A Theoretical Underpinning for Examining Insider Attacks Leveraging the Fraud Pentagon

Keshnee Padayachee

A Theoretical Underpinning for Examining Insider Attacks leveraging the Fraud Pentagon

Keshnee Padayachee [1][0000-0001-7056-4723]

[1] University of South Africa, College of Science, Engineering and Technology, South Africa
padayk@unisa.ac.za

Abstract. The problem of the insider threat is extremely challenging to manage as it involves trusted entities who have legitimate authorization to the information infrastructure of an organization. It has been reasoned that the framing of the Fraud Pentagon may assist in predicting and preventing white collar crimes such as fraud. The Fraud Pentagon considers the elements of motivation, capability, rationalization, opportunity and arrogance which converge in a crime scenario. The current study considers the value of using the Fraud Pentagon in examining insider attacks. This paper evaluates this theoretical framing from an insider threat perspective, thereby assisting researchers, organizations and information security practitioners in understanding its complexity and its application to the insider threat problem.

Keywords: Insider Threat, Fraud Pentagon, Fraud Triangle, Fraud Diamond

1 Introduction

The insider threat problem is extremely challenging to address as it involves trusted users. A survey of cybersecurity professionals (n=472) found that 90% of organizations feel susceptible to insider attacks [1]. This study is limited to malicious insiders who are users that use their legitimate access to an organization's Information Technology (IT) infrastructure to intentionally compromise the confidentiality, integrity, and availability of the organizations IT assets [2]. Malicious insiders typically respond to deterrents such as reducing motivations and removing opportunities [3]. The elements of motivation and opportunity form the basis of several models proposed to mitigate the insider threat. The Capability-Motivation-Opportunity (CMO) framing [4] is most commonly used toward managing the insider threat [5] while it has been reported that most practitioners use the Fraud Triangle [3] (originally proposed by [6]) which considers the elements of opportunity, motivation and rationalization, to manage the insider threat. The Fraud Diamond extends the Fraud Triangle to include capability [7]. The Fraud Diamond has been explored towards mitigating the insider threat problem [8, 9]. The insider threat problem is considered to be a "moral grey area" as it "allows insiders to undervalue their actions and to resort to rationalizations" [10]. It may be contended that character traits could be a factor in influencing these rationalizations [11]. The Fraud Pentagon is the next evolution in understanding the constructs underpinning fraud, as it extends the Fraud Diamond with the trait of

arrogance – it deals with the "why" element of crime [12]. The aim of this paper is to explore the interaction and the indicators of the elements of motivation, opportunity, rationalization, capability and arrogance on an insider in a criminogenic event.

A strategy to mitigate the insider threat cannot view the aforementioned constructs in isolation. Studies suggest that these constructs are not discrete but may have interdependencies [13-16]. For instance, it has been shown that in some contexts that opportunities combined with occupational status may be a greater driver than motivation and rationalization [17]. Further it has been shown in financial crime, that individuals who are considered predators, do not need the motivation nor the rationalization to engage in maleficence, they merely require the opportunity to be lured into crime [18].

However, there appears to be a dearth of studies that consider the interdependencies between the Fraud Pentagon and the insider threat problem. A related study by [19] who considered internal and external fraud, did not probe the interdependencies as a primary objective. Therefore, this study is a preliminary step in developing a theory for examining the insider attacks based on the vertexes of the Fraud Pentagon. This paper contributes to the cybersecurity domain in two cogent ways. First, the current elucidation will be useful to cybersecurity practitioners and researchers in generating solutions to the insider threat problem. Second, a presentation of the framing of the theoretical underpinning will assist cybersecurity practitioners in leveraging theories from criminology to manage insider threat problems. The rest of the paper is organized as follows – Section 2 presents related work; Section 3 explicates the theoretical framework; Section 4 presents the implications for practice and the paper concludes with Section 5.

2 Related Work

The review of the related work involved a preliminary systematic review which is summarized in Table 1, to identify the prevalence of the models based on fraud theories within insider threat literature.

Table 1. A Preliminary Systematic Review

Database	CMO Model	Fraud Triangle	Fraud Diamond	Fraud Pentagon
IEEE Computer	1	1	1	0
ACM Digital Library	2	0	0	0
Science Direct	3	4	1	0
Google Scholar	37	78	31	3

This involved searching the most specialized databases for cybersecurity, that is, IEEE Computer, Science Direct, ACM Digital Library [20] and searching Google Scholar for additional grey literature. The terms used in the review were constructed using the following criteria: [All: "insider threat"] AND [All: "CMO Model"]; [All:

"insider threat"] AND [All: "fraud triangle"]; [All: "insider threat"] AND [All: "fraud diamond"] AND [All: "insider threat"] AND [All: "fraud pentagon"]. A wider search with more generic search terms may have revealed a greater number of items, however, evidently there is a trend that the Fraud Pentagon has not been given due consideration in cybercrime. A generic search using only the term "fraud pentagon" found 2 unrelated records on Science Direct and 337 records on Google Scholar. A scan of the records found that the Fraud Pentagon is gaining momentum in other fields such as financial fraud and academic fraud.

The CMO model appears to be widely accepted toward managing the insider threat. Greitzer et al. [21] designed an ontology for an insider threat risk model based on the CMO model. Maasberg et al. [22] developed a model that considers the Dark Triad of personality traits based on the CMO model, however, they emphasized that further empirical research is required. Kandias et al. [23] proposed a model, which may be used to predict high-risk insiders based on the CMO model. It appears that the Fraud Triangle is also commonly referenced to manage the insider threat. Hoyer et al. [24] developed an architectural model to unify the fraud triangle to achieve better detection and prevention of the insider threat.

The Fraud Diamond is also commonly referenced in the literature. Goel et al. [9] considered a conceptual model that would provide probes to target the behavioral components of motivation, capability, opportunity, and rationalization in order to detect malicious insider threats. For example, a probe might present a pop-up message indicating "monitoring software is suspended" and the aim is to determine if the insiders will change their search behavior in response to this communication. The model proposed by [8] extended the CMO Model posed by Kandias et al. [23] in four cogent ways by including (1) the element of rationalization (2) prevention (3) contextual information and (4) privacy-preservation.

The Fraud Pentagon that was proposed by [12] and extends the Fraud Triangle with the elements competence and arrogance, is least cited. The paper by Ahmad et al. [19] is most comparable to this research, which considered the effect of digitization as an intervening variable between the elements of the Fraud Pentagon as associated with occupational fraud and external fraud in the telecoms industry. Ahmad et al. [19] reason that technology has helped to reduce some types of fraud by reducing opportunities for crime, however, there is a need to consider a holistic framing that includes organizational culture and processes. This work did not consider the interdependencies of the Fraud Diamond on occupational fraud. Evidently there is a need for more studies to demonstrate the viability of using the Fraud Pentagon for insider threat mitigation.

3 A Theoretical Underpinning for Insider Attacks

Pressure is also considered as the motive/incentive [13] for crime. The classification by Kassem and Higson [25] was extended to include elements that may provoke a motivated insider to commit maleficence [26]. Hence the indicators of pressure are – 1. personal pressure (i.e. financial as caused by gambling or debts); 2. organizational

pressure (i.e. low salaries, unfair treatment, job dissatisfaction, job transfer); 3. external pressure (i.e. threats to financial stability, ego, image, and reputation, social engineering) and 4. provocations (i.e. frustration, stress, disputes, emotional arousal, peer pressure).

Poor security controls and poor management oversight create opportunities for cybercrime [8]. Dellaportas [17] derived indicators suggesting that situations that create opportunities for crime include: lack of controls to prevent and detect maleficence, the ability to bypass controls that prevent and detect maleficence, failure to discipline perpetrators, lack of awareness, indifference, or an incapacity to detect maleficence and the lack of an audit trail.

Insider threats have a proclivity to justify their deeds [3]. Kaptein and Van Helvoort [27] explain that the term neutralization coined by Sykes and Matza [28] was intended to refer to the "justification given before the act instead of the term rationalization that refers to the justification given after the act". Criminals may prepare their rationalizations using a "vocabulary of adjustment" before they act, these verbalizations are intrinsically linked to their motivations for criminality [6]. For an in-depth commentary on the relationship between neutralization techniques and the insider threat, see [29] and [30]. Siponen and Vance [29] proposed a number of neutralization techniques that would be appropriate for the information security domain based on the techniques advanced by Sykes and Matza [28] and Minor [31]. Indicators of neutralization include – "denial of injury"; "defense of necessity"; "condemnation of the condemners" (i.e. attacking those who "disapprove of his/her violations" by denigrating them as "hypocrites" [28]); "appeal to higher authorities" (i.e. disregarding principles of the "larger society for the demands of the smaller social groups" to which the offender belongs [28]); "metaphor of the ledger" [32] (i.e. claiming entitlement to indiscretion as they are mostly good [31]) and "denial of responsibility".

A consideration of the knowledge and skills of insiders to address the insider threat problem [33] should be accorded significance. Capability consists of traits such as knowledge and power; intellect; strong ego; confidence and arrogance; ability to conceal fraud and coerce others [7]. Huff et al. [34] proposed a model for end user sophistication consisting of three facets of capability – breadth (knowledge and skill), depth (background and mastery), and finesse (creativity). However, competence (as designated by the Fraud Pentagon) is a variation of capability as it involves the ability to bypass internal controls, develop a concealment strategy and control social situations via manipulation [35]. To some extent the Fraud Pentagon splits the capability element derived by [7] into competence and arrogance. The distinction of the personality trait of arrogance which effects the ability of the person to see the cost-benefit analysis of crime [7] is highly significant as it underscores the human element in a crime scenario. Maasberg et al. [22] who chronicled the characteristics of insider threats found the following similarities among the cases – "unusual need for attention" a "sense of entitlement/above the rules", arrogance, "compensatory behaviors for self-esteem", "lack of impulse control", "lack of conscience" and "chronic rule violations". Indicators of 'arrogance' (described in [35]) can be detected in individuals with the following characteristics – large ego; suppressive attitude (i.e. a bully) "autocratic management style" and fear of losing power [36]. Further arrogance is

indicated by individuals who assume that they are above controls, policies and regulations and assume they have immunity against them [16].

While the theoretical underpinning of the Fraud Pentagon suggests that all elements converge unilaterally in a crime scenario, studies suggest otherwise. For instance, if an insider is unable to rationalize an act of misconduct, then the misconduct is not considered to be an appropriate opportunity [14]. As the studies within the cybersecurity domain are limited, we will now consider studies from other domains in this discourse.

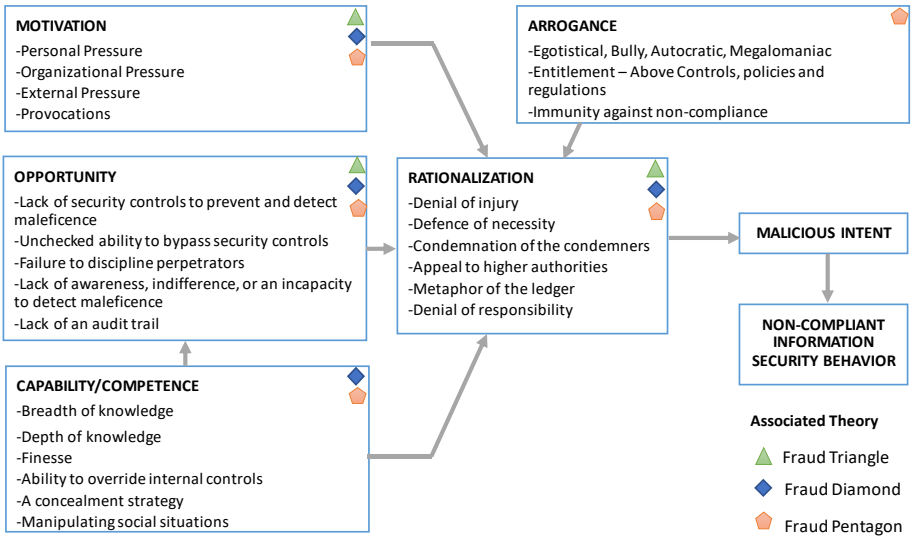

Fig. 1. A Theoretical Underpinning for Examining Insider Attacks

Several studies found that arrogance was not a significant determinant for deviances [36-38]. However, Christian et al. [39] concluded that all five elements including arrogance influenced corporate fraud while [16] found that the work environment acts as an intervening variable between arrogance and unethical behavior in the workplace. The study by Harrison [15] based on the Fraud Diamond showed that the perception of opportunity is positively influenced by capability and that rationalization is influenced by motivation, opportunity and capability leveraging the Theory of Planned Behavior (TPB) [40]. The constructs of TPB considers one's intention in attaining a goal, in this case non-compliant information security behavior. Maasberg et al. [22] also argued for using TPB when considering the relationship between capability, motive and opportunity and the Dark Triad of Traits with respect to the insider threat. Evidently, an individual who is invoking techniques of neutralization (i.e. rationalizations) shows evidence of maladaptive behavior [41], and this suggests that personality is a mediating factor in the process [42]. Thus, arrogance influences the rationalization construct. Appropriating from the propositions of Harrison [15] and Maasberg et al. [22], the theoretical underpinning shows how the elements of the fraud pentagon result in non-compliant information security behavior in Figure 1.

4 Implications for Practice

There is an overlap between cybercrime and white-collar crime as it relates to occupational crime. There is a conceptual overlap between cybercrime as technology is used in the perpetration of white-collar crime [43]. Clearly insider threat crime is subsumed within this definition of white-collar cybercrime. Insider threat crime is characteristically committed within the course of the insider's typical duties at work [2]. The categories of cybercrime that this theoretical framework would have as implications include – insider sabotage (i.e. using an organization's IT infrastructure to cause harm to the organization or an individual); insider theft of intellectual property (IP), insider fraud (i.e. unauthorized modification, addition or deletion of data) [2].

As the insider threat problem shares many similarities with white-collar crime it would be sensible to consider mitigation strategies from well-established criminology theories [44]. For example, several researchers applied the Situation Crime Prevention (SCP) theory [26] to cybercrime ([45-47]). SCP has been applied to the insider threat problem [47, 48]. The theory considers five categories (and 25 subcategories) of opportunity-reducing measures – increase effort, increase risks, reduce rewards, reduce provocations and remove excuses. These techniques were given digital analogies [44-46]. Some of the categories of the SCP theory may be mapped as a mitigation strategy towards curbing the manifestation of the Fraud Pentagon elements.

Some techniques that could be used to increase the effort and thus make an *opportunity less appealing* could be access controls, key splitting [44], segregation of duties [46], background checks [46], offsite storage of data [47], web access controls [44], filtering downloads [46], termination procedures [46], least privilege [44], file access permission [47] and periodic audits [47]. The increase the risks category involves increasing the perception that "the risk of detection, resistance and apprehension associated with maleficence [49] would be high". Techniques that could make an opportunity appear to be less appealing with respect to increasing the risk of being caught include: incident reporting [44], audit trails and event logging [46], a two-person sign-off [46] and resource usage monitoring [45].

The reduce provocations category involves removing "noxious stimuli from the environment" [49] that may precipitate a crime. This category considers situations that act as triggers or precipitators to an individual who is already *motivated* [50]. Strategies that have been suggested to reduce the insider from being provoked into maleficence include – dispute resolution and disciplinary processes [44]. The reduce the rewards category involves reducing the perception that the benefits of the crime [49] would be worthwhile. The reward for crime is a motivating factor. The strategies for reducing the benefit of cybercrime for insider threats include watermarking [45], digital signatures [46], encryption [46] and automatic data destruction mechanisms [45]. These strategies reduce the value of the information asset stolen (i.e. IP theft). Some insiders may gain satisfaction from damaging their employer's reputation (i.e. sabotage). This motivation can be minimized by continuity management [44] and incident management [44] which may reduce the desire for crime. It is challenging to determine the intrinsic forces involved in propelling an insider's motivation. Techniques involving conducting a linguistic analysis of mails [51], collecting information about

computer usage and communication patterns [52] may be used as indicators of a motivated insider.

The remove excuses category involves *suppressing the rationalizations* of a criminal [49]. Therefore the remove excuses category can be used as a mechanism towards neutralization mitigation [49]. These techniques involve – setting rules (i.e. policies and procedures); posting instructions (for example e-mail disclaimers [45]), alerting conscience and assisting compliance.

Capability and arrogance cannot be mitigated, per se. However, these elements may be used to identify high risk individuals (i.e. background checks) who require targeted training. The capability of an insider to do irreparable damage to an organization's IT infrastructure can be diluted by using role-based access controls [53] where an individual's right to information and access is limited to their privileges. Arrogance also negatively impacts top management and it is suggested there should be leadership interventions to coach individuals on the nature of arrogance and its negative impacts [54].

5 Conclusion

The primary contribution of this paper is the propositions generated from the theoretical framing demonstrated that the constructs of the Fraud Pentagon may not act in synergy. This is significant as it would be of importance to determine the numerous permutations of the constructs that need to be mitigated or detected under specific scenarios. An added contribution of this work is the implications for practice which demonstrated how the vertexes of the Fraud Pentagon could be suppressed to overcome the insider threat. Appropriating the arguments from Lokanan [55] which were propositioned with respect to the limitations of the Fraud Triangle, we can extrapolate the following shortcomings of the framing. First, the framing does not consider collusion. Second, the rationalization, arrogance, and motivation legs of the framing are difficult to quantify. Third, not all constructs are present in a criminogenic event. This was also explored by Sorunke [56] who coincidently proposed an alternative Fraud Pentagon which includes a construct of personal ethics instead of arrogance. These shortcomings will be the objective of future research endeavors.

References

1. Cybersecurity Insiders: Insider Threat Report, https://www.cybersecurity-insiders.com/portfolio/insider-threat-report/ (2019), last accessed 2021/05/28.
2. Cappelli, D.M., Moore, A.P., Trzeciak, R.F.: The CERT guide to insider threats: how to prevent, detect, and respond to information technology crimes (Theft, Sabotage, Fraud). Addison-Wesley, Upper Saddle River, New Jersey (2012).
3. Farahmand, F., Spafford, E.H.: Understanding insiders: An analysis of risk-taking behavior. Information Systems Frontiers 15(1), 5–15 (2013).
4. Schultz, E.E.: A framework for understanding and predicting insider attacks. Computers & Security 21(6), 526–31 (2002).

5. Tan, S.-S., Na, J.-C., Duraisamy, S.: Unified psycholinguistic framework: an unobtrusive psychological analysis approach towards insider threat prevention and detection. Journal of Information Science Theory and Practice 7, 52–71 (2019).
6. Cressey, D.R.: Other people's money; a study of the social psychology of embezzlement. Free Press, New York, NY, US (1953).
7. Wolfe, D.T., Hermanson, D.R.: The fraud diamond: Considering the four elements of fraud. The CPA Journal, 38–42 (2004).
8. Mekonnen, S., Padayachee, K., Meshesha, M.: A privacy preserving context-aware insider threat prediction and prevention model predicated on the components of the fraud diamond. In: Annual Global Online Conference on Information and Computer Technology (GOCICT), pp. 60–5. IEEE, Louisville, KY, USA (2015).
9. Goel, S., Williams, K.J., Zavoyskiy, S., Rizzo, N.S.: Using active probes to detect insiders before they steal data. In: 23rd Americas Conference on Information Systems, pp. 1–8. AIS, Boston, Massachusetts (2017).
10. Padayachee, K.: An insider threat neutralisation mitigation model predicated on cognitive dissonance (ITNMCD). South African Computer Journal 56(1), 50–79 (2015).
11. Fagade, T., Tryfonas, T.: Hacking a Bridge: An Exploratory Study of Compliance-based Information Security Management in Banking Organization. In: Callaos, N., Gaile-Sarkane, E., Hashimoto, S., Lace, N., Sánchez, B. (eds.) Proceedings of the 21st World Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI 2017), pp. 94–9. International Institute of Informatics and Systemics, Orlando, Florida, USA (2017).
12. Marks, J.: Fraud Pentagon – Enhancements to the Three Conditions Under Which Fraud May Occur, https://boardandfraud.com/2020/05/21/fraud-pentagon-enhancements-to-the-fraud-triangle-and-under-which-fraud-may-occur/ (2020), last accessed 2021/05/31.
13. Schuchter, A., Levi, M.: The fraud triangle revisited. Security Journal 29(2), 107–21 (2016).
14. Beebe, N.L., Roa, V.S.: Improving organizational information security strategy via meso-level application of situational crime prevention to the risk management process. Communications of the Association for Information Systems 26(1), 329–58 (2010).
15. Harrison, A.J.: The effects of technology on interpersonal fraud. Iowa State University, Ames, Iowa (2014).
16. Analisa: Factors influencing unethical behaviour in banking industry. Journal of Contemporary Accounting 2(2), 97–107 (2020).
17. Dellaportas, S.: Conversations with inmate accountants: Motivation, opportunity and the fraud triangle. Accounting Forum 37(1), 29–39 (2013).
18. Dorminey, J.W., Fleming, A.S., Kranacher, M.-J., Riley, R.A., Jr.: Beyond the Fraud Triangle. The CPA Journal 80(7), 17–23 (2010).
19. Ahmad, A.H., Masri, R., Zeh, C.M., Shamsudin, M.F., Fauzi, R.U.A.: The Impact of Digitalization on Occupational Fraud Opportunity in Telecommunication Industry: A Strategic Review. PalArch's Journal of Archaeology of Egypt/Egyptology 17(9), 1308–26 (2020).
20. Rea-Guaman, A., San Feliu, T., Calvo-Manzano, J., Sanchez-Garcia, I.: Systematic review: Cybersecurity risk taxonomy. In: Mas, A., Mesquida, A., O'Connor, R.V., Rout, T., Dorling, A. (eds.) International Conference on Software Process Improvement, pp. 137–46. Springer, Cham, Switzerland (2017).
21. Greitzer, F., Purl, J., Becker, D., Sticha, P., Leong, Y.M.: Modeling expert judgments of insider threat using ontology structure: Effects of individual indicator threat value and class membership. In: Bui, T.X. (ed.). Proceedings of the 52nd Hawaii International Conference on System Sciences, pp. 3202–11. Grand Wailea, Maui, Hawaii (2019).

22. Maasberg, M., Warren, J., Beebe, N.L.: The dark side of the insider: detecting the insider threat through examination of dark triad personality traits. In: Bui, T.X., Sprague, R.H. (eds.) 48th Hawaii International Conference on System Sciences (HICSS), pp. 3518–26. IEEE, Los Alamitos, California (2015).
23. Kandias, M., Mylonas, A., Virvilis, N., Theoharidou, M., Gritzalis, D.: An insider threat prediction model. In: Katsikas, S., Soriano, M., Lopez, J. (eds.) International Conference on Trust, Privacy and Security in Digital Business, pp. 26–37. Springer, Heidelberg (2010).
24. Hoyer, S., Zakhariya, H., Sandner, T., Breitner, M.H.: Fraud Prediction and the Human Factor: An Approach to Include Human Behavior in an Automated Fraud Audit. In: 45th Hawaii International Conference on System Sciences, pp. 2382–91. IEEE, Maui, Hawaii, USA (2012).
25. Kassem, R., Higson, A.: The new fraud triangle model. Journal of Emerging Trends in Economics and Management Sciences 3(3), 191–5 (2012).
26. Clarke, R.V.: Situational crime prevention: Theory and practice. British Journal of Criminology 20(2), 136–47 (1980).
27. Kaptein, M., Van Helvoort, M.: A model of neutralization techniques. Deviant Behavior 40(10), 1260–85 (2019).
28. Sykes, G.M., Matza, D.: Techniques of neutralization: A theory of delinquency. American sociological review 22(6), 664–70 (1957).
29. Siponen, M., Vance, M.: Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. MIS Quarterly 34(3), 487–502 (2010).
30. Willison, R., Warkentin, M.: Beyond Deterrence: An Expanded View of Employee Computer Abuse. MIS Quarterly 37(1), 1–20 (2013).
31. Minor, W.W.: Techniques of neutralization: A reconceptualization and empirical examination. Journal of Research in Crime and Delinquency 18(2), 295–318 (1981).
32. Klockars, C.: The Professional Fence. Free Press, New York (1974).
33. Magklaras, G.B., Furnell, S.M.: Insider threat prediction tool: Evaluating the probability of IT misuse. Computers & Security 21(1), 62–73 (2002).
34. Huff, S.L., Munro, M.C., Marcolin, B.: Modelling and measuring end user sophistication. In: Lederer, A.L. (ed.). Proceedings of the 1992 ACM SIGCPR conference on Computer personnel research, pp. 1–10. ACM, New York, NY, United States (1992).
35. Marks, J.: The Mind Behind The Fraudsters Crime: key Behavioral and Enviromental Elements, Crowe Holrath LLP (presentation), https://www.fraudconference.com/uploadedFiles/Fraud_Conference/Content/Course-Materials/presentations/23rd/ppt/10C-Jonathan-Marks.pdf (2012), last accessed 2021/05/28.
36. Nindito, M.: Financial statement fraud: Perspective of the Pentagon Fraud model in Indonesia. Academy of Accounting and Financial Studies Journal 22(3), 1–9 (2018).
37. Muhsin, K., Nurkhin, A.: What Determinants of Academic Fraud Behavior? From Fraud Triangle to Fraud Pentagon Perspective. In: International Conference on Economics, Business and Economic Education, pp. 154–67. KnE Social Sciences, Dubai (2018).
38. Evana, E., Metalia, M., Mirfazli, E.: Business Ethics in Providing Financial Statements: The Testing of Fraud Pentagon Theory on the Manufacturing Sector in Indonesia. Business Ethics and Leadership 3(3), 68–77 (2019).
39. Christian, N., Basri, Y., Arafah, W.: Analysis of fraud triangle, fraud diamond and fraud pentagon theory to detecting corporate fraud in Indonesia. The International Journal of Business Management and Technology 3(4), 1–6 (2019).

40. Ajzen, I.: From intentions to actions: A theory of planned behavior. In: Action control, pp. 11–39. Springer, (1985).
41. Padayachee, K.: Joint Effects of Neutralisation Techniques and the Dark Triad of Personality Traits on Gender: An Insider Threat Perspective. In: 2021 Conference on Information Communications Technology and Society (ICTAS), pp. 40–5. IEEE, Durban, South Africa (2021).
42. Simola, P., Virtanen, T., Sartonen, M.: Information Security is More Than Just Policy; It is in Your Personality. In: Cruz, T., Simoes, P. (eds.) ECCWS 2019 18th European Conference on Cyber Warfare and Security, pp. 459–65. Academic Conferences and publishing limited, UK (2019).
43. Payne, B.K.: White-Collar Cybercrime: White-Collar Crime, Cybercrime, or Both. Criminology, Criminal Justice, Law & Society 19(3), 16–32 (2018).
44. Coles-Kemp, L., Theoharidou, M.: Insider Threat and Information Security Management. In: Probst, C.W., Hunker, J., Gollmann, D., Bishop, M. (eds.) Insider Threats in Cyber Security, pp. 45–71. Springer, Boston, MA (2010).
45. Beebe, N.L., Roa, V.S.: Using Situational Crime Prevention theory to explain the effectiveness of Information Systems Security. In: 2005 SoftWars Conference, pp. 1–18. Las Vegas, Nevada (2005).
46. Willison, R.: Understanding the perpetration of employee computer crime in the organisational context. Information and Organization 16(4), 304–24 (2006).
47. Hinduja, S., Kooi, B.: Curtailing cyber and information security vulnerabilities through situational crime prevention. Security Journal 26(4), 383–402 (2013).
48. Willison, R., Siponen, M.: Overcoming the insider: Reducing employee computer crime through situational crime prevention. Communications of the ACM 52(9), 133–7 (2009).
49. Smith, T.R., Scott , J.: Policing and Crime prevention. In: Mackey, D.A., Levan, K. (eds.) Crime prevention, pp. 6–-88. Jones & Bartlett, Burlington, Massachusetts (2011).
50. Cornish, D.B., Clarke, R.V.: Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. Crime Prevention Studies 16, 41–96 (2003).
51. Brown, C.R., Watkins, A., Greitzer, F.L.: Predicting insider threat risks through linguistic analysis of electronic communication. In: 46th Hawaii International Conference on System Sciences, pp. 1849-58. IEEE, Wailea, Maui, Hawaii (2013).
52. Memory, A., Goldberg, H.G., Senator, T.E.: Context-aware insider threat detection. In: Twenty-Seventh AAAI Conference on Artificial Intelligence Workshop, pp. 44–7. Bellevue, Seattle (2013).
53. Sandhu, R.S., Coyne, E.J., Feinstein, H.L., Youman, C.E.: Role-based access control models. Computer 29(2), 38–47 (1996).
54. Toscano, R., Price, G., Scheepers, C.: The impact of CEO arrogance on top management team attitudes. European Business Review 30(6), 630–44 (2018).
55. Lokanan, M.E.: Challenges to the fraud triangle: Questions on its usefulness. Accounting Forum 39(3), 201–24 (2015).
56. Sorunke, O.A.: Personal ethics and fraudster motivation: The missing link in fraud triangle and fraud diamond theories. International Journal of Academic Research in Business and Social Sciences 6(2), 159–65 (2016).