Journal of Management & Organization (2021), **27**, 911–929
doi:10.1017/jmo.2018.57

RESEARCH ARTICLE

Developing a conceptual model for insider threat

Monica T Whitty[1,2]*

[1]Department of Media and Communication, University of Melbourne, Melbourne, VIC, Australia and [2]WMG, Cyber Security Centre, University of Warwick, Coventry, UK
*Corresponding author: monica.whitty@unimelb.edu.au

(Received 29 October 2017; revised 13 August 2018; accepted 16 August 2018; first published online 13 November 2018)

Abstract
This paper sets out 99 case studies of insider attacks that took place in the UK. The study involved interviewing investigators, heads of security, information technologists, law enforcement, security officers, human resource managers, line managers, and coworkers who knew the insider. The analysis elucidates how to identify insiders and pathways to these attacks. It also highlights examples of archetypal insiders, in addition to the 'disgruntled employee' (e.g., 'the show off', 'the career criminal', 'the addict', etc.). In contrast to other studies, this study highlights multiple pathways to an attack. A conceptual model is set out that considers indicators (both physical and cyber) that might be monitored in an insider risk detection programme. The model stressors need to continuously seek out methods to close down opportunities as well as to monitor behavioural change. It also elucidates potential deterrence and prevention strategies for organisations to consider in an ethical and legal manner.

Keywords: insider threat; security; cyber security; grounded theory; crime prevention; crime detection

An insider can be anyone working within a central government department or a commercial organisation that *intentionally* exploits or intends to exploit his/her legitimate access to an organisation's assets for unauthorised purposes. Examples include theft (intellectual property [IP], company secrets, money, data), fraud, terrorism, reputation damage, blackmail, denial of service attacks, introduction of viruses, worms, Trojan horses, corruption or deletion of data, altering data, and password cracking (Cappelli, Moore, & Trzeciak, 2012; Nurse et al., 2014). An insider is also often understood to be those whose actions cause harm to an organisation through accident (e.g., accidentally downloading malware onto an organisation's equipment). There is a dearth of research on insiders, which is mostly because organisations often prefer to ignore the problem or, at least, do not publicly admit they have a problem so as to avoid reputational damage (Randazzo, Kenney, Kowalski, Cappelli, & Moore, 2005). Moreover, often when an insider is identified, organisations are more concerned with removing the threat (employee) than learning about the person who caused the attack and their reasons for causing harm to the organisation. The available research has mainly focussed on fraud (e.g., Gill, 2007; Schuchter & Levi, 2016) or the accidental insider (e.g., Magklaras & Furnell, 2001; Ophoff, Jensen, Sanderson-Smith, Porter, & Johnston, 2014). The focus of this paper is on intentional insiders, in general, who act maliciously, either for his/her own purposes or on behalf of some other party.

At present, managers have difficulties predicting who might be an insider within their organisations and the conditions (external or internal) which might turn an employee into an insider. Gaining greater insights into the typology of an insider and their pathways to criminality is, therefore, crucial if we are to identify more effective methods to deter, detect, and prevent these types of attacks on organisations. This paper specifically examines, via the analysis of case studies on a range of insider attacks: (a) how to identify potential insiders and (b) pathways to these attacks. The findings are used to develop a conceptual model that could assist with human and automatic detection as well as prevention of insider attacks.

Background

The harm that insiders might cause an organisation is not a trivial matter. It has been argued that insiders continue to pose threats to organisations, often equal to or greater in volume to outside threats (CERT Program (Carnegie Mellon University) and Deloitte, 2011; Richardson, 2011; Kroll, 2015). Kroll, for example, reports that in 2015, of the companies they surveyed that experienced fraud where the perpetrator was known, 81% involved at least one insider (which they point out was a 72% increase from their previous survey). The report also notes that in spite of these figures, organisations' concerns about insider issues are relatively low. Those organisations that do recognise the problem often take a more technical approach to detect and prevent, often neglecting the 'human element' (Legg et al., 2013). There has been some research outlining the typology of an 'insider'; however, this research is considerably limited and as the earlier literature review highlights, it is difficult to predict or identify insiders from current empirical research. In addition, current literature provides few recommendations on how to change workplace conditions or vet employers to prevent insider attacks on their organisations.

Demographic indicators

According to the available research, insiders are more likely to be men between the ages of 20 and 45 years (Shaw & Stock, 2011; CIFAS, 2012; CPNI, 2013). Centre for the Protection of the National Infrastructure (CPNI, 2013) examined 120 insider cases and identified that males were more frequently insider attackers (82%) than females (18%), they tended to be between 31 and 45 years old (49%), usually full-time permanent staff (88%), with customer-facing (20%), financial (11%), and security staff (11%) posing the most prominent risk. Threat episodes ranged from <6 months (41%) to >5 years (11%) and 60% of insiders had worked for the company for <5 years. The types of roles insiders were employed in appeared evenly split between managerial (45%) and nonmanagerial positions (49%), with higher prevalence among university graduates (58%).

With respect to insiders who commit fraud, Credit Industry Fraud Avoidance System, in the UK, maintains an 'internal fraud database' and members of Credit Industry Fraud Avoidance System can report the details about insider attacks that involve fraud. They reported that the average age for an insider is 30 years, with the majority between the ages of 21 and 30 years. They believe that the proportion of men and women who commit fraud in organisations is a 60:40 split (which is about the same as the working population).

With respect to IP theft, Shaw and Stock (2011), in a summary of the literature, found that male employees, with an average age of 37 years, who are employed in technical positions, commit the majority of IP theft. They also found that about 65% of employees who commit insider IP theft had already accepted a new job and that those who commit this crime typically steal using the authorisation privileges they had been given access to in the job. Although the above findings need to be treated with caution, they do suggest that the monitoring of potential insiders based on demographic data alone would be: (a) too resource intense and (b) yield too many false positives. The research also suggests that there might be some value in distinguishing between different types of attacks (e.g., fraud, IP theft, etc.) when outlining the anatomy of insider attacks.

Dispositional indicators

Dispositional indicators can provide useful data about insiders, which might be used in the monitoring and risk assessments of employees. Turner and Gelles (2003) believe the following

https://doi.org/10.1017/jmo.2018.57 Published online by Cambridge University Press

psychological indicators need to be considered when examining insider risk: self-centredness, arrogance, risk-taking, manipulative, coldness, narcissism, self-deception, and defensiveness. CPNI (2013) have also identified from a sample of 120 cases a number of personality characteristics, including immature, low self-esteem, amoral and unethical, superficial, prone to fantasising, restless and impulsive, lacks conscientiousness, manipulate, emotionally unstable, evidence of psychological or personality disorders. Some of these characteristics map onto well-established and recognised personality traits (e.g., those in OCEAN – openness, conscientiousness, extraversion, agreeableness, and neuroticism and the dark triad – narcissism, psychopathy, and Machiavellianism). Shaw and Stock (2011) outline a number of personality traits that are typically exhibited by an insider, including antisocial traits, difficulties getting along with others, being above the rules, impulsivity, tendency to blame others, ambitious, and greedy. Their research, however, focussed on insider theft of IP and therefore cannot be generalised to all insider attacks.

Gaining a greater understanding of the psychological make-up of an insider might help organisations identify at-risk employees. To date, however, businesses and government organisations have conducted most of this research, and many of the categories employed are not traditional labels used by psychologists. As a further point, some of the personality characteristics that indicate a potential insider might also be traits sought out in an employee (e.g., ambition, Machiavellianism). Therefore, it might be counter-productive to spend resources monitoring employers based on their personality profile alone, as well as unethical (given that it might be discriminatory to label these as individuals as 'at-risk' employers) (Schultz, 2002). At present, we know little to inform organisations of the utility of monitoring at-risk employees based on their psychological profile.

Behavioural indicators

The manner in which a person behaves might also be an indicator of insider activity. Maloof and Stephens (2007) found that insiders carrying out IP theft can be detected by comparing an insider's volume of printing and Internet use with the pattern of Internet use and printing expected for their organisational role. Emotional state, such as feeling stressed or depressed has also been identified as behavioural indicators of insiders (e.g., Turner & Gelles, 2003; Shaw & Stock, 2011). Interestingly, Taylor et al. (2013) found that in hypothetical scenarios of insider attacks, those individuals who role-played insiders were more likely to alter their language to become more self-focussed and show greater negative effect compared with their noninsider coworkers. As with psychological characteristics, research on behavioural indicators suggests they might be useful in detecting insider threats. Further research could potentially yield interesting results. However, these same behavioural indicators might instead be the result of an incident in someone's life (e.g., grieving over the death of a loved one, stressed about meeting deadlines, etc.), rather than the intention to cause harm to an organisation. This again raises the question of ethics and accuracy in detection on behaviours alone.

Motivations

Understanding employees' goals and expectations might be useful for detecting and predicting insider threats. Numerous motivations for committing an insider attack have been noted in the literature, although it is the general consensus that disgruntlement is one of the main motivations for an insider attack (Band, Cappelli, Fischer, Moore, Shaw, & Trzeciak, 2006; Moore, Cappelli, & Trzeciak, 2008; Moore, Cappelli, Caron, Shaw, Spooner, & Trzeciak, 2011; Shaw & Stock, 2011; Cappelli, Moore, & Trzeciak, 2012). Moore et al. (2011) describe the 'disgruntled employee' as someone who is dissatisfied with their job due to a rejected request for a promotion, raise, or relocation. They also contend that a subset of disgruntled employees is the 'entitled independent'. According to these researchers, an 'entitled independent' is an insider who previously actively

https://doi.org/10.1017/jmo.2018.57 Published online by Cambridge University Press

contributed to the development of the IP of a product, and once they leave that organisation believe they are entitled to a share of this IP. Given this sense of entitlement, they are motivated to steal the product. Individual gain is another obvious motivation (Moore et al., 2011). This might be a financial gain (e.g., fraud) and/or nonmonetised personal gain, such as revenge. The alleviation of certain stressors has been identified as another motivation (CPNI, 2013; Shaw & Stock, 2011). Stressors might include financial problems, relationship difficulties, legal problems, loss of status, disagreement, and conflict with coworkers; however, not all people with the same circumstances or stressors commit insider attacks.

It is important that research further examines how common 'disgruntlement' is as a motivator or whether there are other motivations to commit insider attacks. If disgruntlement appears to be the main tipping point, then managers might make this the main focus of their attention in preventing insider attacks. However, if research identifies other motivations, then managers will need to cast their nets wider or else they will miss other important warning signs.

Opportunity/environment

Criminologists highlight the importance of considering 'opportunity' when developing predictive models of criminality. Cressey's (1953) 'Fraud Triangle' is an example of a theory that takes into account opportunity for individuals to commit fraud, including insider attacks. In this model, three factors are present in every instance of occupational fraud: motivation, rationalisation (the fraudster's ability to justify the act), and opportunity (the situation that enables fraud to occur). According to the theory, the individual first has a financial problem, which is nonshareable, and they become motivated to commit fraud. Second, they perceive an opportunity to commit fraud and have the skills to do so. Third, individuals employ rationalisations to give themselves permission to commit fraud. Although this theory has been popular among criminologists, it does have its critiques. For example, Huber (2016) has criticised the simplicity of the model. Moreover, rationalisation is a defence mechanism employed well beyond fraudsters to justify 'bad behaviour' (see, e.g., Freud, 1936/1992, who first outlined this psychological concept).

Some researchers have acknowledged that 'the immediate environment may not only afford potential opportunities but also help in provoking criminal behaviour' in the workplace (Willison & Siponen, 2009: 133). Willison and Siponen provide a list of 25 techniques that could be used in situational prevention of insider attacks. Examples include controlling access to facilities (e.g., swipe cards for office access), denying benefits (e.g., not having a clear desk and computer screen could lead to reduced rewards), and setting rules (e.g., security policies). Of course, opportunity is not simply about access privileges that employees hold legitimately but can also include perceived opportunities to illegitimately gain access (e.g., tailgating, stealing passwords, and hacking into systems).

Research Objectives

This paper examined which psychological, behavioural, and social variables (in both the physical and cyber realms) are important when identifying potential insider attackers. Typologies of insider attackers were also examined to determine whether previous findings might be replicated and/or whether new typologies might be identified. In addition to identifying variables, potential pathways that might lead to an attack were investigated. In so doing, the work produced in this paper offers a conceptual model for organisations to consider when detecting, deterring, and preventing insider attacks.

Method

Materials

A case study methodology was used for this investigation. Cases were either about an individual insider or a group of individuals that included one or more insiders. The attack took place within

https://doi.org/10.1017/jmo.2018.57 Published online by Cambridge University Press

the year before the interviews taking place. They involved semi-structured interviews where various people who knew (managers, fellow employees, HR personnel, heads of security and their teams, law enforcement officers dealing with the case) the insider was interviewed about the job role of the insider; their general behaviour in the workplace, before and after the attack; their observations regarding the person's personality and behaviour; the person's circumstances before and after the attack (both at organisation they conducted the attack as well as previous employment); information about the person outside of the workplace (e.g., socially, networks); their understanding of the person's motivation for the attack; details about how the insider went about the attack; and how the attack was detected. Approximately 2–3 people were interviewed per case study. Although the basic structure of the interview was adhered to for each participant, because each case was unique, and the person interviewed had different insights about the person (especially because of their role in the workplace), participants did not receive identical interview schedules.

Procedure

The University Ethics Committee first approved the study. The researchers then approached approximately 80 organisations (typically the head of security or HRs) inviting them to participate in the study about insider threat. Of these initial approaches, 21 organisations agreed to participate in the study. Approaches were made either to the head of security or HRs who then proceeded to organise interviews with people familiar with the employee to be interviewed by the researchers involved in the project.

In line with grounded theory, the intention was to either find support for previous assumptions about insiders as well as to gain new insights into an under-researched field. Although the researcher was mindful of the previous literature, participants were asked open-ended questions in order to gain new insights and there were no hypotheses developed. Participants were not given a tick box list of attributes to consider regarding the insider and the attack but instead were asked to volunteer their own insights.

In total, 99 case studies were collected from organisations that were willing to participate. To ensure anonymity and due to nondisclosure agreements, organisations cannot be named here; however, the types of organisations included are financial sector (64 cases, from five organisations), retail sector (16 cases from two organisations), public sector (six cases from three organisations), telecommunications providers (four cases from two organisations), high school (two cases from two organisations), labourer business (two cases from two organisations), insurance provider (one case), courier business (one case), nursery (one case), warehouse (one case), and prison (one case). Interviews were conducted face-to-face and the duration of each interview for each case study typically ranged from 30 min to 2 hr. When clarification was needed a second interview was conducted.

Participants

Participants in this study included individuals working in the types of organisations described earlier. For ethical and legal reasons, we cannot disclose the names of these organisations. Participants included are managers, fellow employees, HR personnel, heads of security and their teams, and law enforcement officers dealing with the case.

Grounded theory analysis

Given the dearth of literature available on insiders and the lack of systematic research, grounded theory was deemed an appropriate methodology for this study (Glaser & Strauss, 1967). Grounded theory allows researchers to keep an open mind to newly emerging theories from the data. It is an inductive, theory discovery methodology that allows the researcher to develop theory, while at the same time grounding the theory in data collected in empirical research.

https://doi.org/10.1017/jmo.2018.57 Published online by Cambridge University Press

Notably, there are different schools of thought regarding the implementation of grounded theory. In fact, sometime after their seminal work, Glaser and Strauss famously disagreed about how this method ought to be carried out. Strauss and Corbin's (1988) understanding of grounded theory is implemented in this research. In this approach, data can be examined to develop new theories (inductive analysis) but previous theory and hypotheses need not be ignored (deductive analysis). In this type of analysis, there is initially open coding, followed by axial coding (a reduction and clustering of categories), a final development of selective coding, and finally the development of theory. These steps are highlighted in the results and interpretation section.

Results and Interpretation

Sample description

The types of attacks reported in our case studies are fraud (80%), reputational damage (7%), theft (7%), IP/data theft (6%), identity theft (3%), money laundering (2%), procurement fraud (2%), and working illegally (1%), where 10% of cases involved more than one type of insider attack. The much higher number of fraud cases might be because (a) these types of attacks are more frequent across organisations and/or (b) organisations are more likely to detect this threat and/or (c) organisations feel more comfortable reporting fraud compared with other types of threats (e.g., IP theft).

In most cases there was a person working in isolation (68%); however, 32% of the cases involved a group (some of which included outsiders). In 50% of the cases the insider received a custodial sentence, 13% received a community service order, and 15% received a suspended sentence; 80% of the insiders were dismissed and 3% resigned. Among the participants, 62% of the insiders were males and 38% were females, with ages ranging from 19 to 62 years (mean = 31.39 years).

Analysis

Open coding was conducted in this first phase of the analysis, followed by axial coding, where a reduction and clustering of categories were carried out. All the data were independently coded by two coders and where discrepancies arose, we discussed the coding to arrive at an agreed category. There were only three incidents where we disagreed. The discrepancies in coding were on the personality characteristics. These were discussed, and an agreement was made as to how to code these three incidents. As a further note, interviewees were not asked to code for personality but rather to describe the personality of the insider. We opted for this method given that most interviewees were not trained psychologists. The coders, however, were trained psychologists – making it more appropriate for them to code the participants' descriptions of the insiders' personality.

Phase 1: Open coding

In the first round of coding (open coding), the following categories were identified: psychological, behavioural, and social characteristics of the insider; motivations of the insider; opportunities to commit the attack; and how the attack was discovered. Perhaps not surprisingly, these initial categories are similar to previous work (described in the introduction of this paper). The novelty of this research emerged in the new insights gained from an in-depth analysis of the themes and subthemes identified under each of these categories.

Phase 2: Axial coding

Axial coding was next conducted where themes under each of the main categories were reduced and clustered. The coding conducted in this phase can be found in Tables 1–4. Furthermore,

https://doi.org/10.1017/jmo.2018.57 Published online by Cambridge University Press

Table 5 sets out the archetypal 'insider fraudsters' identified in this phase of the analysis. These are also discussed in detail in the table.

Psychological, behavioural, and social characteristics

Psychological, behavioural, and social characteristics were broken down into the following subcategories: traits (e.g., extraversion, narcissism); life circumstances and actions before employment (e.g., criminal record, working illegally in the country); behaviours displayed at work before the attack (e.g., work affiliation, misconduct); emotions displayed during and leading up to the attack (e.g., stress, anxiety, depression); behaviours and life circumstances during the attack (e.g., showing off newly acquired wealth; unusual hours; increased time logged into secure areas) (see Table 1). As stated earlier, most participants did not have psychological training, and so naming specific personality traits would have proved difficult for them. Instead, the researchers categorised personality traits based on participants' descriptions of the insiders. They did so by drawing from established psychological questionnaires.

Some of the psychological, behavioural, and social characteristics of the insiders identified in this study were similar to previous work. Importantly, novel findings were also identified, especially with respect to the behavioural and social characteristics. Many of these characteristics have not been identified in previous work, such as an increased amount of time logged into secure areas and a change in attitude towards the workplace. Furthermore, archetypal insider fraudsters were identified, which are set out later in this paper (see Table 5). This adds to the literature on types of insiders, which has mostly focussed on the disgruntled employee (as highlighted in the introduction). Some examples of descriptions of psychological, behavioural, and social characteristics are provided in the summarised case studies, which are as follows:

- This individual perpetrated her fraud over the course of 6 years and accumulated over £278,000 before she was caught. She targeted an aged, vulnerable customer who was blind and suffering from advanced Parkinson's disease. In a long-term strategy, she manipulated the customer into signing forged documents transferring power of attorney to her, as well as writing a will, which would have transferred his entire estate to her husband and son when the customer died. Colleagues described her as domineering and assertive, with a clear aim of obtaining as much power within the organisation as possible. Although she was not senior to her peers, it appears that she manipulated them into subservience and saw herself as the 'ersatz store manager'. According to HR, this was not an unreal expectation given that she was a capable employee. When caught, the insider had available funds far exceeding the amount stolen and had been using the funds to send her son to private school as well as to purchase a lavish wedding for her daughter. Although the insider had narcissistic tendencies, more significant was her ability to cynically plan, deceive, coldly manipulate others in pursuit of power and financial goals (indicative of a Machiavellian and psychopathic subclinical personality). (*53-year-old female. Personal Banker at a bank – Insider Fraud: £278,000.*)
- Over the course of seven months, this individual defrauded two vulnerable customers of £40,000, primarily by obtaining signed cheques. The crime was motivated by greed and financial problems, with funds being spent on a holiday and a laptop computer. Colleagues described the individual as a 'troublesome employee' showing a pattern of emotional instability/neuroticism and stress-like symptoms, which might have suggested a potential threat to the organisation. After the individual was sentenced to a 16-month custodial term, she took a 'craft knife' that she had hidden about her person and started slashing at her arms and legs in an apparent effort to commit suicide. (*26-year-old female. Cashier at a bank – Insider Fraud: £40,000.*)

Table 1. Observed psychological and social characteristics (including traits, behaviours, and emotions)

Psychological and social characteristics	Description	%
Traits		
Extraverted	Outgoing, social, sensation seeking, and enthusiastic	25
Narcissism	A sense of entitlement and seeks admiration, attention, prestige, and status	10
Machiavellianism	Manipulative, charming, and highly ambitious person	11
Introverted	Quiet, less involved in the social world	8
Neurotic	Emotionally unstable	4
Psychopathy	Highly impulsive, risk takers, callous, lack of personal effort, and low on empathy	2
Asperger's	Autism spectrum disorder that is characterised by significant difficulties in social interaction and nonverbal communication	2
External locus of control	Fatalist view of the world, believing that events that happen are out of their control	2
Open to flattery	Open to flattery and being coerced by others (e.g., conned into a romantic relationship)	2
Life circumstances and actions before employment		
Gang membership	Socialising with or known member of a gang	9
Criminal record	Previous criminal record – either related or unrelated to current role	6
Working illegally in the country	Working illegally (e.g., limited or no work visa)	3
Presented forged documentation to HR	When applying/accepting the job the candidate presented forged documentation (e.g., birth certificate; education transcripts)	2
Behaviours displayed at work before the attack		
Strong work affiliation	Hard workers that appeared happy with their jobs and organisation	56
Weak work affiliation	Lazy or unmotivated workers that often appeared unhappy with their role and organisation	44
Aggressive	Physically and/or verbally aggressive to others (in or out of the workplace). Online and offline	11
Misconduct	Before the attack, the insider had been in trouble for misconduct at work (e.g., disciplinary suspension; security breaches)	8
Emotions displayed during and leading up to the attack		
Stressed, anxious, depressed	These individuals were described as stressed, anxious, and/or depressed. Many of the insiders were experiencing life stressors beyond the workplace; although the stress could have caused from engaging in the insider attack	20
Behaviours and life circumstances during the attack		
Addiction	Addiction problem, such as alcohol, drugs, shopping. During the attack – and typically leading up to the attack. Might have had this problem before employment	16
Personal hardship	Money needed due to personal hardship (e.g., divorce; partner lost their job; sudden family illness/accident)	15
Coercion/blackmail from others	An outside gang coerced the individual and/or threatened/blackmailed them into conducting the crime	13

https://doi.org/10.1017/jmo.2018.57 Published online by Cambridge University Press

Table 1. *Continued*

Psychological and social characteristics	Description	%
Increased time logged into secure areas	Employee spends greater amounts of time (than they normally would and for no apparent reason) in secure areas (e.g., viewing/editing customer accounts)	9
Showing off newly acquired wealth	Showing off newly acquired wealth without any explanation for the change in financial circumstances – appears to be living beyond their means	8
Change in attitude towards workplace	Change observed by those in the workplace from being highly motivated to low motivated workers	7
Displays signs of disgruntlement	Shows signs of disgruntlement (e.g., due to missed out promotion; unhappy with the way they have been treated)	7
Unusual hours	Turning up to work or leaving at times different to those required or expected and/or different compared with employees in similar roles. Taking longer breaks than permitted	4
Downloading large volumes of data	Downloading large volumes of data and/or emailing large volumes of data	3
Star employee – not meeting targets	A talented, well-regarded employee stops meeting targets and displays signs of distress	3
Absentee	Frequently taking time off work	3

Table 2. Motivations for committing the crime

Motivation	Description	%
Greed/living beyond their means	Intense and selfish desire to acquire wealth. Need money to support their lifestyle and pay-off debts (not acquired from addiction)	55
Need to support an addiction	Money needed to support addiction and/or pay-off insurmountable debt accrued from addition (e.g., alcohol, drug, shopping)	16
Personal hardship	Money needed due to personal hardship (e.g., divorce; partner lost their job; sudden family illness/accident)	15
Coercion/blackmail from others	An outside gang coerced the individual and/or threatened/blackmailed them into conducting the crime	13
Disgruntlement/ revenge	Disgruntled employee – wanting to hurt the organisation/ seek out revenge	7
Entitlement	Act was carried out due to a sense of entitlement (e.g., insider believed they were deprived of promotion/status within organisation that they were entitled to; stealing IP because they had contributed to the development of the product within the organisation)	6
Proof of cleverness	Wanted to prove to self and/or others their ability to commit the crime, undetected	5
Addicted to the crime itself	Appeared addicted to committing the crime – sense of enjoyment from the act itself	3

- This individual claimed £20,000 worth of fraudulent travel and entertainment expenses over the course of two and a half years. Reports from the investigation identified him as a ‘disgruntled employee’ as he believed that he was entitled to a promotion due to his recent performance but ultimately did not receive the promotion. It was thought that he had started to live according to the salary he thought he deserved and was incurring extensive

https://doi.org/10.1017/jmo.2018.57 Published online by Cambridge University Press

Table 3. Opportunities for committing the crime

Opportunity	Description	%
Sought weakness in security	Sought out weakness in security (physical or cyber) in order to commit the crime; deliberately sought out to breach security	45
Exploit others/abused position of authority	Sought out ways to exploit/manipulate others in order to commit the crime; abused position of authority (e.g., vulnerable customers; recruit other insiders)	38
Outsiders assistance	Outsiders helped the insider to commit the crime (one case involved a previous employee)	21
Sought out from onset	Intended to commit the crime from the outset of employment. Set about seeking out an opportunity to commit the crime from the beginning of their employment. Many of these insiders had previous convictions	18
Stumbled across weakness in security	Accidently stumbled across weakness in security (physical or cyber) that prompted them to consider committing the crime	5
Previous employment enabled the crime	Work conducted in the criminals' previous employment enabled the crime (e.g., stolen identities from clients from previous job)	3

Table 4. Discovery

Discovery	Description	%
Digital/video evidence	Digital or cyber evidence obtained after the attack – because suspicions had been raised	61
Monitoring physical/online initiated after the attack	Person was monitored more closely after complaints or suspicions (usually from someone outside of the organisation). The attack was then discovered in real-time and evidence was found of previous attacks	28
Monitoring procedures – real time	Monitoring procedures detected the attack in real time (cyber and/or physical)	28
Customer complaints	Serious complaints by clients/customers about the employee or about problems with their accounts prompted an investigation	28
Suspicious behaviours reported	Suspicious behaviour/caught in the act reported by fellow employees prompted an investigation	19
Outside organisation	An outside organisation detected the attack – evidence was provided via these outside sources, which prompted an internal investigation	9

credit card debt (£60,000). (*47-year-old male. Head of Key Accounts at a large Insurance Provider. Insider Fraud: £20,000.*)

- It was reported that this individual had Asperger's syndrome. He was very hard working and showed a strong affiliation to the organisation for which he worked. He deliberately breached the security of the building (understanding the seriousness of this breach) in which he worked by gaining repeated access to online and physical spaces to which he was not authorised. He used the information he gained from security breaches, including plans of the building, to replicate the building in Second Life. The motivation for this breach appeared to be an opportunity to show off his skills, although it is possible that his motivations were more sinister. He understood that he would most likely be dismissed for breaching security but still decided to take this risk. (*Mid-50s male. Security guard. Security breach – risking the reputation and security of the organisation.*)

https://doi.org/10.1017/jmo.2018.57 Published online by Cambridge University Press

Table 5. Archetypal insider fraudsters

Archetype	Description	n
The Addict	The addict had either a gambling, drug, or alcohol addiction. They were often absent from work and/or worked unusual hours compared with fellow employees (e.g., taking longer lunches). Some of these individuals belonged to a gang. Fellow colleagues often noticed the addiction with some reporting the behaviour. Customers and colleagues often complained about their behaviours. Around the time of the attack they displayed high amounts of anxiety and stressed and demonstrated a weak work commitment	16
Harder times	This type of employee experienced a change in family circumstances. This might have included: a divorce, partner losing their job, a sick child, or spouse. Money is often needed for this change in circumstance. This insider often originally considered a star employee but when the change in circumstances occurs their fraudulent acts involve exploiting others, logging into secure areas, and a change in work patterns. At the time around the attack they display heightened anxiety and stress	12
Pure greed	These individuals were motivated by pure greed. They sought out opportunities, manipulated colleagues, and took advantage of their position/authority/security access. Most of these individuals are Machiavellian and Narcissist, but not all	10
The show off	This type of employee was flamboyant, with an extravagant lifestyle. They would exploit vulnerable people/clients. They were narcissist, extraverted, highly social, and often described as 'the life of the party'. Their expensive clothes and extravagant holidays gave off signs of someone living beyond their means. They were also often a 'star' employee. Some of these individuals were also part of a gang, and some had a drinking problem	8
Disgruntled employee	The same archetype of the disgruntled employee, that has been identified in previous research, was identified in this study. This employee is someone who is dissatisfied with their job due to a rejected request for a promotion, raise, or, relocation.	7
Birds of a feather	These were tight-knitted groups of similar ages (not necessary young) and often shared ethnicity (in this sample groups were either British or African) who worked together on the attack. Sometimes they also operated together with outsiders. Two of these groups had worked for the organisation for many years and were star employees. These individuals were not disgruntled, but rather found an opportunity and by encouraging each other they felt more enabled to commit these crimes. They mostly display a strong work affiliation	6
Career criminal	This employee moves from one job to the next with the intention to commit fraud. They committed fraud soon after commencing employment. They had employment histories of working for short stints in previous jobs. They were greedy, exploited others, logged into secure areas after using a colleague's username and password	5
Clever clogs	This type of employee was motivated to demonstrate their cleverness, rather than purely to gain money. At the time of the attack their work patterns changed (e.g., work hours, where they situated themselves in the building)	4

Motivations

Participants were asked what they believed motivated the criminal in each case to engage in the attack. More than one motivation could be noted in many cases and in 8% of the cases, the motive was unknown. Greed was by far the most common motivation, followed by supporting an addiction, money needed for a personal hardship and coercion were the most common motives (see Table 2). Although personal hardships and coercion were coded under psychological, behavioural, and social characteristics, they were also included here as they could also be classified as motivations. Notably, although the literature on insiders focusses heavily on disgruntlement as a motivation, the research identified very few cases where disgruntlement was a reason for the attack. This is a key finding that moves the thinking about insiders in a new direction. The research in this paper demonstrates multiple insider motivations, thus highlighting that there are many pathways to criminality that managers need to consider. The work here shows that managers should not be too heavily focussed on the disgruntled employee, for if

https://doi.org/10.1017/jmo.2018.57 Published online by Cambridge University Press

they do other insiders are likely to pass undetected. Some examples of descriptions of motivations are provided in the summarised case studies as follows:

- This individual was described by colleagues as 'egotistical' and highly. It was thought that he may have felt entitled to advancement and was already living beyond his means. The fraud was potentially part of a scam involving local businesses to defraud insurance companies in a 'Cash for Crash' scenario. The individual spent the proceeds of the crime on funding his lavish lifestyle, paying for his flashy car, socialising, and purchasing superficial goods. This insider never tried to hide any of his spending such as his expensive car. (*26-year-old male. Cashier at a bank. Insider Fraud: £120,000.*)
- The insider, who had recently separated from his partner, claimed to be coerced by two other insiders within the bank, who approached his house demanding money because his former partner owed them a substantial amount of money. When he refused, they beat him with a hammer and left him for dead. After recovering, the insider was again threatened and forced to take part in the theft operation and, fearing future assault, agreed. The two aggressors used their access to change customer information, which permitted the insider to pose as the customer and make cash withdrawals. This significant act of fraud (totalling £4,000,000) was only uncovered when the victim had difficulties in correctly answering security questions. (*47-year-old male. Customer service staff in a bank. Insider Fraud: £4,000,000.*)

Opportunities

The participants were asked about how the insider was able to commit the attack. Their responses were coded under opportunities (see Table 3). Almost half of the sample consisted of cases where the insider deliberately sought out a weakness in security at their organisation in order to carry out the attack. Notably, in approximately 20% of the cases, outside help was obtained to enable the attack. Examples of opportunities are presented below:

- The individual appeared to have identified himself as a financial expert to his family and taken over partial control of his niece's charitable trust (his niece was a quadruple amputee). After doing so, he suggested that funds be sent overseas in order to optimise the return. When asked to return the funds, he was unable to do so, claiming that the money was tied up by offshore banks. In reality, he defrauded £315,000 from a charitable trust set up to provide his quadruple amputee niece with prostheses and equipment. In addition, he stole £65,000 from his grandmother. He covered his tracks with fake bank statements, and falsely claimed to have put the funds in an offshore account to gain higher interest but appeared unable to return funds. He took out a number of joint loans secured on the family home without the consent or knowledge of his wife, which caused his wife and daughter to be evicted and forced into bankruptcy after their divorce. (*33-year-old male. Risk assessor at a bank. Insider Fraud: £230,000.*)
- The two insiders targeted a wealthy retired customer's account while the customer was on an overseas holiday. They transferred the money into an accomplice's account, by using a blind cashier's computer, turning off her speaking screen so she was unaware that they were using her computer to commit fraud. (*21-year-old male. Counter staff at a bank. Insider Fraud: £96,000.*)
- Prior to resigning from his role as a financial advisor with the bank, this individual emailed his entire customer portfolio to his personal email address and used this information to target victims in his later fraud. He defrauded four elderly and vulnerable customers (aged 84, 87, 94, 98 years respectively) over the course of a two-year period to the value of £120,000. He set up a false 'investment club' and recruited these former customers to invest in the fund. This individual failed to be clear that he

no longer worked for the bank in his dealings with the victims. After he was arrested he appeared 'devastated' and cried during the initial interviews with police and corporate investigators, but gave the impression of being dismissive of the charges. Colleagues were surprised to learn that of his crime given they believed it to be 'out of character'. (*early 60s male. Financial advisor. Insider Fraud and IP theft: £120,000.*)

Discovery

This study was also interested in learning about how the attack was discovered, including when the alarm bells were raised and what evidence was needed to detect the attacker (see Table 4). Notably, fewer cases were detected in 'real time' (28%) compared with searching for evidence after the attack (61%). Moreover, of concern were the number of discoveries outside of the organisation, made by customers/clients (28%) and other organisations (9%). Examples of discoveries are presented below:

- Over the course of 2 weeks, this individual used colleagues' login credentials to transfer monies totally £820 into his own account in order to fund a gambling addiction (online roulette) and pay off debts. He identified elderly wealthy customers with accounts showing infrequent activity (possibly hoping that his fraudulent activities might have been unnoticed). The fraud was noticed by a fellow employee and reported to police. (*28 year-old-male. Accounts processor at a call centre. Insider Fraud: £820.*)
- Over the course of two years, the insider stole funds deposited in a night safe. The funds in question were usually deposited uncounted and tallied by the bank staff before being deposited into the company's account. This individual obtained access to the night safe (which usually required two operators) and skimmed £70,000 from the deposits. The company secretary became suspicious about the value of deposits being made and began to count the deposits before putting them in the safe. After the discrepancies were noticed, an investigation was launched. (27 year-old-male. Customer advisor at a bank. Insider Fraud: £70,000.)

Archetypal insider fraudsters

The analysis next moved to identify archetypal cases of insider fraudster – only fraudsters were examined in this part of the analysis given they were the majority of insider cases identified, providing enough data to form clusters. The archetypes do not set out the full details of the insiders' psychological dispositions and pathways to the attack (as is set out in the conceptual model in the next phase), but rather provide additional insights into identifying types of insiders. Archetypes identified included those also found in previous research (e.g., disgruntled employee); however, new archetypes were also revealed in this analysis. Some of these archetypes, although not previously named, resonate with previous research (e.g., 'the addict'), while others, arguably, provide new and novel insights into insiders (e.g., 'the show off', 'birds of a feather', and 'clever clogs'). Notably, there was overlap between 'the show off' and 'pure greed'; however, it was felt there were important differences between these groups making it important to separate. Moreover, the 'show off' might be easier to detect compared with the 'pure greed' archetype. Although further research is needed to confirm these findings, they go some way into developing new theories and understandings about the types of insiders.

Conceptual Model

In the last phase of the analysis, the data were reduced again and clustered to develop a conceptual model. Figure 1 sets out a model for organisations to draw from in the prevention and

https://doi.org/10.1017/jmo.2018.57 Published online by Cambridge University Press

detection of insider attacks. As detailed in the model, prevention steps in the form of vetting and closing down opportunities are outlined before the recruitment of employees. Further prevention steps should be considered when: (a) new opportunities to attack are elucidated, and (b) when

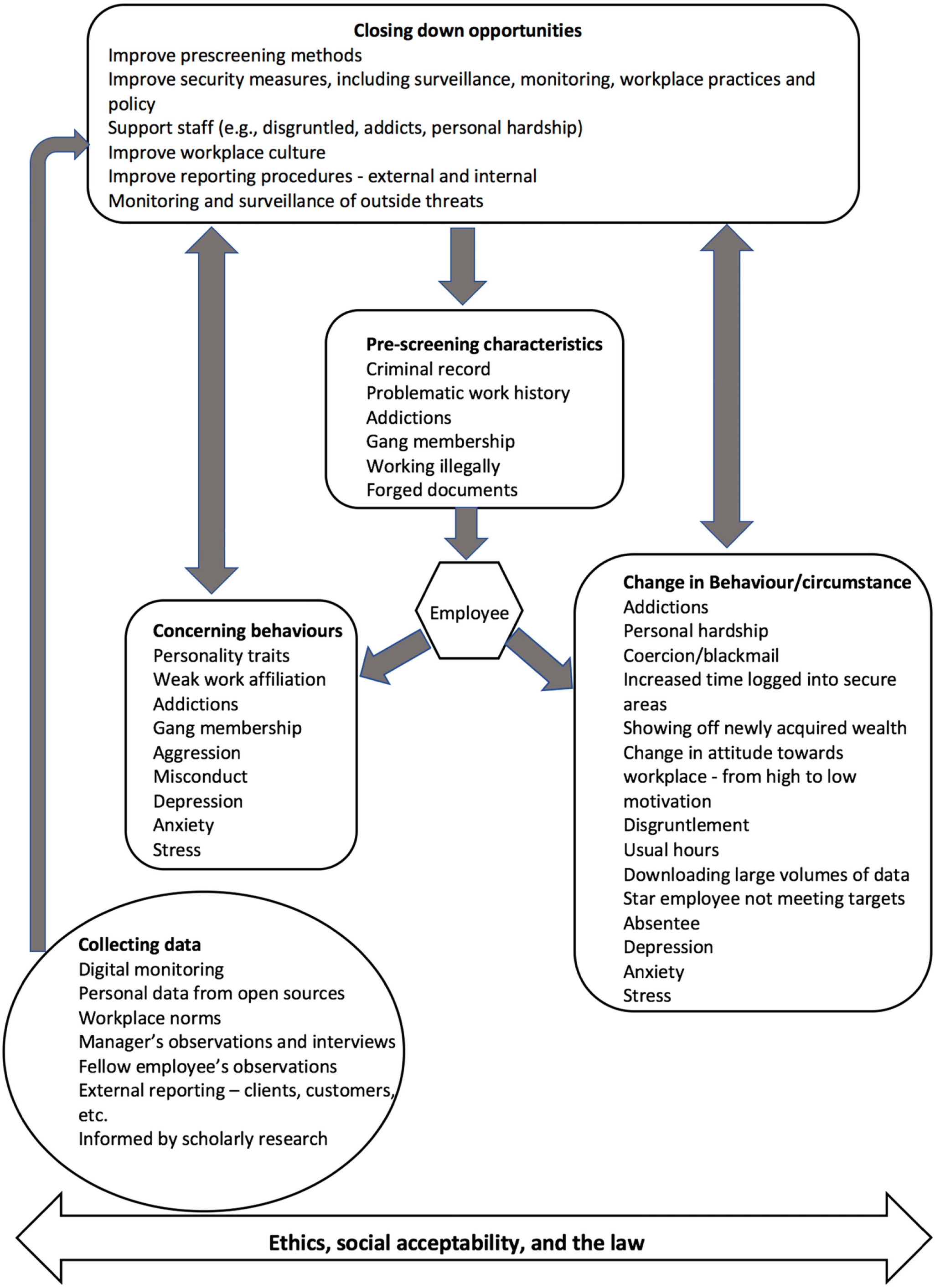
Closing down opportunities
Improve prescreening methods
Improve security measures, including surveillance, monitoring, workplace practices and policy
Support staff (e.g., disgruntled, addicts, personal hardship)
Improve workplace culture
Improve reporting procedures - external and internal
Monitoring and surveillance of outside threats
Pre-screening characteristics
Criminal record
Problematic work history
Addictions
Gang membership
Working illegally
Forged documents
Employee
Concerning behaviours
Personality traits
Weak work affiliation
Addictions
Gang membership
Aggression
Misconduct
Depression
Anxiety
Stress
Change in Behaviour/circumstance
Addictions
Personal hardship
Coercion/blackmail
Increased time logged into secure areas
Showing off newly acquired wealth
Change in attitude towards workplace - from high to low motivation
Disgruntlement
Usual hours
Downloading large volumes of data
Star employee not meeting targets
Absentee
Depression
Anxiety
Stress
Collecting data
Digital monitoring
Personal data from open sources
Workplace norms
Manager's observations and interviews
Fellow employee's observations
External reporting – clients, customers, etc.
Informed by scholarly research
Ethics, social acceptability, and the law

Figure 1. Prevention and detection of insider attacks

https://doi.org/10.1017/jmo.2018.57 Published online by Cambridge University Press

indicators detect a potential problematic employee. Closer monitoring of the indicators highlighted in this research might also help detect an insider. However, it is argued here that ethics, social acceptability, and the law should guide all steps in prevention and detection – to ensure employees are not discriminated against. Moreover, rather than treat an employee as a 'potential insider', it would be prudent to set out transparent and effective practices to support problematic employees to 'nudge' them away from carrying out harm to an organisation.

As a further note, the analysis revealed many pathways to committing an insider attack and suggests that by following a particular pathway to detect a crime might be challenging and resource intense. The model proposed here, therefore, sets out indicators (both physical and cyber) that might be important to observe and used by organisations to prevent and detect insider threats/attacks and best practices to close down opportunities.

Importantly, the model is in flux. New data and re-combinations of data can be feed into the model as new insights are gained – both in scholarly research and as the organisation itself examines its own data. Methods to collect evidence are highlighted in the model, with the important caveat that the ethics, social acceptability, and legality of collecting this data *must* be considered before any collection and analysis. The components of the model are described in more detail below.

Closing down opportunities: This is highlighted at the start of the model. Closing down opportunities includes a combination of prevention and detection. As this research highlights, closing down opportunities (e.g., improved security measures, transparent policies for support for workers, and reporting problematic behaviours) needs to be considered before the recruitment of employees and also needs to be regularly considered and improved in light of new information. As discussed earlier in this paper, the Fraud Triangle includes opportunity as an element to explain why the fraud takes place – arguably, without opportunity there would be no fraud. Although this research concurs, it provides detail to the opportunities that need to be closed down and highlights that this is important with all types of insider threats.

In this research, it was found that insiders sought out weaknesses in the security in order to carry out the attack and many abused their position of authority. Outsiders also helped the insider commit the crime. Prevention, therefore, might involve strengthening security and the development of workplace policy to close down on insider threat opportunities (e.g., not sharing passwords). However, as discussed earlier, prevention might also involve providing support for staff (e.g., disgruntled, those with addictions, personal hardships) – if staff feel supported they might be less inclined to seek out opportunities to create an attack.

In some cases, insiders were an inherent part of the workplace culture – where others were encouraged to enable another insider or sections within an organisation committing an attack (typically fraud) because they had noticed others engaging in such crimes. In other cases, the stress of not meeting targets was believed to lead to the attack. These examples suggest that in some cases the workplace culture needed to be improved to prevent insider attacks.

Finally, the monitoring of outside threats cannot be ignored when considering closing down opportunities for insider attacks. In 21% of the cases reported in this study, an outsider assisted the insider (sometimes instigating the attack and recruiting the insider by instructing them on how to undergo the attack). Therefore, an insider threat and prevention strategy should consider combining monitoring for external threats.

Prescreening characteristics are arguably important for any organisation. However, vetting processes need to be legal and nondiscriminatory. This research found that it would be unhelpful and discriminatory to vet according to personality characteristics. For example, while some psychological characteristics were highlighted as problematic, not all employees that exhibit these traits will go on to be insiders. Machiavellianism and narcissism might be useful traits in some types of roles, for example. Other characteristics that might be helpful to vet include criminal record, problematic work history, addictions, gang membership, working illegally, and forged documents. Ethical and nondiscriminatory practices also, however, need to be considered when

https://doi.org/10.1017/jmo.2018.57 Published online by Cambridge University Press

prescreening for these variables. For example, a person with a criminal past may be reformed and possibly an asset to an organisation. It is noteworthy that for some cases in this research, characteristics that could have been vetted for were not noticed. For example, it is a concern that forged documents and employees who were working illegally were undetected.

Concerning behaviours in this model included those presented by the employees, including personality traits, weak work affiliation, addictions, gang membership, aggressive behaviours (towards staff and/or outside of work), misconduct at work, depression, anxiety, and stress. As with the prescreening characteristics, selective monitoring of some staff over others might be illegal and/or unethical. Moreover, this additional monitoring could potentially be a catalyst for an insider attack – if the employee experiences resentment for deferential treatment. These concerning behaviours and closing down opportunities are linked in both directions of the model. An employer, for example, might notice an employee who presents a problematic behaviour and provide them with support or closer monitoring to assist in prevention and detection. In turn, opportunities might be closed down to prevent some of these types of behaviours: for example, clear policies on aggressive behaviour might prevent or deter this behaviour in the workplace.

Change in behaviours/circumstances was perhaps the more interesting indicators revealed in the case studies. In hindsight, when asked to consider what the organisation knew or learnt subsequent to the attack, numerous indicators were noted that could become part of an organisations' policy to monitor more closely or consider interventions to prevent impending harm to an organisation. The variables included addictions, personal hardship, coercion/blackmail, increased time logged into secure areas, showing off newly acquired wealth, change in attitude towards the workplace – from highly to lowly motivated, disgruntlement, working unusual hours, a star employee no longer meeting targets, absentee, downloading large volumes of data, depression, anxiety, and stress. Interestingly, this list included both cyber and physical behaviours. A change in behaviour/circumstances might be more important to monitor for those who do not necessarily join an organisation with characteristics that appear risky to an organisation. Again, an organisation should be mindful that selective monitoring of some staff over others might be illegal and/or unethical. Moreover, this additional monitoring could potentially be a catalyst for an insider attack – if the employee experiences resentment for deferential treatment.

Collecting evidence: In addition to considering the sorts of variables an organisation might wish to monitor, the model highlights the data needed to detect an insider as well as to improve prevention methods. The data includes new insights within the organisation as well as being informed by scholarly research. In the main, this research found that the discovery of an attack happened after the event – often informed by an outsider or a fellow employee. It would be unwise, therefore, to abandon such methods. Nonetheless, such discovery methods might be improved. It was surprising how few managers and fellow employees reported suspicious behaviour until after a complaint from outside was made – and perhaps methods such as regular interviews/conversations with employees might help highlight problems before an attack. Well-communicated policies on how to report suspicious behaviours might also improve detection, while also being sensitive to problems experienced by employees who whistle-blow, particularly in the UK (see, e.g., Park, Blenkinsopp, Kemal Oktem, & Omurgonulsen, 2008). Effective monitoring of employees in real time would have picked up the attack earlier in most cases. Moreover, future work could include the combination of physical and cyber indicators when monitoring employees. Physical observations might be combined with digital anomalies. Moreover, recent research is improving on the detection of psychological variables via digital communication (e.g., De Choudhury & Counts, 2013; Hogenboom, Bal, Frasincar, Bal, de Jong, & Kaymak, 2013) and such findings might be incorporated into detection tools for insider threat.

Ethics, social acceptability, and the law: Finally, the model asks users to reflect upon and ensure that policy and methods in prevention and detection of insider threat are ethical, socially acceptable (including acceptable practices for that particular workplace and culture), and legal.

https://doi.org/10.1017/jmo.2018.57 Published online by Cambridge University Press

These are important to consider in every aspect of the model. As a further note, if methods are employed that cause upset and distrust amongst the workplace, there is the risk that insider attacks might increase rather than be reduced (Greitzer & Frincke, 2010).

Conclusions

The work conducted in this paper provides a detailed examination of a large sample of insider cases. Interviewing a range of people who knew the insiders provided important insights. Previous work has mostly focussed on fraud or IP theft and rarely together. This study, instead, examined a range of different types of insider cases, providing a much richer picture.

The work here provides a radical re-thinking of the insider problem. To date, research has offered little in respect to pathways to criminality and when they have the models have been fairly basic. In this research, the Fraud Triangle, which is a popular model in criminology, was found to be quite limiting as a predictor of criminality. Previous linear models developed to explain pathways to insider criminality (e.g., Shaw & Stock, 2011) were also shown to miss the numerous pathways and motivations for committing an insider attack. The conceptual model offered in this paper highlights that pathways are not necessarily linear, that there are multiple pathways, and that there is an ongoing need to focus on closing down opportunities and to seek out behavioural change indicators. The model also emphasizes the need to help employees when concerning behaviours are presented rather than simply monitoring employees as if they were an insider on the pathway to an attack.

As highlighted in the introduction, the 'disgruntled employee' is often viewed as the archetypal insider. This research, however, demonstrated that there are many other typologies that managers need to consider. The addict was the more common insider in this research and highlights the need to deal head-on with this problem rather than ignore the issue or move employees with addictions around in an organisation in the hope the issue will disappear. 'Harder times' was the next common archetype – highlighting that problems that are external to an organisation might be much more important to consider compared with disgruntlement. Disgruntlement was, in fact, much further down the list, and while more research is needed to replicate these findings, this research has highlighted that the disgruntled employee is one of many concerns rather than the main issue.

The Internet has added a further threat to organisations providing more opportunities for employees to exploit this medium to cause harm to an organisation – making research in this area all the more urgent. This research found that strategies to closing opportunities for employees to commit insider attacks must also include ensuring all staff adhering to policies regarding good cybersecurity practices (e.g., not sharing passwords, writing passwords down, hacking into systems). In turn, cyber indicators might be used to identify potential insiders (e.g., download volumes, logging in and out times, security breaches). The findings from this study can be used to guide behavioural and automatic insider detection methods and tools.

Admittedly, this study is limited in a number of ways. It is not a representative sample (indeed it is hard to know what a representative sample of an unknown population would look like), and the majority of cases focussed on fraud attacks (given that organisations often prefer to be more closed about other types of attacks, to protect their reputations). The participants interviewed for the study might not be accurate in their insights about the insiders' personality or interpretation of emotions. Moreover, the criminals' perspective in these case studies was not obtained – which would have increased the validity of our findings. Nonetheless, the work here does provide researchers with a rich conceptual model that can be tested and researched in greater depth in future studies.

Acknowledgements. This research was conducted in the context of a collaborative project on Corporate Insider Threat Detection, sponsored by the UK National Cyber Security Programme in conjunction with the Centre for the Protection of National Infrastructure, whose support is gratefully acknowledged. The project brought together three departments of the

University of Oxford, the University of Warwick, and Cardiff University. I would also like to thank Gordon Wright who assisted in the coding of case studies and Prof Mike Levi for his feedback on an earlier version of the paper.

References

Band, S. R., Cappelli, D. M., Fischer, L. F., Moore, A. P., Shaw, E. D., & Trzeciak, R. F. (2006). *Comparing insider IT sabotage and espionage: A model-based analysis* (Technical Report No. CMU/SEI-2006-TR-026). Pittsburgh, PA: Software Engineering Institute. Retrieved from https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8163

Cappelli, D. M., Moore, A. P., & Trzeciak, R. F. (2012). The CERT guide to insider threats: How to prevent, detect, and respond to information technology crimes. USA: Addison-Wesley Professional.

CERT Program (Carnegie Mellon University) and Deloitte (2011). CyberSecurity watch survey: Organisations need more skills cyber professionals to stay secure. *CSO Magazine* Retrieved from http://www.sei.cmu.edu/newsitems/cybersecurity watch survey 2011.cfm

CIFAS (2012). *Staff Fraudscape: Depicting the UK's staff fraud landscape* Retrieved April 8, fromhttps://www.cifas.org.uk/secure/contentPORT/uploads/documents/Cifas%20Reports/External-0-StaffFraudscape_2012.pdf

CPNI (2013). *CPNI insider data collection study – Report of main findings* [Report]. Retrieved from http://www.cpni.gov.uk/Documents/Publications/2013/2013003-insider_data_collection_study.pdf

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

De Choudhury, M., & Counts, S. (2013). Understanding affect in the workplace via social media. Proceedings of the 2013 conference on computer supported cooperative work, pp. 303–316.

Freud, A. (1936/1992). *The ego and the mechanisms of defence*. London: Karnac Books.

Gill, M. (2007). *Learning from fraudsters: Reinforcing the message*. London: Protiviti.

Glaser, B. G., & Strauss, A. (1967). *The discovery of grounded theory: Strategies for qualitative research*. Chicago, USA: Aldine Publishing Co.

Greitzer, F. L., & Frincke, D. A. (2010). Combining traditional cyber security audit data with psychosocial data: Towards predictive modelling for insider threat mitigation. *Advances in Information Security*, *49*, 85–113.

Hogenboom, A., Bal, D., Frasincar, F., Bal, M., de Jong, F., & Kaymak, U. (2013). Exploiting emoticons in sentiment analysis. Proceedings of the 28th annual ACM symposium on applied computing, pp. 703–710.

Huber, W. D. (2016). Forensic accounting, fraud theory, and the end of the fraud triangle. *Journal of Theoretical Accounting Research*, *12*(2), 28–48.

Kroll (2015). Global fraud report: Vulnerabilities on the rise. Retrieved from http://anticorruzione.eu/wp-content/uploads/2015/09/Kroll_Global_Fraud_Report_2015low-copia.pdf

Legg, P., Moffat, N., Nurse, J. R. C., Happa, J., Agrafiotis, I., Goldsmith, M., & Creese, S. (2013). Towards a conceptual model and reasoning structure for insider threat detection. *Journal of Wireless Mobile Networks Ubiquitous Computing and Dependable Applications*, *4*(4), 20–37.

Magklaras, G. B., & Furnell, S. M. (2001). Insider threat prediction tool: Evaluating the probability of IT misuse. *Computers & Security*, *21*(1), 62–73.

Maloof, M. A., & Stephens, G. D. (2007). ELICIT: A system for detecting insiders who violate need-to-know. RAID, International Workshop on Recent Advances in Intrusion Detection, 146–166.

Moore, A. P., Cappelli, D., Caron, T. C., Shaw, E., Spooner, D., & Trzeciak, R. F. (2011). A preliminary model of insider theft of intellectual property (Technical Report No. CMU/SEI-2011-TN-013). Pittsburgh, PA: Software Engineering Institute. Retrieved from http://repository.cmu.edu/cgi/viewcontent.cgi?article=1722&context=sei

Moore, A. P., Cappelli, D. M., & Trzeciak, R. F. (2008). The "big picture" of insider IT sabotage across US critical infrastructures (Technical Report No. CMU/SEI-2008-TR-009). Pittsburgh, PA: Software Engineering Institute. Retrieved from http://www.cert.org/archive/pdf/08tr009.pdf

Nurse, J.R.C., Buckley, O., Legg, P. A., Goldsmith, M., Creese, S., Wright, G. R. T., & Whitty, M. (2014). Understanding insider threat: A framework for characterising attacks, *IEEE Security and Privacy Workshops.*

Ophoff, J., Jensen, A., Sanderson-Smith, J., Porter, M., & Johnston, K. (2014). A descriptive literature review and classification of insider threat research. Proceedings of Informing Science & IT Education Conference (InSITE), 2014 (pp. 211-223).

Park, H., Blenkinsopp, J., Kemal Oktem, M., & Omurgonulsen, Y. (2008). Cultural orientation and attitudes towards different forms of whistleblowing: A comparison of South Korea, Turkey and the UK. *Journal of Business Ethics*, *82*(4), 929–939.

Randazzo, M. R., Kenney, M., Kowalski, E., Cappelli, D., & Moore, A. (2005). Insider threat study: Illicit cyber activity in the banking and finance sector. Technical report: Carnegie Mellon Software Engineering Institute. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a441249.pdf

Richardson, R. (2011). CSI computer crime and security survey. Retrieved from http://www.GoCSI.com

Schuchter, A., & Levi, M. (2016). The fraud triangle revisited. *Security Journal*, *29*(2), 107–121.

Schultz, E. E. (2002). A framework for understanding and predicting insider attacks. *Computers & Security*, *21*(1), 62–73.

https://doi.org/10.1017/jmo.2018.57 Published online by Cambridge University Press

Shaw, E. D., & Stock, H. V. (2011). Behavioral risk indicators of malicious insider theft of intellectual property: Misreading the writing on the wall (White paper). Symantec. Retrieved from https://scm.symantec.com/resources/21220067_GA_WP_Malicious_Insider_12_11_dai81510_cta56681.pdf

Strauss, A., & Corbin, J. (1988). *Basics of qualitative research: Grounded theory procedures and technique*. London: Sage.

Taylor, P. J., Dando, C. J., Ormerod, T. C., Ball, L. J., Jenkins, M. C., Sandham, A., & Menacere, T. (2013). Detecting insider threat through language change. *Law and Human Behavior*, *37*(4), 267–275.

Turner, J. T., & Gelles, M. (2003). *Threat assessment: A risk management approach*. New York, USA: Routledge.

Willison, R., & Siponen, M. (2009). Overcoming the insider: Reducing employee crime through Situational Crime Prevention. *Communications of the ACM*, *52*(9), 133–137.

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