the Dark triad personality traits relate to malicious insider behaviours, aiming for deeper insight into the psychological factors driving cybersecurity breaches. By amplifying the Fraud Triangle with the influence of dark psychological traits we provide a more robust model to understand malicious insider behaviour.

Theoretical Foundation

The theoretical foundation of this research explores three pivotal elements: the phenomenon of insider threats, the role of the Fraud Triangle -a well used and widely accepted risk model in the accounting profession, and the application of the Dark Triad personality traits. Each segment contributes to a holistic understanding of the factors that drive malicious insider cybersecurity behaviour, laying the groundwork for a deeper examination of how individual psychology and situational factors converge to pose risks to organisational security.

Insider Threats

The Cybersecurity & Infrastructure Security Agency (CISA) defines an insider as an individual granted authorised access to or possessing knowledge of an organisation's assets, including personnel, facilities, information, equipment, networks, and systems (CISA, 2023). An insider threat is defined by The National Institute of Standards and Technology (NIST) as the risk by an insider who intentionally or unintentionally, uses their authorised access to compromise the security of an organisation’s operations and assets, harm individuals, affect other organisations or threaten national security (Ross et al., 2020).

Insider misconduct not only jeopardises the assets of an organisation but also places the very survival of the entity at potential risk (Burch et al., 2021). When delving into the realm of insider threats, it proves advantageous to draw a distinction between malicious threats and non-malicious ones. The key divergence lies in intent, where malicious threats emanate from intentional, deliberate acts (CISA, 2023; Maasberg et al., 2020). A malicious insider purposefully engages in actions with the intent of causing harm to an organisation for personal gain or to address a personal grievance (CISA, 2023). These actions involve a range of threats, including intellectual property theft, fraudulent activities, damage from espionage, acts of terrorism, unauthorised disclosure of national security information, and the potential loss or deterioration of organisational resources or capabilities (Maasberg et al., 2015; Ross et al., 2020). Malicious and intentional insider threats are terms used interchangeably throughout the literature. A non-malicious insider threat also referred to as unintentional threats denote actions or inactions undertaken without any malicious intent. Examples include responding to phishing emails or implementing easily guessable passwords (CISA, 2023).

This paper focuses on intentional insider threats who engage in malicious cybersecurity behaviour.

The Fraud Triangle

The Fraud Triangle, initially developed to identify fraudsters in accounting, has evolved into a versatile framework applied across various disciplines, including cybersecurity (Harrison et al., 2018; Jiang, 2022, Maasberg et al., 2020). This theory posits that fraud arises from a combination of three factors: the motivation to commit fraud, the opportunity to do so, and the ability to rationalise the fraudulent act within one's moral code (Cressey, 1950). Some scholars suggest integrating the Fraud Triangle into a causal model, highlighting the progression from moral awareness to ethical decision-making, thereby enriching the understanding of fraud's psychological underpinnings (Epstein & Ramamoorti, 2016; Harrison et al., 2018). This recommendation reinforces our rationale for integrating the Dark Triad—personalities characterised by a deficiency in moral judgment—as a significant layer of influence on each factor of the Fraud Triangle. The Fraud Triangle theory adopts a comprehensive approach from the employee’s perspective, incorporating both the individual and organisational factors to understand its impact on the intent to commit fraud or in the case of this research malicious inside cybersecurity behaviour (Homer, 2020). A prominent point of the triangle is the incentive to commit fraud (Homer, 2020). Insiders possessing a dark trait may have incentives or be under certain work pressures which serve as motivating factors for them to commit malicious cybersecurity actions within their organisation. The second point is that circumstances exist (Jiang, 2022). Situations arise where employees positioned in roles of trust within an organisation perceive opportunities to act upon unethically (Cressey, 1950). Perceived opportunity is defined as the observation that a vulnerability in a control system exists, coupled with the perception that exploiting this weakness can be done without detection (Homer, 2020). Therefore, a perceived opportunity involves having the capability to conduct this act undetected. In the context of cybersecurity this could be weak access management systems and insufficient monitoring of user activities which create the perceived opportunity for an inside threat. Thirdly, individuals who engage in fraud can rationalise their fraudulent behaviour (Cressey, 1950). There exists individuals who possess character traits, attitudes and sets of ethical values that enable them to consciously and deliberately behave in a dishonest manner (Harrison et al., 2018). Individuals who rank high on the Dark Triad traits very much fall into this category of individual. The theory of the Fraud Triangle posits that the stronger the incentive or pressure, the more readily an individual will justify the acceptability of committing fraud (Cressey, 1950). Furthermore, the greater the perceived opportunity or the heavier the pressure, the less justification is needed to propel someone towards engaging in fraudulent behaviour (Homer, 2020).

The three Dark Triad personality traits are believed to shed light on why certain individuals naturally are, or evolve into malicious agents – those who deliberately look for opportunities to engage in fraudulent activities in a frequently repeated manner (Ramamoorti, 2008).

The Fraud Triangle and Dark Triad: Analysing Cybersecurity Insider Threats

This section delves into the critical interplay between the Fraud Triangle and Dark Triad, exploring their collective impact on malicious insider cybersecurity behaviour. The review emphasises the existing gap of the joint consideration of psychological and situational factors in organisational inside threat risk identification, underscoring the need for an integrated approach. It reveals that while individual Dark Triad traits have been linked to unethical workplace behaviours (Harrison et al., 2018), their combined effect within the Fraud Triangle's framework on cybersecurity threats remains underexplored (Maasberg et al., 2020).

There is a noted dearth on insider research which is argued to be due to organisations either preferring to overlook the problem of inside threats or rather not make it public knowledge so to maintain reputation (Whitty, 2021). Organisations that acknowledge the issue concentrate their efforts on implementing threat detection and prevention technologies and overlook the human element (Whitty, 2021). Once insiders are identified, organisations will typically focus on eliminating the threat (employee) rather than understanding the individual behind the attack and their motives for harming the organisation (Whitty, 2021). This significantly contributes to why managers face challenges in forecasting which employees might become insiders and which specific conditions might precipitate such a transformation (Whitty, 2021). In a study carried out by Whitty (2021), 99 case studies of insider attacks were analysed to elucidate how to identify insiders and pathways to these attacks. Their results outlined the following personality traits typically exhibited by insiders as arrogance, coldness, defensiveness, manipulative, self-centredness, self-deception and risk-taking (Whitty, 2021). All listed traits fall under at least one of the Dark Triad personalities. Another study that similarly details a range of characteristics commonly displayed by an insider included antisocial traits, being above the rules, greed, blaming others and impulsivity (Shaw & Stock, 2011). Once again, these traits match with those of the Dark Triad.

Research on the Big Five personality traits coined by (Digman, 1990)—agreeableness, conscientiousness, extraversion, neuroticism, and openness to experience—have provided key insights into their impact on individuals' susceptibility to security violations and organisational behaviour regarding information security (Burch et al., 2021). However, studies on the influence of the Dark Triad's dark personality traits are still in preliminary stages, especially within the cybersecurity realm (Maasberg et al., 2020). Recent studies emphasise the significance of the Dark Triad personality traits in comprehending workplace behaviour (Burch et al., 2021; Harrison et al., 2018; Maasberg et al., 2020; Sariçïçek, 2023). It is noteworthy that these traits frequently surface in insider threat investigations, even though there are no explicitly designated formal constructs for revealing insider behaviour (Maasberg et al., 2015). To illustrate, insider threat research explores antisocial behaviour to depict malicious insiders in terms of workplace deviance (Maasberg et al., 2020a). In addition to established personality models, researchers have pinpointed a lack of empathy and a sense of entitlement as personality attributes directly pertinent to the risk of insider threats (Maasberg et al., 2015, 2020a). Importantly, these attributes align with all three Dark Triad personality traits, reinforcing their significance in the realm of insider threat research (Jakobowitz & Egan, 2006; Paulhus & Williams, 2002).

The importance of recognising such traits prompts the formulation of a model proposing links between the Fraud Triangle, the Dark Triad traits, and malicious cybersecurity behaviour (Maasberg et al., 2020a; Sariçïçek, 2023, Harrison et al., 2018). Suggesting that individuals with characteristics of the Dark Triad are more prone to engaging in activities that undermine organisational goals (Burch et al., 2021; Harrison et al., 2018; Maasberg et al., 2020). By broadening our understanding of the Dark Triad's impact on fraudulent behaviours we provide a comprehensive perspective for the understanding and identification of malicious behaviour so to enhance cybersecurity measures and minimise insider threats. **Table 1** below, outlines how each of the Dark Triad personality traits influences components of the Fraud Triangle.

The exploration of measures of dark personality traits and malicious intent reveals a sophisticated toolbox, featuring prominent tools like the Short Dark Triad (SD3) and conceptual frameworks such as the Fraud Triangle. The SD3 scale serves as a precise instrument for assessing the Dark Triad traits, offering a structured approach to identify potential propensities toward narcissism, Machiavellianism, and psychopathy (Jones & Paulhus, 2014; Maasberg et al., 2015, 2020; Rauthmann & Kolar, 2012; Sariçïçek, 2023). The Fraud Triangle framework, has been applied empirically across a diverse spectrum of criminal behaviours (Homer, 2020), providing a theoretical lens in this research through which the intricate relationship between Dark Triad personality traits and malicious insider behaviour can be examined and understood.

These measures go beyond simple assessment tools; they serve as the foundational elements for developing a model that highlights the relationships among fraud explanation concepts, the Dark Triad traits, and malicious insider cybersecurity behaviour.

Methodology

Our methodology includes an in-depth validation of the innovative approach we propose, centred on enhancing the Fraud Triangle Framework with the Dark Triad personality traits to improve the understanding and detection of malicious insider threats. To achieve this, we engaged with four experts from distinct yet relevant fields, each chosen for their specialised knowledge and practical experience in aspects critical to our research focus. The selection process was guided by the aim to cover a comprehensive range of perspectives:

- **IT Professional 1:** A seasoned white hat hacker leading internal penetration testing at a major global IT firm emphasised the significant impact of malicious insiders and endorsed the use of psychological profiling, including Dark Triad traits, for effective threat mitigation.

- **IT Professional 2:** A globally recognised white hat hacker from the same corporation acknowledged the presence of malicious mindsets among insiders, underscoring the importance of integrating “dark” personality assessments to improve the detection and prevention of insider threats.

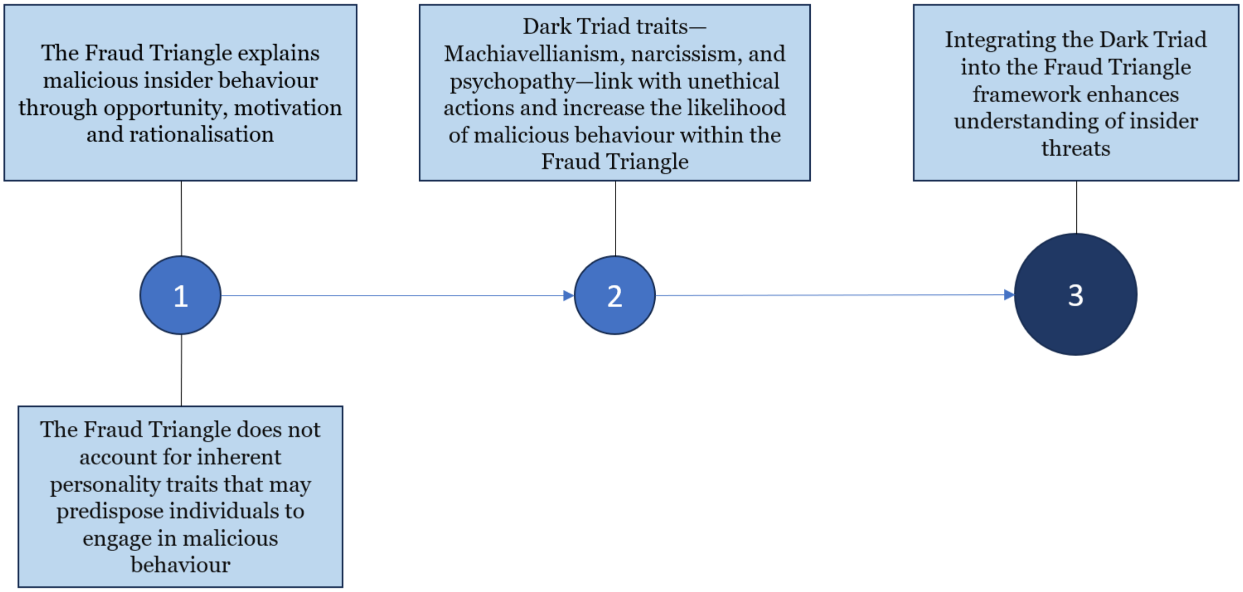
- **Psychologist:** Contributed expertise on the psychological underpinnings of the study, reinforcing the value of psychological profiling, especially in assessing fraudulent risk behavior, for a deeper understanding of insider threats.

- **Criminalist:** Provided criminological insights, validating the integration of criminological theories, particularly the Fraud Triangle, into our study. They concurred that traditional models often overlook personality aspects, a gap our research aims to address by incorporating a personality perspective.

The unanimous agreement among the four experts on the importance of enhancing the Fraud Triangle with Dark Triad personality testing informed our decision to limit expert consultations. Their collective endorsement highlighted the significance of integrating these personality traits into the Fraud Triangle framework, underlining its potential to significantly improve insider threat detection and prevention strategies. This consensus across varied disciplines validates our interdisciplinary approach, reinforcing the importance of this enhanced model in addressing the complexities of insider threats.

Research Argument

The critical thinking and research argument for the formulation of this paper is as follows:



The Fraud Triangle explains malicious insider behaviour through opportunity, motivation and rationalisation

Dark Triad traits—Machiavellianism, narcissism, and psychopathy—link with unethical actions and increase the likelihood of malicious behaviour within the Fraud Triangle

Integrating the Dark Triad into the Fraud Triangle framework enhances understanding of insider threats

The Fraud Triangle does not account for inherent personality traits that may predispose individuals to engage in malicious behaviour

Figure 1: Research argument formulation

Table 1 outlines how each of the Dark Triad personality traits influences components of the Fraud Triangle.

Table 1: The Dark Triad Trait's effects within the Fraud Triangle

Dark Triad Trait	**Effect on Opportunity**	**Effect on Pressure**	**Effect on Rationalisation**	**References**
Machiavellianism	Increases the ability to exploit systemic weaknesses and manipulate situations for personal gain.	May not feel traditional pressures but creates opportunities for gain due to a desire for control and power.	Rationalises fraudulent behaviour as a necessary means to achieve ends, viewing it as part of strategic manipulation.	(Carré et al., 2020; Giammarco & Vernon, 2014; Harrison et al., 2018; Maasberg et al., 2015; Paulhus & Williams, 2002; Rauthmann & Kolar, 2012; Sariçiçek, 2023; Shaw & Stock, 2011.; Whitty, 2021)

Narcissism	Drives the individual to seek positions of power, increasing opportunities for fraud	Pressure is often self-imposed, stemming from a need for admiration and superiority.	Justifies actions through a belief in their superiority and entitlement.	(Carré et al., 2020; Giammarco & Vernon, 2014; Harrison et al., 2018; Maasberg et al., 2015; Paulhus & Williams, 2002; Rauthmann & Kolar, 2012; Sariçiçek, 2023; Shaw & Stock, 2011.; Whitty, 2021)
Psychopathy	Enhances risk-taking behaviours, leading to the exploitation of available opportunities without fear of consequences.	Less affected by external pressures, more by an intrinsic drive for thrill-seeking and immediate gratification.	Views fraudulent acts as acceptable due to a lack of empathy and disregard for societal norms.	(Carré et al., 2020; Giammarco & Vernon, 2014; Harrison et al., 2018; Jones, 2014; Maasberg et al., 2015; & Williams, 2002; Rauthmann & Kolar, 2012; Sariçiçek, 2023; Shaw & Stock, 2011.; Whitty, 2021)

Discussion

The renowned Fraud Triangle whilst foundational as a risk assessment tool for fraudsters has been critiqued as insufficient as it overlooks the aberrant personalities of individuals who are unconcerned with justifying their actions and do not require pressure to act unethically (Epstein & Ramamoorti, 2016). The triangle lacks in personality-based factors as it implicitly presumes a “normal personality type” (Epstein & Ramamoorti, 2016). An average individual may be deterred from fraudulent behaviour with the minimal safeguards of removing opportunities since they would need a compelling motive and a capacity to justify their wrongful actions before engaging in them (Epstein & Ramamoorti, 2016). The socially malevolent personalities of the Dark Triad have no need to rationalise their behaviour, nor do they require a perceived need or an unshakeable burden to engage in malicious behaviour, making it that much more pertinent that these deviant personalities are integrated into the Fraud Triangle (Epstein & Ramamoorti, 2016).

Although there is a recognised correlation between the Dark Triad personality traits and unethical behaviour, research exploring how these traits collectively impact individuals' ethical decision-making remains in its early stages (Harrison et al., 2018). There is scant empirical evidence on how these dark personality traits influence the decision-making processes of individuals who engage in malicious acts, particularly in the cybersecurity domain (Whitty, 2021). Existing studies suggest that individuals scoring high on Dark Triad traits are significantly more prone to committing malicious insider acts when confronted with situational stressors such as motivational triggers, stress, revenge, disgruntlement, entitlement and opportunity (Maasberg et al., 2020; Shaw & Stock, 2011; Whitty, 2021). The theme of Dark Triad traits as potential threats within an organisation emerges prominently in the covered literature exposing the intricate relationship between individual personality characteristics and organisational security vulnerabilities. Acknowledging that "employees are frequently seen as the weakest link in the information security chain" (Maasberg et al., 2020) stresses the pivotal role of human factors in contributing to inside security threats. The research informs how employees, driven by narcissism, Machiavellianism, or psychopathy might exploit their positions for personal gain or engage in intentional cybersecurity violations (Maasberg et al., 2020; Shaw & Stock, 2011; Whitty, 2021). Studies reveal that individuals with Dark Triad personality traits are more prone to committing acts of fraud (Harrison et al., 2018) aligning with the notion that these traits can manifest as insider threats compromising the integrity of organisational cybersecurity (Burch et al., 2021).

Further analysis of the literature revealed that individuals responsible for malicious insider violations displayed Dark Triad traits (Maasberg et al., 2020), with their distinct motivations highlighted by findings that Dark Triad personalities drive employees differently (Burch et al., 2021). This has led researchers to assert that individuals with dark personality traits, particularly psychopaths and Machiavellians, who often exhibit counterproductive work behaviours (Harrison et al., 2018; Maasberg et al., 2020) may pose the most significant security risk. Much attention is drawn to the propensity for individuals with these traits to engage in activities that are detrimental to organisational goals (Burch et al., 2021). Linking this to the studies on fraudulent behaviour found in accountants and employees committing online consumer fraud, it was found that employees who were inclined to commit fraud and those who would be successful in doing so for longer periods showed characteristics belonging to the Dark Triad (Harrison et al., 2018; Sariçïçek, 2023). Additional findings offer noteworthy contributions highlighting the centrality of Dark Triad traits in signalling a shift toward comprehending the psychological dimensions of insider threats (Harrison et al., 2018; Maasberg et al., 2020; Sariçïçek, 2023). Research has delved into specific cases of convicted insider criminals, revealing that all these individuals exhibited distinctive traits associated with dark personalities, with the most prevalent characteristics linked to Machiavellian and psychopathic tendencies (Maasberg et al., 2015, 2020). Research has revealed that individuals exhibiting high psychopathic characteristics are more predisposed to engage in fraudulent activities, as their rationalisation of fraud influences both internal and external motives, shaping their proclivity towards intentional fraudulent behaviours (Sariçïçek, 2023).

Tying all the proposed concepts together it can be posited from the prior research that individuals who rank highly on the Dark Triad of personality traits are more inclined to believe that they possess enhanced opportunities, greater abilities, and stronger motivations to engage in insider malicious cybersecurity behaviour. We can therefore anticipate that such individuals would be more prone to justifying and carrying out malicious acts (Harrison et al., 2018).

From this understanding, it is expected that individuals exhibiting prominent levels of Dark Triad traits are more likely to rationalise and engage in malicious behaviour. Consequently, we introduce our model (**Figure 1**) that posits each of the Dark Triad traits influence the behavioural mechanisms underlying malicious insider cybersecurity actions in distinct ways. This model aims to explore how these personality characteristics affect an individual's propensity towards such malicious actions when faced with each factor of the Fraud Triangle.

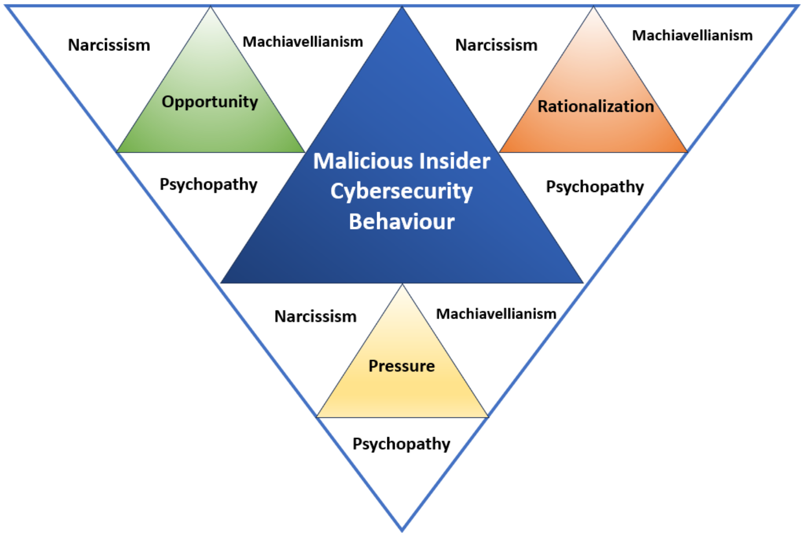


Figure 1: A model of the enhanced Fraud Triad of Dark Triad personalities

By integrating this model into their existing security and human resource (HR) management protocols, organisations can develop targeted interventions aimed at mitigating risks associated with these personality traits. This could include enhanced screening processes during hiring, specialised training programs to foster ethical behaviour, and the implementation of more innovative access control measures that consider an individual's psychological profile. Additionally, the model can guide the development of a comprehensive insider threat program that encompasses continuous monitoring, employee support initiatives, and clear communication of ethical standards, ultimately fostering a security-conscious organisational culture that addresses both technological and human factors in cybersecurity.

Ethics and Legalities

Incorporating Dark Triad personality traits into cybersecurity threat assessments necessitates a judicious approach, balancing organisational security needs against individual privacy rights. Companies employing personality assessments must operate within the framework of privacy laws, employment regulations, and data protection mandates, ensuring tests are relevant, non-discriminatory, and administered under informed consent. Access to test scores is typically restricted to HR personnel and, in certain contexts, management and cybersecurity teams, on a strict need-to-know basis to support team dynamics or insider threat mitigation strategies. The ethical use of these assessments involves strict adherence to confidentiality, transparency about their purpose, and respect for employees' rights, including objections to data use and requests for information deletion. By navigating these legal and ethical considerations carefully, organisations can responsibly leverage psychological insights to enhance their resilience against cybersecurity threats, ensuring a fair and respectful treatment of all employees.

Conclusion and Contribution

In conclusion this study fills a significant gap in academia by exploring malicious cybersecurity insider threats through the lens of the enhanced Fraud Triangle, incorporating the socially malevolent personalities of the Dark Triad. A deep dive into the literature found that individuals prone to malicious insider behaviour frequently display traits of the Dark Triad (Harrison et al., 2018; Shaw & Stock, 2011; Whitty, 2021). Our findings highlight the critical influence of dark personality traits on the propensity for malicious insider cybersecurity violations and advocate for an integrated approach to insider threat prevention that includes psychological insights applied to fraudulent behaviour detection models. To date fraud risk models have been noted to neglect the influence of personalities especially adverse personalities (Epstein & Ramamoorti, 2016). This highlights the necessity for future empirical research to validate and expand upon our model, thereby deepening the understanding of the psychological drivers behind malicious insider behaviour. This paper advocates for a multidisciplinary approach to cybersecurity, urging the integration of technological solutions with a deeper understanding of human behaviour. This approach not only advances the theoretical landscape but also offers practical insights for organisations striving to safeguard against the evolving challenge of insider threats.

Future research should focus on gathering empirical data and employing structural equation modelling (SEM) to clarify the relationships between Dark Triad traits, fraud opportunities, and fraudulent behaviour. This approach will enhance our understanding of how these factors interact and influence one another, offering a deeper insight into the mechanisms driving malicious insider security.

References

BobSulli. (2023, October 14). *Cost Of Insider Risks Global Report—2023 | Ponemon-Sullivan Privacy Report*. https://ponemonsullivanreport.com/2023/10/cost-of-insider-risks-global-report-2023/

Burch, G. F., Batchelor, J. H., Reid, R., Fezzey, T., & Kelley, C. (2021, October 7). The Influence of Employee Personality on Information Security. *ISACA Journal*. Retrieved from https://www.isaca.org/resources/isaca-journal/issues/2021/volume-5/the-influence-of-employee-personality-on-information-security

Carré, J. R., Jones, D. N., & Mueller, S. M. (2020). Perceiving opportunities for legal and illegal profit: Machiavellianism and the Dark Triad. *Personality and Individual Differences, 162*, 109942. https://doi.org/10.1016/j.paid.2020.109942

CISA (2023). Cybersecurity & Infrastructure Security Agency. Defining insider threats. Retrieved from https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threatsCressey, D. R. (1953). Other people's money: A study in the social psychology of embezzlement. Free Press.

Cressey, D. R. (1953). *Other people's money: A study in the social psychology of embezzlement*. Free Press

Digman, J. M. (1990). Personality Structure: Emergence of the Five-Factor Model. *Annual Review of Psychology, 41*(1), 417–440. https://doi.org/10.1146/annurev.ps.41.020190.002221

Epstein, S. R., & Ramamoorti, S. (2016, March 16). Today's fraud risk models lack personality. *The CPA Journal*. Retrieved from https://www.cpajournal.com/2016/03/16/todays-fraud-risk-models-lack-personality/

Giammarco, E., & Vernon, P. (2014). Vengeance and the Dark Triad: The role of empathy and perspective taking in trait forgivingness. *Personality and Individual Differences, 67*, 23–29. https://doi.org/10.1016/j.paid.2014.02.010

Harrison, A., Summers, J., & Mennecke, B. (2018). The effects of the dark triad on unethical behavior. *Journal of Business Ethics, 153*(1), 53–77. https://doi.org/10.1007/s10551-016-3368-3

Homer, E. M. (2020). Testing the fraud triangle: A systematic review. *Journal of Financial Crime, 27*(1), 172–187. https://doi.org/10.1108/JFC-12-2018-0136

Jakobwitz, S., & Egan, V. (2006). The Dark Triad and normal personality traits. *Personality and Individual Differences, 40*(2), 331–339. Retrieved from https://www.researchgate.net/publication/223609325_The_Dark_Triad_and_normal_personality_traits

Jiang, R. (2022). Exploring Employees' Computer Fraud Behaviors using the Fraud Triangle Theory. *Pacific Asia Journal of the Association for Information Systems, 14*, 100–121. https://doi.org/10.17705/1pais.14404

Jones, D. N. (2014). Risk in the face of retribution: Psychopathic individuals persist in financial misbehavior among the Dark Triad. *Personality and Individual Differences, 67*, 109–113. https://doi.org/10.1016/j.paid.2014.01.030

Jones, D. N., & Paulhus, D. L. (2014). Introducing the Short Dark Triad (SD3): A Brief Measure of Dark Personality Traits. *Assessment, 21*(1), 28–41. https://doi.org/10.1177/1073191113514105

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. https://doi.org/10.1145/3408864

Maasberg, M., Warren, J., & Beebe, N. (2015). The Dark Side of the Insider: Detecting the Insider Threat Through Examination of Dark Triad Personality Traits. *2015*. https://doi.org/10.1109/HICSS.2015.423

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. https://doi.org/10.1016/S0092-6566(02)00505-6

Ramamoorti, S. (2008). The Psychology and Sociology of Fraud: Integrating the Behavioral Sciences Component Into Fraud and Forensic Accounting Curricula. *Issues in Accounting Education - Issues Account Educ, 23*. https://doi.org/10.2308/iace.2008.23.4.521

Rauthmann, J., & Kolar, G. P. (2012). How "dark" are the Dark Triad traits? Examining the perceived darkness of narcissism, Machiavellianism, and psychopathy. *Personality and Individual Differences, 53*, 884–889. https://doi.org/10.1016/j.paid.2012.06.020

Ross, R., Pillitteri, V., Dempsey, K., Riddle, M., & Guissanie, G. (2020). Protecting controlled unclassified information in nonfederal systems and organizations (*NIST SP 800-171r2*; p. *NIST SP 800-171r2*). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-171r2

Sariçïçek, R. (2023). The Effect of Dark Personality Traits on The Tendency of Accountants Towards Accounting Fraud. *OPUS Journal of Society Research, 20*(Human Behavior and Social Institutions), Article Human Behavior and Social Institutions. https://doi.org/10.26466/opusjsr.1352064

Shaw, E. D., & Stock, H. V. (2011). Behavioral risk indicators of malicious insider theft of intellectual property: Misreading the writing on the wall (White paper). Symantec. Retrieved from https://www.nationalinsiderthreatsig.org/itrmresources/Behavioral%20Indicators%20For%20Malicious%20Insider%20Theft%20Of%20Intellectual%20Property.pdf

Whitty, M. T. (2021). Developing a conceptual model for insider threat. *Journal of Management & Organization, 27*(5), 911–929. https://doi.org/10.1017/jmo.2018.57