Can security vetting be extended to include the detection of financial misconduct?

Stephan Kühn* and Annamart Nieman

Stephan Kühn has been a security intelligence professional for the past 20 years. He specialised in vetting specifically since 2001. This article was written in partial fulfilment of a master's in Fraud Risk Management at the University of Pretoria (stephankuhn0@gmail.com).

Annamart Nieman is a practising advocate at the Johannesburg Bar. She obtained her doctorate degree in Electronic Evidence in 2006 and lectures on a part-time basis at the Department of Auditing of the University of Pretoria (nieman@law.co.za).

*Correspondence to: Stephan Kühn (stephankuhn0@gmail.com)

Abstract

An analysis of the security vetting files of 19 employees within a South African National Department ("the researched department"), who had been found guilty of financial misconduct in the last five years, uncovered that existing security vetting processes did not detect the financial misconduct of which these employees have been found guilty. This research sets out to establish whether security vetting can be extended to include the detection of financial misconduct within said department and if so, how. Moreover, if security vetting can indeed be so extended, can it possibly enhance the management of fraud risk across all South African public sector departments. Qualitative interviews were conducted with 27 employees, who are key to fraud risk management and security vetting within the researched department. During the interviews, the following 5 themes emerged, were probed and are reported on: (1) the reasons why employees commit financial misconduct and (2) why it is not detected by the security vetting process; (3) the potential alignment of the security vetting process to facilitate the detection of financial misconduct; (4) the following through on security vetting findings, and (5) particularly sharing these findings with

the internal audit and risk management functions within state departments. The research established, firstly, that security vetting can indeed be extended to include the detection of financial misconduct within the researched department, and secondly, that it can enhance the management of fraud risk across all South African public sector departments, given the specific mandate of the State Security Agency ("SSA") and the national security vetting strategy.

Keywords: Security Competence, Vetting, Financial Misconduct, Fraud Risk Management, Risk.

Introduction

Security vetting is increasingly aligned with current and emerging priorities and as a result morphed into much more than what it set out to achieve twenty years ago. In various countries, security vetting is now used not only to determine security competence, but also, to fight fraud, corruption and terrorism, to screen immigrants, and to determine the suitability of candidates for key appointments.

Yet – Tashfeen Malik,[1] the Pakistani woman who along with her husband killed fourteen people in California in 2015 and Edward Snowden,[2] the American National Security Agency ("NSA") contractor who leaked classified information in 2013, seemingly sailed through multiple security vetting interventions. Similarly, and of specific relevance for this article, 19 employees within the researched department and numerous other Tom, Dick and Harries within the South African public sector, despite having undergone security vetting, committed financial misconduct in the workplace.

Why is this? Can security vetting, in fact, be extended to include the detection of financial misconduct in the workplace and if so, how? Moreover, if it can indeed be so extended, can security vetting enhance the management of fraud risk across all South African public sector departments? These are the questions that this research is charged with.

Article 1 of the National Strategic Intelligence Act 39 of 1994 ("the Intelligence Act"), defines a vetting investigation as the prescribed investigation to be followed in determining a person's security competence, which, in turn, is defined as a person's

ability not to compromise classified information (referred to as "security vetting" hereinafter). Security competence is measured against a person's susceptibility to extortion, blackmail and bribes and seeks to assess his or her loyalty to the State and other essential institutions. Security vetting for applicants, and security re-vetting for current employees (collectively referred to as the "security vetting of employees" hereinafter) follow the same methodology: the security vetting process consists of interviews and utilises aids such as record checks, polygraph examinations and interactions with evaluators who must ensure that there are no investigation gaps.[3]

In line with the international trend of extending the application of security vetting for multiple purposes, the South African public service has similarly been required to do so in response to the President's 2012 State of the Nation address, in which he undertook to include initiatives, such as the vetting of personnel working in supply chain management in government departments, in the fight against corruption.[4] This was echoed by the Minister for State Security during his budget vote speech on 26 April 2016. These pronouncements have created an expectation within the public service, and possibly also within the general public, that security vetting would not only determine an official's security competence but would also identify employees with a propensity for financial misconduct.[5]

The State Security Agency ("SSA") is mandated to conduct security vetting throughout the South African Public Service in accordance with article 2A of the Intelligence Act. The South African Police Service ("SAPS") and the South African National Defence Force ("SANDF") are the only two state departments that are currently still responsible for their own security vetting but their approach is in large part aligned to that of the SSA as Cabinet approved a national security vetting strategy in 2006 that is applicable to all state departments.[6] In addition, much progress has been made in reworking the 2006 national security vetting strategy in support of the plan to create a single security vetting agency within South Africa, as also reported on by the Minister for Sate Security during his 2016 budget vote speech.[7] It is accordingly argued that this research, although conducted in respect of one National Department, would have universal application across South African state departments.

In addressing the research questions set out above (i.e. whether security vetting can be extended to include the detection of financial misconduct in the workplace and if so, how), the following four questions were explored:

1. Why are employees committing financial misconduct and why is this not detected by the security vetting process?
2. What questions should be included in the security vetting process that would facilitate the detection of financial misconduct?
3. How should these findings be followed through on?
4. Would it assist efforts to combat financial misconduct if pertinent security vetting findings were to be shared with the internal audit and risk management functions within state departments?

Literature review

What inspires employees to commit financial misconduct? Greed is often the answer, but then again, not all greedy people commit financial misconduct in response to their greedy impulses.[8] A study conducted by Albrecht[9] and colleagues, compared fraud perpetrators, property offenders and college students. They found that fraud perpetrators have more similarities with college students than with property offenders [it is helpful to note that in the Federal Bureau of Investigation's ("FBI's") Uniform Crime Reporting ("UCR") Program, "property crime" includes the offenses of burglary, larceny-theft, motor vehicle theft, and arson].[10] Employees who later perpetrate fraud have the very same characteristics and skills that companies are looking for in employees, and have profiles similar to those of honest people. It is therefore very difficult to predict which employee would turn to financial misconduct.

In line with the above, research conducted by Colwill[11] found that although 70% of fraud is committed by employees, a full 90% of security controls and monitoring effort is focussed on external threats. The Association for Certified Fraud Examiners ("ACFE")[12] uses the 30/40/30 principle, which maintains that 30% of employees are honest all the time, 40% are dishonest all the time, and that the remaining 30% can be swayed to be either honest or dishonest, depending on the circumstances. Employers

should therefore not only appoint honest employees but also keep them honest and identify dishonest employees.

Employers need to continuously monitor employees to identify and anticipate areas of concern.[13] The United Kingdom's Fraud Prevention Service ("CIFAS") highlights vetting, internal corporate culture and the monitoring of employees as the key measures to combat employee fraud effectively.[14] Nixon and Kerr[15] also argue that employers too often ascribe to a false sense of assurance by believing that employees who were honest on the day they were hired, would remain honest throughout their careers. Employees are human and the values, thoughts, beliefs and behaviour of human beings are never cast in stone. People evolve as they are exposed to other people's beliefs and changing situations, which could potentially change their own behaviours and values in turn. In addition, predictions at the point of hiring are not accurate, and vetting can, at best, be an effective way of ensuring a basic level of trust only at a specific point in time. In the absence of accurate foresight, however, vetting has proved to be the best available and most acceptable predictor of future behaviour.[16]

A report published by the Chartered Institute of Management Accountants ("CIMA") in 2008,[17] indicates that no internal control system is completely flawless, and would thus not eliminate all fraud. Focussing on common fraud indicators can, at best, provide an early warning sign that fraud is being perpetrated. Thus, an effective fraud risk management plan focuses on prevention and detection, and includes a response plan to be implemented when fraud is detected. Employees would generally be provided with channels for reporting concerns about fraud and other types of financial misconduct. Typically, these channels include the line managers and/or a hotline. Proactive data analysis can also be conducted to indicate anomalies in financial transactional data that require further investigation. This report did not regard vetting as a fraud detection method.[18] The ACFE's 2016 '*Report to the nations on occupational fraud and abuse*'[19]lists a number of detection methods but, peculiarly, vetting is also not listed as one of them.

This peculiarity is what triggered the researchers' analysis of the security vetting files of 19 employees within the researched department that were found guilty of financial

misconduct (specifically fraud, theft and corruption) in the last five years. The findings from this analysis, in fact, supported the omission of security vetting processes from the list of occupational fraud and abuse detection methods, as it laid bare that existing security vetting processes did not detect the financial misconduct of which these employees have been found guilty. It can accordingly be argued that security vetting, as a measure to detect and identify financial misconduct, is not effective and therefore can also not be listed as a fraud detection method in line with the above reports. This might be attributed to the fact that security vetting focusses primarily on determining someone's security competence.

The incorporation of Donald Cressey's[20] fraud triangle into the security vetting process may contribute to the extension of its application to fraud risk management. The fraud triangle is well known within the fraud risk management environment and is used to explain and study the phenomenon of fraud. The fraud triangle as we know it today consists of three elements, namely pressure or perceived pressure, opportunity and rationalisation. The elements of the fraud triangle are interactive in that the greater the perceived opportunity or the more intense the pressure the less rationalisation it requires for someone to commit fraud. It is also argued that the more dishonest the person is, the smaller the opportunity and/or the pressure it takes to persuade that person to commit fraud.[21]

LaSalle[22] introduced accounting students to the fraud triangle (using an interdisciplinary approach) and achieved positive results. The ability of the accounting students to assess risks improved by the addition of this further dimension to their accounting skills when compared with the efforts of fellow students who had only been exposed to the Committee of Sponsoring Organisations' Internal Control-Integrated Framework. The fraud triangle has now been accepted into international auditing standards, and assists in analysing individual fraudulent behaviour. Similarly, it can be argued that the fraud triangle should also be introduced and used during security vetting investigations.

Opportunities are created or mitigated by companies depending on the insight and ability of management to perceive and understand the pressures and rationalisations that form part of the thought processes of employees, and other less controllable and

predictable influences.[23] Rubasundram[24] argues that the challenge when implementing mitigating processes is that too many controls can cause bureaucratic strangulation, which would cost additional money and time. The cost to develop controls capable of preventing all types of fraud may exceed the benefits, and even the most robust of controls may become ineffective over time.[25] There are also those employees who simply want to see if they can get away with something undetected, and would continue to challenge controls simply because "beating the system" has become a personal challenge.[26]

The pressure component of the fraud triangle can be divided into financial pressure, vice pressure, work related pressure and other pressures.[27] Financial pressure can be subjective, and hence the concept of perceived pressure is preferred in the fraud triangle paradigm. Employees compare themselves with friends, colleagues and neighbours who may appear to be better-off, and this may lead to a desire to be equal or better off in terms of wealth, lifestyle and possessions.[28] Financial pressure is primarily caused by personal insecurity, manifesting as greed, living beyond one's means, high personal debt, medical debt, personal financial loss, and from unexpected financial needs. Vice pressures are caused by drugs, alcohol, gambling and expensive sexual relations.[29] Kassem and Higson[30] state that the term "work-related pressures" refers to the pressure on employees to report results that are better than actual performance, and include the financial interests of management that link bonuses to the achievement of good results.

Domzalski[31] advances that the manner in which employees deal with these pressures would be determined by their personal integrity. Integrity would guide not just the ethical conduct of the employee but also the manner in which he or she would rationalise his or her conduct and decisions. Rationalisation is the process by which fraudsters justify their criminal behaviour. Typically, they would say, "I am just borrowing the money and will pay it back once I win the money back from the casino", or they may nurture the feeling that "the department owes me for all the extra hours I put in." Rationalisations used by perpetrators can include denial of responsibility and this allows them to view themselves as morally responsible individuals being forced to act unethically. They shift the moral responsibility of their

acts to another person, entity, or situation by blaming it on circumstances beyond their control.[32]

According to Silverstone and Sheetz[33] white-collar criminals' have the ability to accommodate both the normal and the awkward simultaneously, without experiencing conflict within themselves. They are able to do this through acts of "mental deftness" which allow them to circumvent behavioural norms that would otherwise result in their perceiving themselves as criminal or deviant.

Fraud perpetrators also argue that their actions do not cause anyone harm and that fraud is a victimless crime. Brown, Esbensen and Geis[34] are of the view that a victimless crime involves consensual participation, which would naturally not be the case when an employer is being defrauded. Large cases of fraud have also lead to companies closing down and many employees losing their jobs. This way of thinking is also present when perpetrators argue that they had to steal to feed their families, or believe that because they stole from the rich and gave to the poor, it does not constitute any crime.[35]

Research conducted by Hollinger and Davis[36] furthermore found empirical support for a correlation between disgruntlement and dishonesty. The rationalisation of these disgruntled employees is that they steal from their employers to resolve their feelings of anger and unfair treatment. Often employees work within an organisation for many years without committing fraud until a trigger factor such as financial problems; changes, resulting in job dissatisfaction; or simply an opportunity to commit fraud presents itself, which then tips the scale towards dishonest behaviour.[37]

Albrecht and colleagues[38] found that employees who commit fraud, rapidly get used to the extra income, and this almost always brings about a change in lifestyle. Very few perpetrators save some of the money that they illegally obtain, and thus the most obvious sign of fraud is an otherwise inexplicably extravagant lifestyle. Perpetrators may thus buy expensive cars, homes, jewellery and clothes, and while fellow employees may notice this they do not ask where the money comes from.

Whilst ongoing security vetting may not necessarily identify red flags such as accounting anomalies (although it could) it would highlight behavioral red flags.[39] The security vetting process can be used to identify pressures and opportunities for rationalisation that might exist in the lives of employees. These red flag situations can then be used for further investigation. Red flags indicate unusual circumstances and actions that stand out from normal activity patterns. It does not mean that there is fraud, but that there may be a need to investigate further.[40]

A common finding emerging from concluded investigations is that the warning signs of changes in employees' attitudes, actions, and behaviours were noticed by colleagues, but not acted on. They either did not realise the situation's significance or did not know where to report it.[41] Despite the recent increase in the number of red flags being raised, many of these are being ignored, which results in missed opportunities to identify fraud.[42] Fellow employees may typically be able to identify these tell-tale signs before a formal security vetting is conducted. Singh and Nayak,[43] in fact, used a 360-degree viewpoint approach when they studied bank fraud in India, where they identified, amongst other fraud indicators, a lack of fraud awareness amongst employees as a significant contributor to the occurrences. The Indian government, after having uncovered numerous cases of espionage, furthermore considered the establishment of a positive vetting cell that employs a 360 degree intense security profiling that includes the assessment and background checks of officials and their family members, before granting them clearance to access top secret files.[44]

Security vetting is, however, costly and labour intensive. The Australian government, for example, reports that about 350 000 employees have an active clearance status, in comparison with the 15 000 clearances issued per year about 15 years ago. The concern is that while not all of these employees are in need of clearance in order to perform their intended tasks, the system seems unable to make the distinction, resulting in exponentially accelerating associated costs.[45] In addition, access to IT systems and databases is critical. Australia's Vetting Agency experienced first-hand the extent to which its IT systems compromises reliability and functionality.[46] It is therefore submitted that security vetting should be a risk-driven process, which should translate into fewer but more effective security vettings being conducted.

To further optimise the return on investment made in doing security vettings, it is sensible to follow a focussed approach by determining beforehand what the desired outcomes of the security vetting process should be. Security vetting criteria should accordingly be in line with the focus or objective of vetting candidates and should be strictly adhered to. France, for example, has updated their vetting criteria after the recent Paris bombings, and their definition of 'suspicious behaviour' now also includes, refusing to work under a female manager. This criterion was reportedly used to withdraw security clearances for 70 employees at French airports last year.[47] The focus of vetting in France, it can be deduced, is in support of counter terrorism efforts, when using this criterion as part of their criteria.

It is also important that the security vetting process should not be predictable to the extent that it limits the return on the investment made. It is with this in mind that the Attorney-General of Australia, for example, requested that "dynamic vetting" be explored – the information about an employee who requires a clearance should be obtained by the security vetting agency, rather than being provided by the employee him or herself.[48]

Research design

The initial analysis of the security vetting files of 19 employees of the researched department, who had been found guilty of financial misconduct in the last five years, uncovered that existing security vetting processes did not detect the financial misconduct of which these employees have been found guilty.

This elicited the research questions that this research is charged with, namely whether security vetting can be extended to include the detection of financial misconduct in the workplace and if so, how. Building on these questions, the focus of this research is whether security vetting can enhance the management of fraud risk across South African public sector departments. Given the specific mandate of the SSA to conduct security vetting throughout the South African Public Service and the reworking of the national security vetting strategy of 2006 in support of the plan to create a single security vetting agency within South Africa, it is argued that the answers to these research questions within the context of the researched department would have

universal application. Therefore, although this case study was conducted within a single national government department, it is probable that the findings would be duplicated if the study were to be replicated in other departments. The findings can accordingly be considered sufficiently robust to contribute positively to the research questions.[49]

Method

Qualitative research was conducted, making use of an exploratory case study, as the intervention being evaluated has no clear or single set of outcomes.[50] Yin[51] advances that the use of a case study is ideal when the envisaged research addresses a descriptive and explanatory question (such as how or why something happened) with the aim to produce a first-hand understanding of people and events. One useful qualitative research method identified by Labuschagne[52] is the use of open-ended interviews that result in the (usually *verbatim*) recording of the respondents' experiences, opinions and knowledge. Open ended questions are exploratory in nature and allow the respondent to provide any answer they identify as appropriate or informative, without forcing the selection of possibly inappropriate or sub-optimally relevant preselected options.[53]

For purposes of this research, and with the intention to provide respondents with an opportunity to consider their answers, four such open-ended questions were sent to the intended respondents prior to the face-to-face interviews. These questions were as follows:

1. Why are employees committing financial misconduct and why is this not detected by the security vetting process?
2. What questions should be included in the security vetting process that would facilitate the detection of financial misconduct?
3. How should these findings be followed through on?
4. Would it assist efforts to combat financial misconduct if pertinent security vetting findings were to be shared with the internal audit and risk management functions within state departments?

The requisite ethical clearance and consent from stakeholders were duly obtained and processed.

Sample

Permission was obtained to interview 27 key employees within the researched department, charged with fraud risk management (including internal audit and risk management) and security vetting (including vetting investigations, polygraph examinations, vetting evaluations and management). An initial group of 15 employees was interviewed, where after further employees were interviewed until a data saturation point was reached, being the point at which no new information was added.

Data collection and analysis

Personal interviews were conducted with the 27 key employees within the researched department and data comprised their responses to the four open ended questions, set out above, which were used to structure and standardise the interviews.

To preserve the anonymity of the 27 employees of the researched department who were interviewed, their responses were identified according to their number in the interview sequence. Data collected from the interviews was then consolidated in one document. The data was analysed qualitatively using a manual process; the use of the computer coding program AtlasTi was investigated but not used due to the manageable extent of the data. Coding was done for each of the four questions which uncovered five themes, as set out below under interview findings.

Data was then categorised under these five themes in accordance with the responses received. Responses unrelated to the questions were initially kept, but later discarded during the categorisation of data. Not all respondents had the same level of understanding of the security vetting process, emphasising in itself the importance of co-operation between the respondents' domains. The findings were submitted to a senior line manager (who was also interviewed) as part of a peer review process.

Results

The findings from the interviews are discussed next under the five primary themes identified during the data coding and analysis phase of the research process.

Theme 1: Reasons for committing financial misconduct:

(a) Financial pressures

Financial pressures were listed by about a third (9) of the respondents as a primary reason why employees might commit financial misconduct. According to these respondents, it is human nature to be opportunistic and greedy, and the pressure to act dishonestly builds as employees gradually take on increasingly onerous financial responsibilities, such as expensive cars, houses and/or simply start living beyond their means. Their lifestyles cannot be supported by their incomes, and their inability to service their debts inevitably leads to stress, which in turn renders them vulnerable when opportunities to commit financial misconduct arise.

It should be borne in mind that employees, when initially appointed, might not have had any criminal intensions, nor shown any desire to get involved in financial misconduct. Security vetting, as currently practiced, would therefore not detect a tendency for financial misconduct because the security vetting process primarily reviews history, and at the specific stage that the security vetting security is conducted, the employee may not have participated in or committed any financial misconduct yet. The decline into financial misconduct might only happen at a later stage due to changes in life circumstances, for example. The security vetting investigator must therefore be attentive to sudden changes in lifestyle and employees' character references should also be specifically questioned on this.

(b) Opportunities to commit financial misconduct

Some of the respondents (3) indicated that ineffective and weak controls within a department, coupled with poor management and a lack of clarity of the duties of employees in respect of these controls, enable financial misconduct. Employees with financial problems are entrusted with, for example money, valuable assets or

information, which present them with opportunities to resolve or better their financial positions, albeit by committing financial misconduct.

(c) Rationalisation of financial misconduct

Some of the respondents (3) listed the ability to rationalise as a significant reason why employees commit financial misconduct. Security vetting cannot pre-emptively detect the intention to commit financial misconduct. It is a slow-growing attitudinal change: employees gradually become disgruntled, they may feel the department does not give them the recognition they deserve and/or that they do not have satisfactory career prospects. As the impulse to commit financial misconduct becomes stronger, these employees may start looking for opportunities.

Dissatisfaction is reportedly being used to rationalise misconduct, and management should identify and resolve these issues timeously. Security vetting investigators must appropriate the requisite attention to the red flags associated with comments such as "I have three children at university", "my wife loves spending money", "I have large house payments that are killing me" and so forth.

Discussion

Financial pressures, coupled with opportunities to commit financial misconduct and the ability to rationalise such misconduct, are cited as the main reasons why employees commit financial misconduct. This accords with the fraud triangle, discussed in the literature review.

Theme 2: Factors hindering security vetting efforts to detect financial misconduct:

(a) Reliance on information supplied by the employee

More than half of the respondents (16) advanced that security vetting does not detect financial misconduct, or associated risk indicators, because the process relies on information supplied by the employee that is subjected to the security vetting process.

Even if the security vetting investigator therefore asks questions relating to financial misconduct, the employee might not divulge the information during the interview. The employee is, in fact, able to lead the security vetting investigation. The security vetting process and interviewers seem to be too dependent on the subject's self-assessment, apparently circumventing an independent assessment and verification of the information provided.

Financial documents should be sourced by the security vetting team and no reliance should automatically be placed on the employee's ability or willingness to provide them with a full set of statements. In addition, three months' bank statements, which is the current norm, are not enough to determine a trend.

Security vetting investigators rely on the references provided by the employee even though such references are highly unlikely to be independent: friends and family members would rarely say negative things about the employee, and these references are also routinely re-interviewed during each security re-vetting cycle. Security vetting investigators must therefore identify their own references, ensuring that they are relevant to the needs of the investigation.

(b) Polygraph questions are not focussed on financial misconduct

More than a third of the respondents (10) stated that polygraph questions are "standard", and that these questions should be aligned in accordance with the purpose of the security vetting process, and also to the particular employee being vetted. The security vetting findings should inform the questions for use during future polygraph testing. The identification of financial misconduct would be more likely if the polygraph interview questions are relevant to or directed at uncovering such misconduct. Instead, questions routinely relate to substance abuse and the leaking of information.

(c) Security vetting investigators are not trained to identify financial misconduct

More than half of the respondents (16) commented that security vetting investigators received insufficient training in the investigation of financial misconduct and simply

do not have sufficient depth of knowledge of associated processes, such as supply chain management. Security vetting investigators would be better positioned to identify indicators of fraud and corruption if they were trained to do so. Indicators of fraud are sometimes present but are overlooked or escape further investigation. This observation made by the respondents was confirmed during the analysis of the security vetting files of the 29 employees within the researched department.

The training of security vetting investigators should also include interviewing skills and investigative techniques, to bring their skills in line with those of the elite investigative units within the SAPS and the office of the Public Protector.

(d) Enforcement of legislation and/or tone from the top

Almost half of the respondents (12) identified a lack of enforcement of legislation within the department and no clear tone from the top as significant contributors to the security vetting process not detecting financial misconduct. Once the findings are presented, little, if anything, is done about it and recommendations are routinely ignored. It appears to be common knowledge that there are "no consequences" for negative security vetting findings. It is the prerogative of the accounting officer to decide how to respond, if at all, to security vetting findings. The consequence is that security vetting is not always taken seriously, as employees know that even negative findings and recommendations are unlikely to affect their careers adversely. Thus, there should be a policy of "no clearance, no entry" to employment in the public service: a valid and vigorously performed clearance should be a condition of employment.

Efforts to address this aspect of the problem could include conducting awareness campaigns in order to inform employees that it is their duty to report financial misconduct and that failure to do so represents, in itself, misconduct. Employees do not always know where to report misconduct. It is suggested that the security vetting investigators and process could be used to report financial misconduct, and that this would provide specific focus to the security vetting of the employee against whom the allegations have been levelled.

(e) Quality versus quantity

A few of the respondents (4) highlighted the fact that the departmental emphasis is on the number of files concluded per month, which makes it virtually impossible to follow up on fraud indicators because of the time constrains dictated by the work load. The pressure on security vetting investigators to adhere to these tight deadlines has a negative impact on the quality of the reports generated. The constant pursuit of higher production has allowed poor quality fieldwork to be submitted by security vetting investigators and is seemingly deemed acceptable by evaluators and management. Quality is thus sacrificed for quantity, as statistics indicating improved throughput impress the powers that be.

(f) The predictability of the security vetting process

About half of the respondents (14) stated that the security vetting process is open to manipulation because it has become an established and standardised routine. Security vetting has been done in an unimaginative and repetitious manner for some time and employees know that. Knowing when the security vetting interviews are due also allows employees to manipulate their financial statements not to attract attention during the security vetting process. Employees acquire loans to prop up their financial positions, but might then experience financial problems soon after the conclusion of the security vetting process.

Security vetting is typically only conducted every five years, regardless of the risks inherent in the specific area where the employee is employed. There should be employee and employment-specific concerns that the security vetting investigator must seek to answer, and this should then inform the selection references to be investigated.

Security vetting should be informed by the risks present both within the department and externally – the failure to contextualise is debilitating to the security vetting process. An organisation’s top management should be clear about the reasons why they call for security vetting at all. These reasons must inform the content and method of the security vetting process

Discussion

The respondents assert that the over-reliance on information supplied by the employee is not conducive to the detection of financial misconduct. Independent sources of information should be sourced by the security vetting investigator. Polygraph questions must be aligned with the purpose of the security vetting and the particular employee and must be based on the security vetting process. These findings are echoed in the literature review with the Attorney-General of Australia calling for "dynamic vetting" and that information about an employee for purposes of security vetting should be sourced by the security vetting agency and not simply requested from the employee him or herself.[54]

The observations made by respondents that indicators of fraud are sometimes present but overlooked or escape further investigation, are confirmed during the analysis of the security vetting files of the 19 employees within the researched department. Security vetting investigators must furthermore receive training in fraud risk management, financial investigations and interviewing techniques. This may enable them to identify financial misconduct, as was the case for the accounting students in LaSalle's[55] study referred to in the literature review. If properly trained, security vetting investigators may furthermore be empowered to customise and prevent the predictability of the security vetting process.

Quality of security vetting is sacrificed for quantity, as statistics indicating improved throughput impress the powers that be. The associated dangers were, however, clearly demonstrated in the Edward Snowden case referred to in the literature review. The United States Investigation Services Incorporated ("USIS") processed hundreds of thousands of cases, many of them poorly, in an attempt to meet company revenue targets: Snowden's was one of them.[56]

Theme 3: Proposed alignments to security vetting interviews to enable the detection of financial misconduct.

(a) Questions focusing on finances

Almost a third of the respondents (7) pointed out that some security vetting investigators do not ask questions that pertain to financial misconduct, at all. To detect or prevent possible financial misconduct, emphasis should be placed on investigating the financial situation of an employee. In addition, it would seem prudent for security vetting investigators to thoroughly analyse and question the details of financial statements provided by employees, and possibly to widen the conversation to include the finances of spouses and partners.

(b) Third party questions

Some of the respondents (4) proposed that the security vetting process should include questions about fellow colleagues, specifically whether the interviewee has ever observed any wrongdoing on their part. If such wrongdoing is raised, details thereof must be pursued. In further support of efforts to improve the rigour of the security vetting process, the references of employees must be asked about their financial lifestyle, and whether they have observed any recent or drastic changes in the lifestyle of the employee.

(c) Lifestyle questions

Almost a quarter of the respondents (10) raised the issue of lifestyle audits and advised that a formal analysis of the financial affairs of employees (including specifically also the income and expense statement), should inform the questions that need to be asked during the security vetting interview. For example, if the expenses exceed the income but apparently without causing financial difficulties, the security vetting investigator should determine the sources of possible additional income. If the additional income cannot be found in the form of legitimate deposits into the employee's bank account, or are not being carried by a spouse or relative, it must be determined how such excess expenses (for example school fees or vehicle finance

agreements) are paid. Databases such as those maintained by the FIC and SARS, and posts and blogs on social media should all be cross-referenced against the stated income of employees. Frequent cash transactions should raise concerns and employees must be questioned about them.

(d) Social media questions

A few of the respondents (5) indicated that social media should be referenced in the security vetting process as these platforms may reveal a great deal about an employee. The use of social media in the security vetting process would also give the security vetting investigator more insight into the character, status, and motivations of the person that they are vetting, and would enable the security vetting process to be more focussed.

(e) The functions performed by the department and the role of the employee must determine the questions

Almost a third of the respondents (8) posited that the security vetting investigator should understand the functions of the department and also the role that the employee plays within the department. Thus if it is, for example, suspected that identity documents are being sold by Home Affairs employees, the security vetting investigator should already know, before the interview, the role that the employee plays regarding the issuance of identity documents. The security vetting investigator should have sufficient familiarity with the system to have some knowledge of how the employee could abuse his or her position to commit financial misconduct. Pertinent questions (also relating to fellow colleagues) include the following examples: “Did someone ever offer you money for an identity document?” or “Do you know if any of your colleagues have ever been offered money for an identity document?” The same type of questions should also inform the polygraph examiner’s preparations. In other words, the vetting planning process should start with the supervisor informing the security vetting investigator about the business processes within the department where security vetting is about to be conducted, even before handing out the specific files. Involving security vetting evaluators at this preparatory stage could also play a

beneficial role in determining what information should be collected by the security vetting investigators.

(f) Work performed outside of the public service

Almost a quarter of the respondents (10) proposed the inclusion of questions addressing possible performance of private work outside of the public service. At present analyses of remunerative work performed outside of the public service are not being done. Security vetting investigators must therefore identify behavioural patterns that might be suggestive of the conduct of undeclared "outside work" by analysing, for example, the employee's movement register (log that captures arrival and departures to and from the office) entries.

A copy of the employee's declaration of financial interest as provided to his or her employer must be obtained and its information verified against the findings of the security vetting investigation. Similarly, any official requests to perform remunerative work outside of the context of his or her employment and any additional income(s) generated as a result thereof, must also be examined and understood.

Discussion

Most respondents in the study, instead of listing specific questions, preferred to indicate where the focus of such questions should be so as to enable the detection of financial misconduct. Questions should revolve around the financial affairs and lifestyle of an employee and should be customised to the role that the employee fulfils within a particular department. Any work performed outside of the department must be investigated. There are numerous questions that can be asked but listing these questions would just create another standard set of questions – with the same risks inherent in the predictability that plagues the current questioning styles and processes. Questions should furthermore be posed to third parties, such as interviewees and fellow employees, who may be best placed to comment on any financial misconduct or apparent lifestyle changes.

The importance of social media checks is now more apparent than ever, as evidenced by Tashfeen Malik, the Pakistani woman referred to in the literature review, who passed three background screening tests when she moved from Pakistan to the USA, and yet her social media posts about jihad were not found.[57]

The Australian government, also referred to in the literature review, called for a more focused approach to security vetting.[58] Security vetting should be a risk-driven process, which should translate into fewer but more effective security vetting investigations being conducted.

Theme 4: Following through on security vetting findings

(a) Action on security vetting findings

About a third of the respondents (8) were of the opinion that security vetting findings are not always implemented in a consistent and transparent manner, and that management permits too many exceptions and decision overrides. Security vetting findings should, in principle, be considered binding and not dismissed as mere recommendations.

Cases of employees suspected of financial misconduct should be handed over to the department's security division for investigation and, when necessary, to the SAPS. Departments should have an anti-corruption policy and strategy in place that includes details on how to report and investigate suspected corruption. Specific processes should be implemented to ensure that red flags that are picked up on during the security vetting processes are monitored and tracked to appropriate outcomes.

Respondents indicated that security clearances should not be issued to employees who have become a liability to a department. Such employees should be demoted or transferred to sections with fewer opportunities for unauthorised conduct. The reasons for denying an employee a security clearance should also be published and communicated to the rest of the department to emphasise the seriousness of the offense, and to sensitise employees to not becoming involved in similar conduct. This

would create awareness of the importance of security vetting within all government departments.

(b) Monitoring/managing negative findings so as to prevent escalation into misconduct

About a quarter of the respondents (10) offered suggestions on how to manage negative findings that are not serious enough to prevent the issuance or withdrawal of a clearance status. It was held that these outcomes should be communicated to the employee and to his or her line management, and must be accompanied by an offer to assist the employee to overcome the problems.

There should, however, be zero tolerance once misconduct has taken place. Every exception creates a precedent. Management in all national departments should be advised that when red flags or risks are uncovered during security vetting processes, similar circumstances should call for more vigilant scrutiny. However, respondents agreed that a distinction should be made between findings affecting an individual employee and findings that have an impact on section- or department-wide organisational systems and procedures.

Where findings identify an individual perpetrator, that employee could be assisted by enrolling him or her in an Employment Assistance Program (EAP). The actions of the more serious offenders, whose actions affect the organisation, should be investigated and analysed by the entity's risk division. Security vetting evaluators should build products that address these trends and security vetting investigators should be informed and empowered to improve the focus and effectiveness of the security vetting process.

The accounting officers (departmental Directors-General) must be made to understand the risks of retaining an employee in the supply chain management area if a security vetting process has found that he or she has, for example, previously accepted bribes and that a clearance can therefore not be issued.

(c) Central database

Almost a third of the respondents (8) proposed that there should be a central database containing all security vetting findings, as this would enrich the security vetting process. Thus, there could be a centrally maintained database at the Department of Public Service, for instance, that contains all security vetting findings and disciplinary records of all employees. Prospective employees must then also be screened against this database as employees do move between departments, sometimes before the conclusion of a disciplinary hearing. Such a database would go a significant way to preventing the re-hiring of high risk misconduct-prone employees.

Discussion

Security vetting finding trends, and the risks associated with these trends, within a department must be managed systemically. The French government, for example, updated their security vetting criteria after the Paris bombings to manage the risks associated with employees refusing to work under a female manager.[59] It can also be deduced from this new criterion that the French government, directs security vetting at countering terrorism.

A central database containing all security vetting findings would enrich the security vetting process. Access to IT systems and databases is critical, as was illustrated in the literature review by referring to Australia's Vetting Agency and the extent to which its IT systems compromises reliability and functionality.[60]

The importance of effective and comprehensive databases is also illustrated by the challenges encountered while attempting to screen Syrian refugees entering the USA. A war-torn country that has limited criminal and terrorist databases against which to check refugee details and immigration authorities are limited to essentially relying on interviews with people that claim to know the refugee, a process that has its own limitations as were highlighted in the literature review.[61]

Theme 5: Sharing security vetting findings with internal audit and risk management

(a) Ensuring the implementation of security vetting recommendations

Some of the respondents (2) said that it would benefit the security vetting process if findings were to be shared with the internal audit and risk management functions, as this would allow for, or trigger, thorough investigations, including possible disciplinary actions and further legal sanction. Both external and internal audit have the authority to follow up on situations where an employee remains in the same position despite not having an appropriate security clearance.

(b) Contributing to the identification of organisational risks

Almost a third of the respondents (8) agreed that communicating security vetting findings to the risk management and audit functions would assist in the identification of operational and organisational risks by enabling the development of risk indicators and controls, which would be tested during audits. Security vetting findings may also be used to determine whether there are ineffective risk controls within the department and in this way, render the audit and risk management functions more pro-active. The findings of the security vetting process can be used to introduce more, and more effective, control measures in ongoing efforts to prevent or eliminate financial misconduct. Furthermore, if employees without clearances are identified in a consolidated database, departments would be enabled to decide whether to employ such a person at all or whether he or she can be transferred to a lower risk function.

(c) *Mitigating risks*

Almost a fifth of the respondents (5) stated that it would assist them if the security vetting findings were promptly communicated to risk management units. This would enable the proactive implementation of mitigating controls throughout the department, thereby reducing opportunities to commit similar acts of financial misconduct. Respondents acknowledged that employees are being corrupted, influenced, and paid

off to override controls. Risk and audit functions should therefore be informed promptly if control measures are not effective or are being overridden.

(d) Symbiotic flowing of information between security vetting, risk and audit functions

About a third of the respondents (8) were of the opinion that security vetting findings should be reported to the internal audit and risk management functions, and that these structures must also provide information to the security vetting structures to inform and focus the security vetting process. As an employee risk management tool, security vetting forms part of the greater risk management tool-chest, hence it would be beneficial to share the results of the security vetting process between all other risk management practitioners. This should strengthen the collective effort of these functions. Considering that financial misconduct appears to mutate and exhibits fluctuating degrees of intensity, it is only through the collaborative efforts of all role players involved in risk management that considerable attempts can be made to successfully combat such financial misconduct.

(e) Identifying risk trends within the department

Almost a third of the respondents (8) highlighted the importance of identifying risk trends within a department. In doing so, the department would be able to see where it is vulnerable and develop internal policies and counter-measures to combat the threats. Security vetting statistics should therefore not just be reported as numbers. Risk management is concerned with trends and findings related to processes which would help to determine if risks are increasing or being sufficiently mitigated. This, in turn, would affect the risk profile of the department, and would alert those conducting the security vetting process to anticipate possible financial problems that so often lead to financial misconduct.

One of the respondents referred to current studies which indicate that we are now living in what is described as the Volatile, Uncertain, Complex and Ambiguous (VUCA) world, characterised by diverse risks that cannot be identified or mitigated by a single profession. Multi-disciplinary efforts are required. Collaboration between

labour relations, departmental ethics task teams, administrative boards and operational divisions would inform a better understanding of a department's risk picture. Such risk picture should be shared by all the stakeholders, including all assurance providers and investigative teams. Respondents indicated that it is important to note that the specific risk being discussed here is "financial misconduct" and that security vetting is just one of the control measures that should be implemented in an effort to minimise or eliminate this risk. Departments should also have other controls in place that should support the entity-wide, combined effort to minimise or eliminate the risk.

Discussion

Security vetting, internal audit and risk management functions should share pertinent findings to support the achievement of better results in the fight against fraud and corruption. This approach is in line with recommendations emerging from the study conducted by Singh and Nayak,[62] that organisations should follow a 360 degree approach by including all employees in the security vetting process. Security vetting is furthermore but one of the risk management tools available. Synergies and the symbiotic flow of information between the security vetting, audit and risk functions would significantly enhance fraud risk management efforts.

Conclusion

The research established, firstly, that security vetting can indeed be extended to include the detection of financial misconduct within the researched department, and secondly, that it can enhance the management of fraud risk across all South African public sector departments, given the specific mandate of the SSA and the imperatives of a South African national security vetting strategy.

In accordance with the fraud triangle, the research established that financial pressures, coupled with opportunities to commit financial misconduct and the ability to rationalise such misconduct, are the main reasons why employees commit financial misconduct.

The research uncovered certain factors which hinder the detection of financial misconduct during the security vetting process. One such factor is the over-reliance on information supplied by the employee. This is not conducive to the detection of financial misconduct and independent sources of information should be sourced by the security vetting investigator. Polygraph questions must also be aligned with both the purpose of the security vetting and the particular employee, and must be directed by the security vetting process. Another such factor hindering the detection of misconduct is the lack of training of security vetting investigators in fraud risk management, financial investigations and interviewing techniques. If properly trained, security vetting investigators may also be empowered to customise and prevent the predictability of the security vetting process. A further factor is the sacrifice of the quality of security vetting for quantity, as statistics indicating improved throughput impress the powers that be. The lack of clarity at organisational top management level about the reasons why security vetting is called for, in the first instance, is another contributing factor. Security vetting must risk-based, focussed and contextualised. Lastly, the lack of enforcement of legislation within the department and no clear tone from the top are further factors which hinder the detection of financial misconduct. Employees should also be made aware of their duty to report financial misconduct.

From the research it emerged that the detection of financial misconduct could possibly be enabled by certain alignments to the security vetting process. Firstly, the focus of questions must be aligned to enable the detection of financial misconduct. However, whilst there are numerous questions that can be asked, listing these would just create another standard set of questions. Questions should revolve around: the financial affairs and lifestyle of an employee; the role of the employee within the particular department; and work performed outside of the department. Secondly, questions should also be posed to third parties, such as interviewees and fellow employees, as these parties may often be best placed to comment on any financial misconduct or apparent lifestyle changes. Thirdly, social media checks are becoming increasingly important and should be pursued. Lastly, a focussed, risk-driven approach should be followed by determining beforehand what the desired outcomes of the security vetting process should be.

From the research it is concluded that security vetting findings must be actioned visibly, consistently and transparently. Cases of financial misconduct must be investigated and not only should employees be appropriately sanctioned, but they should also be seen to be so sanctioned. Red flags picked up on during the security vetting processes must be tracked to appropriate outcomes lest opportunities to identify financial misconduct are missed. Negative findings must be managed, and may have to be managed differently, on an individual and organisational basis. Security vetting finding trends within a department, and the risks associated with these trends must be managed systemically. A central database containing all security vetting findings would enrich the security vetting process.

The research suggested that the sharing of security vetting findings with internal audit and risk management would yield certain positive outcomes in that it would ensure the implementation of such findings by triggering thorough investigations; it would contribute to the identification of organisational risks and risk trends and the mitigation thereof; it would further strengthen the collective pro-active efforts by the security vetting, audit and risk management functions; and it would enhance fraud risk management efforts.

Future Research

It is recommended that this study could be replicated in the private sector. A holistic view of the extended use of security vetting in both the public and private sectors to detect financial misconduct, and the ways in which to do so, would advance the fight against fraud and corruption.

Notes

[1] How did Tashfeen Malik pass 'rigorous' US visa screening?, *Fox News*, 13 December 2015, www.foxnews.com/us/2015/12/13/tashfeen-malik-reportedly-passed-background-checks-despite-questionable-social/?intcmp=hpbt1,(Accessed on 27 May 2016).

[2] US security check company that greenlighted Snowden slapped with $30mn for fraudulent practices, *RT News,* 20 August 2015, www.rt.com/usa/312904-snowden-background-security-firm/, (Accessed on 26 May 2016).

[3] *Intelligence Service Regulations 2014*, Chapter XXVI,www.gov.za/documents/intelligence-service-act-regulations-0,(Accessed on 19 July 2016).

[4] *State of The nation Address 2012*,www.thepresidency.gov.za/pebble.asp?relid=6389,(Accessed on 14 July 2015).

[5] *Budget Vote for Department of State Security 2016,*www.gov.za/speeches/minister-david-mahlobo-state-security-agency-dept-budget-vote-201617-26April-2016-0000,(Accessed on 27 April 2016).

[6] *National Vetting Strategy 2016*, www.dpsa.gov.za/dpsa2g/documents/ep/2007/14_1_1_p_23_11_2007.pdf,(Accessed on 19 July 2016).

[7] *Budget Vote for Department of State Security 2016,*www.gov.za/speeches/minister-david-mahlobo-state-security-agency-dept-budget-vote-201617-26April-2016-0000,(Accessed on 27 April 2016).

[8] JT Wells, Why Employees Commit Fraud, *Journal of Accountancy*, 2001,89, https://o-search.proquest.com.innopac.up.ac. /docview/206773009?pq-origsite=gscholar,(Accessed on 03 February 2016).

[9] WS Albrecht,et al, *Fraud Examination*, 4th ed., South Western Press, 2012, 33-34.

[10] Federal Bureau of Investigation, Uniform Crime Report, Crime in the United States,2014,1, https://ucr.fbi.gov/crime-in-the-u.s/2014/crime-in-the-u.s.-2014/offenses-known-to-law-enforcement/property-crime/property-crime.pdf,(Accessed on 12 October 2016).

[11] C Colwill, Human factors in information security: The insider threat – Who can you trust these days? *Information Security Technical Report*, 2010, 186-187,www.sciencedirect.com,(Accessed on 11 February 2016).

[12] J Pickens, Fraud: The Wolf in Sheep's Clothing, *Arledge and Associates*, 12February 2016, www.jmacpas.com/fraud-the-wolf-in-sheep's-clothing,(Accessed on 19 July 2016).

[13] C Colwill, Human factors in information security: The insider threat – Who can you trust these days? *Information Security Technical Report*, 2010, 191-193, www.sciencedirect.com,(Accessed on 11 February 2016).

[14] CIFAS, Staff fraud and dishonesty Managing and mitigating the risks, Guide, June 2012, 18,www.cipd.co.uk/publicpolicy/policy-reports/staff-fraud-dishonesty.aspa,(Accessed on 10 February 2016).

[15] WB Nixon, and KM Kerr, *Background Screening and Investigations. Managing Hiring Risk From the HR and Security Perspectives,* Elsevier Press, 2008, 134.

[16] FA Colaprete, *Pre-Employment Background Investigations for Public Safety Professionals,* CRC Press, 2012,17.

[17] CIMA, Fraud Risk Management.A Guide to good Practice, 2008,39, http://www.cimaglobal.com/Documents/ImportedDocuments/cid_techguide_fraud_risk_management_feb09.pdf.pdf,(Accessed on 17 March 2016).

[18] KPMG Forensic, Fraud Risk Management. Developing a Strategy for Prevention, Detection and Response, 2006, 6-16,www.KPMG.com,(Accessed on 17 March 2016).

[19] ACFE, Report to the Nations on Occupation Fraud and Abuse, 2016, 23, www.acfe.com/rttn.aspx,(Accessed on 06 April 2016)

[20] Cressey's Fraud Triangle – Part 1: Perceived Pressure, 2011, 2-3,https://learnaboutfraud.wordpress.com/2011/06/29/cresseys-fraud-triangle-part-1-perceived/pressure/(Accessed on 02 October 2015).

[21] WS Albrecht, GW Werns, and TL Williams, *Fraud. Bring Light to the Dark Side of Business*, McGraw-Hill Press, 1995, 20-22.

[22]RE LaSalle, Effects of the fraud triangle on students' risk assessments, *Journal of Accounting Education*, 25:1, 2007, 74-87.

[23] WS Albrecht,et al, *Fraud Examination*, 4th ed., South Western Press, 2012, 103.

[24] GA Rubasundram, Perceived "Tone From The Top" During A Fraud Risk Assessment. *Procedia Economics and Finance*, 2015,106,www.sciencedirect.com, (Accessed on 03 February 2016).

[25] JW Dorminey, et al, Financial Fraud. A New Perspective on an Old Problem, *The CPA Journal, 2012,*65.

[26] Cressey's Fraud Triangle – Part 1: Perceived Pressure, 2011, 2-3,https://learnaboutfraud.wordpress.com/2011/06/29/cresseys-fraud-triangle-part-1-perceived/pressure/(Accessed on 02 October 2015).

[27] WS Albrecht, GW Werns, and TL Williams, *Fraud. Bring Light to the Dark Side of Business*, McGraw-Hill Press, 1995, 20-22.

[28] L Bezuidenhoud, Constructing an Organisational Climate Model to Predict Potential Risk of Management Fraud*,* 2014, 76, http://uir/unisa.ac.za/bitstream/handle/10500/18421/bezuidenhoud_1.pdf?, (Accessed on 02 October 2015).

[29] WS Albrecht, GW Werns, and TL Williams, *Fraud. Bring Light to the Dark Side of Business*, McGraw-Hill Press, 1995, 20-22.

[30] R Kassem and A Higson, The New Fraud Triangle Model, *Journal of Emerging Trends in Economics and Management Sciences,* 2012,192,(Accessed on 04 October 2015).

[31] PT Domzalski, Cooking the Fraud Triangle: A Recipe for Disaster, 2009,3, www.financialexecutives.org/eweb/upload/chapter/Philadelphia/Cooking%20the%20Fraud%20Triangle%20-%20A%20Recipe%20for%20Disaster.pdf,(Accessed on 02 October 2015).

[32] S Dellaportas, Conversations with inmate accountants: Motivation, opportunity and the fraud triangle. *Accounting Forum,* .37,:1, 2013,32.

[33] H Silverstone and M Sheets, *Forensic Accounting and Fraud Investigation for Non-Experts,* Wiley Press, 2004, 30.

[34] SE Brown, F Esbensen and G Geis, *Criminology.Explaining Crime and Its Context*, Elsevier Press, 2013,572.

[35] LJ Siegel*, Criminology,* Thomson Wadsworth Press, 2003, 402.

[36] RC Hollinger, and JL Davis, *Employee Theft and Staff Dishonesty.The Security Handbook,* New York: Palgrave Macmillan Press, 2003, 212.

[37] KPMG, Who is the typical fraudster, 2011,3, www.KPMG.com.(Accessed on 17 Ferbruary 2016).

[38] WS Albrecht,et al, *Fraud Examination*, 4th ed., South Western Press, 2012, 148, 152.

[39] M Kranacher, RA Riley and JT Wells, *Forensic Accounting and Fraud Examination,* Wiley Press, 2011, 193.

[40] S Padgett, *Profiling the Frauddster.Removing the Mask to Prevent and Detect Fraud*. Wiley Press, 2015,73.

[41] C Colwill, Human factors in information security: The insider threat – Who can you trust these days? *Information Security Technical Report*, 2010, 186-187, www.sciencedirect.com,(Accessed on 11 February 2016).

[42] KPMG, Who is the typical fraudster, 2011,12, www.KPMG.com.(Accessed on 17 Ferbruary 2016).

[43] T Singh and S Nayak, Frauds in Banking Corporate Governance Issues. CCS Project Report, 2015,1-4, http://tejas.iimb.ac.in/articles/Banking%20Frauds_Tejas_Jan2016.pdf,(Accessed on 10 April 2016).

[44] Y Yadav, Fear of moles prompts vetting of Babus. *New Indian Express*, 24 March 2013, www.newindianexpress.com/nation/article1514585.ece,(Accessed on 26 May 2016).

[45] M Mannheim, Secret state: costly government security clearances 'spiralling out of control', *Canberra Times*, 23 June 2014,www.canberratimes.com.au/national/public-service/secret-state-costly-government-security-clearances-spiralling-out-of-control-20140617-zsapb.html,(Accessed on 30 May 2016).

[46] R Pearce, Govt security vetting systems still unreliable despite costly upgrades. IT systems hinder government security vetting, *Computerworld*,10 June 2015, www.computerworld.com.au/article/577077/govt-security-vetting-systems-still-unreliable-despite-costly-upgrades/, (Accessed on 25 May 2016).

[47] L Dearden, Paris attacks: 70 staff have security clearance revoked for suspected 'radicalisation' at French airports, *Independent News,* 15 December 2015,

www.independent.co.uk/news/world/europe/paris-attacks-70-staff-have-security-clearance-revoked-for-suspected-radicalisation-at-french-a6773691.html, (Accessed on 24 May 2016).

[48] A Coyne, Brandis boosts vetting of APS staff to prevent insider threats, *IT News*, 02 September 2014, www.itnews.com.au/news/brandis-boosts-vetting-of-aps-staff-to-prevent-insider-threats-391656, (Accessed on 30 May 2016).

[49] J Gerring, What is a Case Study and What Is It Good for?, *American Political Science Review*,98:2, 2004,342,www.jstor.org/stable4145316,(Accessed on 16 March 2016).

[50] P Baxter, and S Jack, Qualitative Case Study Methodology: Study and Implementation for Novice Researchers. The Qualitative Report, 13:4, 2008, 548, http://nsuworks.nova.edu/tqr/vol13/iss4/2. (Accessed on 16 March 2016).

[51] RK Yin, Case Study Methods. 2004, 2-3, www.cosmoscorp.com/Docs/AREAdraft.pdf. (Accessed on 08 April 2016).

[52] A Labuschagne, The Qualitative Report, 8:1, 2003,http://www.nova.edu/sss/QR/QR/8-1/labuschagne.html, (Accessed on 10 April 2016).

[53] Fluid Surveys, Comparing Close Ended and Open Ended Questions, 2013,http://fluidsurveys.com/university/comparing-closed-ended-and-open-ended-questions/, (Accessed on 10 April 2016).

[54] A Coyne, Brandis boosts vetting of APS staff to prevent insider threats, *IT News*, 02 September 2014, www.itnews.com.au/news/brandis-boosts-vetting-of-aps-staff-to-prevent-insider-threats-391656, (Accessed on 30 May 2016).

[55]RE LaSalle, Effects of the fraud triangle on students' risk assessments, *Journal of Accounting Education*, 25:1, 2007, 74-87.

[56] US security check company that greenlighted Snowden slapped with $30mn for fraudulent practices, *RT News,* 20 August 2015, www.rt.com/usa/312904-snowden-background-security-firm/, (Accessed on 26 May 2016).

[57] How did Tashfeen Malik pass 'rigorous' US visa screening?, *Fox News*, 13 December 2015, www.foxnews.com/us/2015/12/13/tashfeen-malik-reportedly-passed-background-checks-despite-questionable-social/?intcmp=hpbt1,(Accessed on 27 May 2016).

[58] M Mannheim, Secret state: costly government security clearances 'spiralling out of control', *Canberra Times*, 23 June 2014,www.canberratimes.com.au/national/public-service/secret-state-costly-government-security-clearances-spiralling-out-of-control-20140617-zsapb.html,(Accessed on 30 May 2016).

[59] L Dearden, Paris attacks: 70 staff have security clearance revoked for suspected 'radicalisation' at French airports, *Independent News,* 15 December 2015, www.independent.co.uk/news/world/europe/paris-attacks-70-staff-have-security-clearance-revoked-for-suspected-radicalisation-at-french-a6773691.html, (Accessed on 24 May 2016).

[60] R Pearce, Govt security vetting systems still unreliable despite costly upgrades. IT systems hinder government security vetting, *Computerworld*,10 June 2015, www.computerworld.com.au/article/577077/govt-security-vetting-systems-still-unreliable-despite-costly-upgrades/, (Accessed on 25 May 2016).

[61] J Markon, Senior Obama officials have warned of challenges in screening refugees from Syria. *Washington Post*, 17 November 2015, www.washingtonpost.com/news/federal-eye/wp/2015/11/17/senior-obama-officials-have-warned-of-challenges-in-screening-refugees-from-syria/,(Accessed on 26 May 2016).

[62] T Singh and S Nayak, Frauds in Banking Corporate Governance Issues. CCS Project Report, 2015,1-4, http://tejas.iimb.ac.in/articles/Banking%20Frauds_Tejas_Jan2016.pdf,(Accessed on 10 April 2016).

Bibliography

Albrecht, W. Steve, Chad O. Albrecht, Conan C. Albrecht, and Mark F. Zimbelman. Fraud Examination. 4th ed. Mason, OH: South-Western, 2012.

Albrecht, W. Steve, Gerald W. Werns, and Timothy L. Williams. Fraud: Bringing Light to the Dark Side of Business. Burr Ridge, IL: Irwin Professional, 1995.

Association of Certified Fraud Examiners. Report to the Nations on Occupation Fraud and Abuse: 2016 Global Fraud Study. Austin, TX: ACFE, 2016.

Baxter, Pamela, and Susan Jack. 'Qualitative Case Study Methodology: Study and Implementation for Novice Researchers'. The Qualitative Report 13, no. 4 (2008): 544–559. http://nsuworks.nova.edu/tqr/vol13/iss4/2

Bezuidenhoud, Leon. 'Constructing an Organisational Climate Model to Predict Potential Risk of Management Fraud'. PhD diss., University of South Africa, 2014.

Brown, Stephen E., Finn-Aage Esbensen, and Gilbert Geis. Criminology: Explaining Crime and Its Context. Waltham, MA: Anderson, 2013.

Chartered Institute of Management Accountants. Fraud Risk Management: A Guide to Good Practice. London: CIMA, 2009.

CIFAS, and Chartered Institute of Personnel and Development. Tackling Staff Fraud and Dishonesty: Managing and Mitigating the Risks. London: CIFAS, 2012.

Colaprete, Frank A. Pre-Employment Background Investigations for Public Safety Professionals. Boca Raton, FL: CRC Press, 2012.

Colwill, Carl. 'Human Factors in Information Security: The Insider Threat – Who Can You Trust These Days?' Information Security Technical Report 14, no. 4 (2010): 186–196. doi:10.1016/j.istr.2010.04.004

Coyne, Allie. 2014. 'Brandis Boosts Vetting of APS Staff to Prevent Insider Threats'. IT News, 02 September. https://www.itnews.com.au/news/brandis-boosts-vetting-of-aps-staff-to-prevent-insider-threats-391656

Dearden, Lizzie. 2015. 'Paris Attacks: 70 Staff Have Security Clearance Revoked for Suspected "Radicalisation" at French Airports'. Independent News, 15 December. http://www.independent.co.uk/news/world/europe/paris-attacks-70-staff-have-security-clearance-revoked-for-suspected-radicalisationat-french-a6773691.html

Dellaportas, Steven. 'Conversations with Inmate Accountants: Motivation, Opportunity and the Fraud Triangle'. Accounting Forum 37, no. 1 (2013): 29–39. doi:10.1016/j.accfor.2012.09.003

Domzalski, Patricia T., and R. S. M. McGladrey. 'Financial Executives International: Philadelphia Newsletter'. Cooking the Fraud Triangle: A Recipe for Disaster. February 2009.

Dorminey, Jack W., Aaron Scott Fleming, Mary-Jo Kranacher, and Richard A. Riley. 'Financial Fraud: A New Perspective on an Old Problem'. The CPA Journal 82, no. 6 (2012):

61–65. https://www.nysscpa.org/news/publications/the-cpa-journal/article-preview?ArticleID=11063

Federal Bureau of Investigation. Uniform Crime Report: Crime in the United States, 2014 – Property Crime.

Federal Bureau of Investigation. https://ucr.fbi.gov/crime-in-the-u.s/2014/crime-in-the-u.s.-2014/offenses-known-to-law-enforcement/property-crime/property-crime.pdf

FluidSurveys. 'Comparing Closed-Ended and Open-Ended Questions'. FluidSurveys. http://fluidsurveys.com/university/comparing-closed-ended-and-open-ended-questions/

Gerring, John. 'What Is a Case Study and What Is It Good For?' American Political Science Review 98, no. 2 (2004): 341–354. doi:10.1017/S0003055404001182

Hollinger, Richard C., and Jason L. Davis. 'Employee Theft and Staff Dishonesty'. In The Security Handbook, edited by Martin Gill, 203–228. 1st ed. New York, NY: Palgrave Macmillan, 2003.

Kaiser, Tom. 2011. 'Cressey's Fraud Triangle – Part 1: Perceived Pressure'. Learnaboutfraud, 29 June. https://learnaboutfraud.wordpress.com/2011/06/29/cresseys-fraud-triangle-part-1-perceived/pressure/

Kassem, Rasha, and Andrew Higson. 'The New Fraud Triangle Model'. Journal of Emerging Trends in Economics and Management Sciences 3, no. 3 (2012): 191–195. http://jetems.scholarlinkresearch.com/abstractview.php?id=558

KPMG. Fraud Risk Management: Developing a Strategy for Prevention, Detection and Response. Amstelveen: KPMG, 2014.

KPMG. Who Is the Typical Fraudster? KPMG Analysis of Global Patterns of Fraud. Amstelveen: KPMG, 2011.

Kranacher, Mary-Jo, Richard A. Riley, Jr., and Joseph T. Wells. Forensic Accounting and Fraud Examination. Hoboken, NJ: John Wiley & Sons, 2011.

Labuschagne, Adri. 'Qualitative Research – Airy Fairy or Fundamental?' The Qualitative Report 8, no. 1 (2003): 100–103. http://nsuworks.nova.edu/tqr/vol8/iss1/7/

LaSalle, Randall E. 'Effects of the Fraud Triangle on Students' Risk Assessments'. Journal of Accounting Education 25, no. 1 (2007): 74–87. doi:10.1016/j.jaccedu.2007.03.002

Mahlobo, David. 'Minister David Mahlobo: State Security Agency Dept Budget Vote 2016/17'. Republic of South Africa. http://www.gov.za/speeches/minister-david-mahlobo-state-security-agency-dept-budgetvote-201617-26-apr-2016-0000

Mannheim, Markus. 2014. 'Secret State: Costly Government Security Clearances "Spiralling out of Control"'. Canberra Times, 23 June. http://www.canberratimes.com.au/national/public-service/secretstate-costly-government-security-clearances-spiralling-out-of-control-20140617-zsapb.html

Markon, Jerry. 2015. 'Senior Obama Officials Have Warned of Challenges in Screening Refugees from Syria'. Washington Post, 17 November.

http://www.washingtonpost.com/news/federal-eye/wp/2015/11/17/senior-obama-officials-have-warned-of-challenges-in-screening-refugees-from-syria/

Nixon, W. Barry, and Kim M. Kerr. Background Screening and Investigations: Managing Hiring Risk from the HR and Security Perspectives. Burlington, MA: Butterworth-Heinemann, 2008.

Padgett, Simon. Profiling the Fraudster: Removing the Mask to Prevent and Detect Fraud. Hoboken, NJ: John Wiley & Sons, 2015.

Pearce, Rohan. 2015. 'Govt Security Vetting Systems Still Unreliable Despite Costly Upgrades'. Computerworld, 10 June. http://www.computerworld.com.au/article/577077/govt-security-vettingsystems-still-unreliable-despite-costly-upgrades/

Pickens, John. 2016. 'Fraud: The Wolf in Sheep's Clothing'. Arledge & Associates, 12 February. http://www.jmacpas.com/fraud-the-wolf-in-sheep's-clothing

Republic of South Africa. National Strategic Intelligence Act, No. 39 of 1994. Cape Town: Government Gazette.

Republic of South Africa. 'Intelligence Service Regulations 2014'. Pretoria: Republic of South Africa, 2014.

Republic of South Africa. National Vetting Strategy 2016. Pretoria: Republic of South Africa, 2016.

Rubasundram, Geetha A. 'Perceived "Tone from the Top" during a Fraud Risk Assessment'. Procedia Economics and Finance 28 (2015): 102–106. doi:10.1016/S2212-5671(15)01087-4

Siegel Larry J. Criminology. Thomson Wadsworth Press, 2003.

Silverstone, Howard, and Michael Sheets. Forensic Accounting and Fraud Investigation for Non-Experts. 1st ed. Hoboken, NJ: John Wiley & Sons, 2004.

Singh, Tamanna, and Siddharth Nayak. Frauds in Banking: Corporate Governance Issues. Meerut: Chaudhary Charan Singh University, 2015.

'Tashfeen Malik Reportedly Passed Background Checks Despite Questionable Social Media Posts'. 2015.Fox News, 13 December. http://www.foxnews.com/us/2015/12/13/tashfeen-malik-reportedly-passedbackground-checks-despite-questionable-social/?intcmp=hpbt1

'US Security Check Company that Greenlighted Snowden Slapped with $30mn for Fraudulent Practices'. 2015. RT, 20 August. http://www.rt.com/usa/312904-snowden-background-security-firm/

Wells, Joseph T. 'Why Employees Commit Fraud'. Journal of Accountancy, February (2001). http://www.journalofaccountancy.com/issues/2001/feb/whyemployeescommitfraud.html
Yadav, Yatish. 2013. 'Fear of Moles Prompts Vetting of Babus'. New Indian Express, 24 March. http://www.newindianexpress.com/nation/2013/mar/24/fear-of-moles-prompts-vetting-of-babus-461449.html

Yin, Robert K. Case Study Research: Design and Methods. 3rd ed. Thousand Oaks, CA: 2003.

Zuma, Jacob. ‘State of the Nation Address 2012’. Speech given to the Parliament of the Republic of South Africa, Cape Town, 9 February 2012.