Information & Computer Security

509

The prince of insiders: a multiple pathway approach to understanding IP theft insider attacks

Monica Therese Whitty and Christopher Ruddy
Department of Software Systems and Cybersecurity, Monash University, Melbourne, Australia

David Keatley
School of Law and Criminology, Murdoch University, Perth, Australia

Marcus Butavicius
Australian Defence Science and Technology Group, Edinburgh, Australia, and

Marthie Grobler
CSIRO Data61, Sydney, Australia

Received 9 November 2023
Revised 14 May 2024
Accepted 25 May 2024

Abstract

Purpose – Intellectual property (IP) theft is an increasing threat that can lead to large financial losses and reputational harm. These attacks are typically noticed only after the IP is stolen, which is usually too late. This paper aims to investigate the psychological profile and the socio-technical events that statistically predict the likelihood of an IP threat.

Design/methodology/approach – This paper analyses 86 IP theft cases found in court documents. Two novel analyses are conducted. The research uses LLMs to analyse the personality of these insiders, which is followed by an investigation of the pathways to the attack using behaviour sequence analysis (BSA).

Findings – These IP theft insiders scored significantly higher on measures of Machiavellianism compared to the normal population. Socio-technical variables, including IP theft via photographs, travelling overseas, approaching multiple organisations and delivering presentations, were identified. Contrary to previous assumptions that there is a single pathway to an attack, the authors found that multiple, complex pathways lead to an attack (sometimes multiple attacks). This work, therefore, provides a new framework for considering critical pathways to insider attacks.

Practical implications – These findings reveal that IP theft insiders may come across as charming, star employees rather than the stereotype of disgruntled employees. Moreover, organisations' policies may need to consider that IP theft occurs via non-linear and multiple pathways. This means that sequences of events need to be considered in detecting these attacks instead of anomalies outright. The authors also argue that there may be a case for "continuous evaluation" to detect insider activity.

Originality/value – This paper offers a new framework for understanding and studying insider threats. Instead of a single critical pathway, this work demonstrates the need to consider multiple interconnected

This research was supported by a grant funded by the Department of Defence Next Generation Technologies Fund (NGTF) initiative.

Information & Computer Security
Vol. 32 No. 4, 2024
pp. 509-522
Emerald Publishing Limited
2056-4961
DOI 10.1108/ICS-11-2023-0210

pathways. It elucidates the importance of a multidisciplinary approach and provides opportunities to reconsider current practices in detection and prevention.

Keywords Insider threat, IP theft, Machiavellianism, Behaviour sequence analysis, Socio-technical, Multiple critical pathways, Multidisciplinary, Situational crime prevention, Cybersecurity

Paper type Research paper

1. Introduction

Intellectual property (IP) theft is arguably one of the foremost international concerns that impact global economics. The Australian Security Intelligence Organisation Director-General of Security in Australia, Mike Burgess, stated that we are witnessing the "most sustained, sophisticated and scaled theft of IP and expertise in human history" (Tomazin, 2023). This attack may be conducted by insiders seeking a financial opportunity, state actors already inside an organisation or state actors working with an insider (Tomazin, 2023).

In general, insiders are often described as either malicious (intentional) or accidental. Research typically considers malicious insiders as a homogenous group – all intending to cause harm to an organisation and gain personally. Moreover, they are often regarded as disgruntled employees (Shaw *et al.*, 2013). Consequently, workplace policy assumes that monitoring for particular cyber events is sufficient for insider threats in general (Wei *et al.*, 2024) and requiring managers to monitor for specific behaviours will bring to light an insider in an organisation (Colwill, 2009). Arguably, however, different types of attackers may have slightly different motives and other distinguishable characteristics (Whitty, 2021). Therefore, this paper has focused on one type of insider attack – IP theft. Notably, this paper is a revised and extended version of the work that originally appeared in Whitty *et al.* (2023), with the content having been updated and the focus in this paper is an additional analysis that considers the personality of on insider and a deeper dive into the implications for policy.

IP theft may pose a considerable threat to organisations. These insiders gain access to organisations' data, systems and business secrets to steal IP for financial gain or revenge (Cappelli *et al.*, 2012; Nurse *et al.*, 2014; Shaw and Sellers, 2015). Harms include financial, reputational and IP losses (Sarkar, 2010). The economic cost of IP theft has been estimated to be 1%–3% of the gross domestic product of developed countries or approximately US $180bn–US$540bn for the USA (Ciuriak and Ptashkina, 2021).

Little is known about the personality profile of an insider. Often, they are believed to be employees who have become disgruntled with the organisation because of an event, such as missing out on promotion (Shaw *et al.*, 2013); however, research has also found that surprisingly, star employees may be insiders (Whitty, 2021). Concerning personality, although few studies have formally investigated the psychological profile of an insider, researchers have found that malicious insiders often display antisocial behaviours, are entitled and lack empathy (Pfleeger *et al.*, 2010; Shaw *et al.*, 1999).

Artificial intelligence (AI) tools exist to detect insider IP theft, and policies have been developed to prevent it; however, much work is still needed in this space. Tools such as Darktrace, Sureview and Spector 360 create records of employees' digital behaviours and use AI to learn what normal online activities are and deviations from the norm (Nurse *et al.*, 2014). However, these systems are limited because people's behaviour may change (e.g. according to workload or life stressors), and normal may differ according to employee role or cultural change within an organisation (Whitty, 2021). These methods can have a high false-positive rate (Al-Mhiqani *et al.*, 2022). Rule-based solutions for known attacks and anomaly

detection can help improve detection technologies (Liu *et al.*, 2020). However, these systems do not record physical behaviours and psychological states (Whitty, 2021), which have also been found to signify the risk of insider IP theft (Walker-Roberts *et al.*, 2018; Whitty, 2021), nor do they differentiate between attack types (fraud, sabotage and IP theft), which may involve different risk indicators (Cappelli *et al.*, 2012; Whitty, 2021; Whitty *et al.*, 2023).

Researchers have developed critical pathway models to help predict the likelihood that an employee will become a malicious insider (Shaw and Sellers, 2015; Shaw and Stock, 2011; Whitty, 2021). This approach considers predisposing factors, such as personality traits, stressors, concerning behaviours, networks, contextual risk setting and maladaptive organisational responses. Pathway models consider events beyond detecting an anomaly or a series of technical events. Understanding these series of events may better inform policies on detection and prevention rather than having to identify a single trigger point.

1.1 Aims of the paper

This paper has two main objectives: to learn more about the psychological profile of IP theft insiders and to understand the pathways that lead to an attack, considering both technical and physical behaviours. Drawing from our findings, we intend to guide practitioners in developing more effective policies for detecting and preventing IP theft insider attacks. In contrast to qualitative models developed in pathway analysis of insiders, we will examine the interdependencies and statistical connections between behaviours. In this way, we can more precisely predict the likelihood that certain behaviours will lead to an IP theft insider attack.

1.2 Background

The scholarly research on insider threats is rather slim, even more so for IP theft insider cases. According to the available research, insiders are more likely to be men between 20 and 45 years old, with slightly more insiders holding a university qualification (Whitty, 2021). IP theft insiders are typically male employees with an average age of 37 years (Shaw and Stock, 2011; Shaw, 2023). Approximately 65% of employees who commit insider IP theft have already accepted a new job, and those who commit this crime typically steal using their access privileges.

The personality of insiders has been speculated; however, little research has empirically examined the profile of an insider, and none, to our knowledge, has examined the personality of IP theft insiders. The research has focused chiefly on the dark triad, which are antisocial traits including narcissism, Machiavellianism and psychopathy. Dark traits, for instance, have been associated with counterproductive workplace behaviours (O'Boyle *et al.*, 2012). Dark traits, such as antisocial personality disorder, are more evident in a sample of malicious insiders compared with the general population (Liang *et al.*, 2016). These few studies suggest that it may be prudent to learn more about the personality profile of an insider.

The current understanding of the pathway to an IP theft attack is basic. The malicious insider seeks to identify business secrets to steal or has been involved in creating the IP for the organisation; they then move to copy that information (downloading digital devices) and finally leave that organisation, selling the IP or taking it to another organisation (Shaw and Stock, 2011). IP theft is considered challenging to detect or prevent, as the theft appears to occur quickly, with little warning. Insiders leave an organisation before detection (Cappelli *et al.*, 2012; Warren, 2015; Shaw, 2023), which is too late for IP theft.

1.3 The current study and theoretical framework

This research sought to learn more about the psychological profile of an insider and the pathways that lead to an attack. We intend to achieve our objectives by using natural language processing to examine evidence of personality traits and by investigating socio-technical variables evident in

previous IP theft cases and statistically examine their chronological order. Socio-technical means that organisational systems must be understood by bringing together social and technical factors and treating them as interdependent variables of a complex system (Appelbaum, 1997). For example, combining factors, such as tailgating to get into a secure area with misusing a secure system. This approach will help with detection tools, monitoring techniques (technical and human observation) and policy development to prevent and detect threats of IP theft.

For the first part of the study, we drew from the "dark triad", a psychological theory of personality (Paulhus and Williams, 2002). In particular, we focus on Machiavellian traits, which include being cynical, charming and motivated to deceive and manipulate others. People who score high on measures of Machiavellianism are strategic and planful and display a lack of concern with relationships (Paulhus and Williams, 2002). Concerning IP theft, insiders need to deceive their employers and colleagues to covertly steal an organisation's assets and charm potential buyers to sell off these assets secretly. It would be reasonable, therefore, to conjecture that IP theft insiders may score higher than the average population on measures of Machiavellianism.

In addition, Situational Crime Prevention Theory provides a valuable lens through which to examine insider threats and guides the approach taken in this paper (Clarke, 1980). According to the theory, crime may be prevented by removing opportunities for offending, increasing the perceived effort and the risk of being apprehended, reducing anticipated rewards and provocations and removing excuses. Accordingly, we may discover methods to interject or develop policies to make it more difficult for potential IP theft insiders to continue down the predicted pathway to commit these attacks. In line with our objectives, the following research questions were posed:

RQ1. Do IP theft insiders display Machiavellian traits more than the general population?

RQ2. What socio-technical variables are involved in an insider IP theft attack?

RQ3. What are the sequences of behaviours that lead to an insider IP theft attack?

RQ4. How might our findings be used in policy to prevent IP insider theft?

2. Methodology

Before conducting the research, the university ethics committee approved the study (project ID: 33066). We performed a ChatGPT-4 query on 86 insider IP theft case documents to examine Machiavellian traits. To explore the socio-technical variables involved in an insider IP theft attack, we conducted a grounded theory analysis (Strauss and Corbin, 1988) on the same 86 cases of IP theft. To examine the statistical relationships between these variables, we conducted a behaviour sequence analysis (BSA) (Keatley, 2018; Keatley *et al.*, 2019).

2.1 Data

The 86 IP theft cases were identified from online searches of court documents on legal websites. Cases were identified by using the terms "IP theft", "trade secret" or "trade secret theft" in Google searches of news reports and by searching within the U.S. Department of Justice website, using the terms "inurl:justice.gov" alongside the terms "IP theft", "trade secret" or "trade secret theft". Then, court documents were obtained by searching for the insider's name and using the terms "filetype:pdf" or "inurl:courts". Most documents were drawn from the U.S. Department of Justice website (www.justice.gov). However, documents were also sourced from the US Govinfo (www.govinfo.gov), Casetext (www.casetext.com), Justia (www.justia.com), Dokumen (https://dokumen.tips), Cite Case Law (https://cite.case.law) and other legal websites. To ensure anonymity, we de-identified the insiders by referring to each case as a number.

Almost all cases were heard in the USA and at the District Court level, and some were in the US Court of Appeals. Insiders were sentenced to terms of imprisonment in 45 of these cases. These cases occurred between 1985 and 2020; most cases (74 cases, or 86%) were committed between 2004 and 2018. One short description of a case is summarised below:

A 40-year-old military contractor stole the personal identifying information (PII) of active and reserve service members, veterans and their dependents and some civilian personnel. Through collaboration with a network of co-offenders, this PII was then used to re-direct money from personal bank accounts, pensions and disability benefits, and the stolen money was then laundered. The insider, a medical facility employee, obtained the PII by accessing a health record database that included names, social security numbers, military ID numbers, dates of birth, home addresses and other PII. He exfiltrated the PII by photographing his computer screen and distributing the images to his overseas conspirators. The insider's co-offenders used the stolen PII to gain access to further online non-public information. They obtained financial information, and they then altered payments and redirected transactions. The stolen funds were then deposited, withdrawn and sent overseas using an international transfer service. The insider was sentenced to 151 months imprisonment.

2.2 Natural language processing

Large language models (LLMs) have been used to analyse text-based personality recognition tasks (Ji *et al.*, 2023; Rao *et al.*, 2023). In our analysis, quotes made by insiders were manually extracted from the cases. Quotes or directly attributable quotes were not found in 53 of the cases. Four cases were excluded from the analysis due to an insufficiency of quotes. Case 1 was excluded because the quoted text was a letter submitted by the insider to the court during sentencing. Cases 5, 22 and 81 were omitted due to the limited number of quotes detected. In the final data set, 29 cases were included.

For this analysis, we selected the Machiavellianism items developed for the SD4 (Short Dark Tetrad Scale) (Neumann *et al.*, 2022). The ChatGPT-4 query was a zero-shot prompt in that examples of text and responses were not provided; however, akin to previous research, prompting was in the chain-of-thought format (Ji *et al.*, 2023), as it directed the LLM to take a systematic, step-by-step approach to the analysis of each quote. The prompt explained the context, provided the insider's name, included the Machiavellianism items and responses, and requested an overall score and any quotes scoring particularly high on Machiavellianism. The population mean (3.35) and the standard deviation (0.67) for the Machiavellianism scale of the SD4 were used to compare with the sample mean.

2.3 Grounded theory

In line with previous research investigating insider threat (Whitty, 2021), the first phase of our analysis used grounded theory (Strauss and Corbin, 1988). This allows for the development of new theories (inductive analysis) and acknowledges previous theories and hypotheses. Given that much work is needed to uncover the cyber and socio-technical variables involved in IP insider threat, we began our analysis acknowledging previous indicators (MITRE, 2023; Whitty, 2021) but were open to elucidating new ones.

2.4 Behaviour sequence analysis (BSA)

Next, we conducted a behavior sequene analysis (BSA) to investigate pathways to insider IP theft. BSA enables the identification of statistically significant transitions between one behaviour or event and the next and the mapping of these into chronological sequences (Keatley, 2018). BSA enables the identification of behaviours that emerge early in the offending process and is therefore conducive to supporting the prevention of insider IP theft. The method's focus on the

sequence of behaviours or events also offers a means to guide insider IP theft detection in that identifying early indicators of insider behaviours could inform subsequent data collection and analysis. Although not previously applied to analyse the behaviour of insiders – or insider IP theft, more specifically – BSA has been used to examine crimes such as murder (Keatley, 2018).

3. Results

3.1 Natural language processing findings

A one-sample *t*-test was conducted to determine whether the sample mean score for Machiavellianism differed from the population mean. The assumptions were met to carry out a *t*-test. The analysis revealed a significant difference, $t(28) = 4.53$, $p < 0.001$. The sample mean was 3.82 (SD = 0.56). Moreover, the scores showed some variability, and the sample size of 29 is sufficient for statistical inference. A z-score of 0.71 was computed, indicating the sample mean was approximately 0.71 standard deviations above the population mean of 3.35, with a population standard deviation of 0.67. These findings reveal that the average Machiavellianism score for the IP theft insiders was significantly higher than the population mean. ChatGPT-4 assessed the insiders in our sample as significantly more Machiavellian than average, and the sample mean was found to lie within the top 25.78 of population scores.

3.2 Grounded theory analysis findings

Initially, categories were identified and then separated into variables. Actions performed by the insiders were identified as behaviours, and external circumstances (e.g. being arrested) were categorised as events (see Table 1). Many more variables leading up to an insider attack were identified than previously known. Known events were identified from an extensive review of the literature (noting that there is a dearth of literature on this topic due to access to data; see Whitty, 2021 for a review of the literature) including unauthorised access and misuse of the organisation's systems, downloading data and physical behaviours, such as recruiting co-offenders (Cappelli *et al.*, 2012; MITRE, 2023; Shaw and Stock, 2011; Shaw, 2023; Whitty, 2021). Unknown variables included copying data using photography, in-person or electronic discussions that refer to the theft, being approached by a rival organisation, recruiting or trying to recruit a co-offender, travelling overseas, providing data to another government, delivering presentations, especially when the audience included rival companies, taking steps to abscond (e.g. purchasing flights), and discovery after the insider made details of the theft public. Whilst, in hindsight, some of these variables, such as taking photographs, may seem obvious, previous research has not reported these findings.

3.3 Behaviour sequence analysis findings

The BSA provides findings in state transition diagrams, which typically highlight stronger (i.e. those with higher frequency and standardised residual [SR]) pairings in the data. End-users and novice readers can easily interpret these flow-type diagrams. One caveat of the diagrams is to recall that they are underpinned by lag-one analysis – which are pairings of behaviours. While the diagram may appear to show longer sequences of codes (e.g. A → B → C), this would not be the correct way to interpret the diagram. Instead, the diagram should be read as A → B, B → C.

A BSA was applied to the events and behaviours (socio-technical variables) identified in the Grounded Theory Analysis. A state transition diagram was then drawn to illustrate the sequence of behaviours and events in order of occurrence (Figure 1). On the diagram, arrows connecting cells are presented with varying breadth to represent SR scores. These measure the strength of the difference between observed and expected values and reflect the relative likelihood of one behaviour or event preceding another. Broader arrows represent greater SR scores, meaning these connections are more likely to occur (Keatley, 2018). Given that a

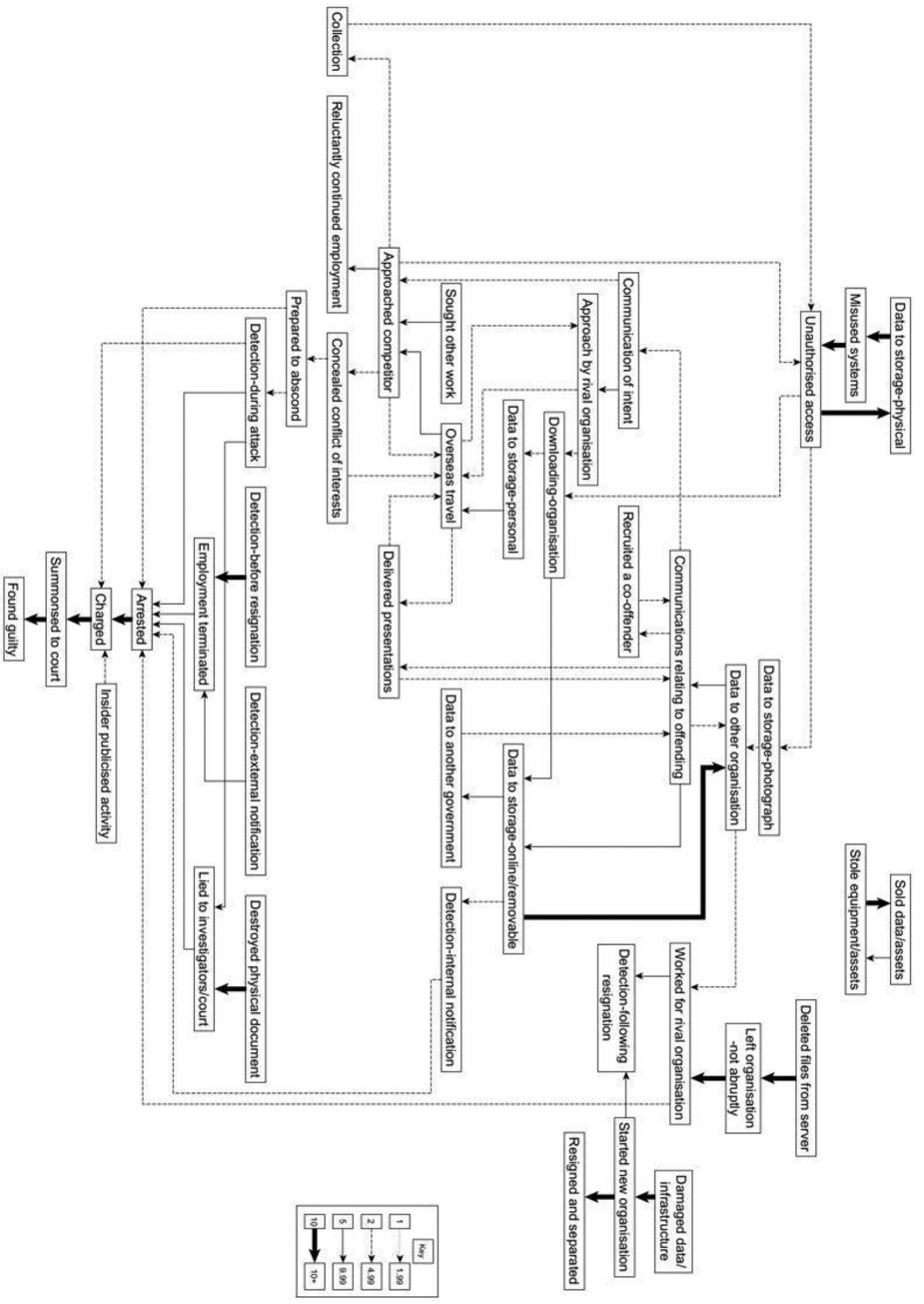
Table 1. Behaviours and events identified through the grounded theory analysis

Behaviour/event	Definition
Approached by rival organisation	Approaches to the insider by another company
Approached competitor	Contact with potential, sponsors or other employers
Arrested	Being detained in relation to the IP theft
Collection	Attempts to gather data of interest to the insider's goal
Concealed conflict of interests	Dishonesty concerning affiliations with another organisation
Communication of intent	Statements referring to future involvement in insider activity
Communications relating to offending	In-person or electronic discussions that refer to the theft
Damaged data/infrastructure	Damage, including manipulating and destroying data
Data to another government	The provision of stolen data to a foreign government
Data to another organisation	Providing the victim organisation's data to another company
Data to storage – online/ removable storage	Moving to online storage or to detachable devices, such as a USB, CD or floppy disk
Data to storage – personal	Movement of data to the insider's own device
Data to storage – photograph	Copying data using photography
Data to storage – physical	Conversion of data to a printed format
Downloading – organisation	Downloading the victim organisation's data using its network
Deleted files from server	Concealment of insider activity through the removal of files
Delivered presentations	Delivering talks or speeches, especially to potential sponsors
Destroyed physical document	Elimination of data in a printed format
Detection – before resignation	Discovery before the insider departure
Detection – during attack	Discovery during the commission of the offense
Detection – external notification	Discovery following advice provided by an outsider
Detected – following resignation	Discovery of the IP theft after the insider had given notice
Detected – internal notification	Discovery based on information from another employee
Employment terminated	Discontinuation of the insider's employment
Found guilty	Being found guilty of wrongdoing in court
Insider publicised activity	Discovery after the insider made details of the theft public
Left organisation – not abruptly	Departing the victim organisation in a typical manner
Lied to investigators/court	Dishonesty during legal or investigative processes
Misused systems	Unauthorised use of the organisation's systems
Overseas travel	Moving outside the country of victim organisation
Prepared to abscond	Taking steps to flee, including by purchasing flights
Recruited co-offender	Involving, or attempting to involve others in the theft
Reluctantly continued employment	Expressions of a desire to depart the victim company, but continuing to work for the victim company
Resigned and separated	Giving notice, then departing the victim organisation
Sold data/assets	Profiting from the organisation's data or assets
Sought other work	Attempts to obtain alternative employment
Started new organisation	Establishing another organisation, especially a competitor
Stole equipment/assets	Theft of an organisation's physical assets
Summoned to court	Being directed to attend court
Unauthorised access	Viewing or using data or systems without permission
Worked for rival organisation	Commencing work with another organisation

Source: Created by authors

complete diagram would include too many nodes and transitions to be interpretable, cut-off criteria were applied and only transitions with SR scores above three were included in the diagram – consistent with the BSA procedure (Keatley, 2018).

The state transition diagram (Figure 1) shows the complexity of IP theft. Contrary to previous understandings of IP theft, there are multiple pathways to consider, which are not all



Source: Created by Authors

Figure 1. State transition diagram of behaviours and events leading to IP theft

linear. For example, approaches to a competitor were an antecedent to overseas travel (n = 4, SR = 3.57), concealment of a conflict of interest (n = 3, SR = 4.78), unauthorised access (n = 6, SR = 3.30) and a sequitur to other behaviours. These include overseas travel (n = 5, SR = 4.99), seeking other employment (n = 4, SR = 7.20) and unauthorised access (n = 4, SR = 2.25). Approaches by a rival organisation were also both antecedents – to overseas travel (n = 3, SR = 4.64) and communications relating to offending (n = 4, SR = 1.92) and a sequitur to behaviours. Notably, the recurrent nature of many behaviours that comprise the pathways also exists.

4. Discussion

This paper reports on personality and socio-technical behaviours evident in IP theft insider attacks. In addition, we investigated the temporal order of these behaviours, the interdependencies between indicators and the statistical likelihood of one preceding another. The work presented here provides a new understanding of the type of person an IP theft insider may present themselves as and the pathways that lead to IP theft attacks. It also suggests new ways forward for policymakers.

Considering *RQ1*, contrary to the bulk of the research on insider threat, our research found that our sample of IP theft insiders did not present as disgruntled but as charming and manipulative. Considering the skills needed to deceive to steal IP and successfully charm others to purchase the IP (also a highly risky activity for the buyer), it makes sense that IP theft insiders may score higher on Machiavellian ratings than the general population.

The Grounded Theory Analysis addressed *RQ2*. This analysis identified socio-technical variables consistent with earlier research (Cappelli *et al.*, 2012; MITRE, 2023; Shaw and Stock, 2011; Whitty, 2021), such as unauthorised access and misuse of the organisation's systems, downloading data and physical behaviours, such as recruiting co-offenders. The downloading of large volumes of data is a variable frequently noted in the literature on IP theft. However, new variables were also found. One of the most interesting new indicators revealed was the use of photography to record IP. In hindsight, these may seem obvious findings, but perhaps due to the absence of research on insider threat, these findings have not been previously reported. This finding has important implications for policy and questions the utility of AI programmes mentioned earlier in this paper (e.g. Darktrace) that rely on analysing online behaviours. Current detection methods would miss an important and necessary indicator.

In addition to concerns about using digital devices to photograph IP, there are other smart devices, including wearables (e.g. smart contact or lenses that can record or wearable cameras), which may also avoid detection. Policies around limits of digital devices in particular zones and increased security access might be a desirable method forward for some organisations; however, they may still not be effective for those with undetectable wearables. For sensitive IP, an investigation into an additional layer of security could be applied, similar to the EURion Constellation used to prevent money from being photocopied (Sriman *et al.*, 2023).

Other new socio-technical variables identified in our study included communications referring to details of the IP theft, travelling overseas, approaches to different organisations and the delivery of presentations. It would be unlikely that AI tools would pick up some of these behaviours. Policies around travel may involve stricter protocols (e.g. consideration of a detailed itinerary, frequency of travel, country of travel with attention to sanction lists and job role). It may be necessary to partner co-workers in travel to prevent opportunities to meet with potential co-offenders.

To our knowledge, previous work has yet to identify the delivery of presentations in the pathway to an IP insider attack. This may be because the few available IP insider studies have focused on what occurs in the place of work and how IP might travel via digital devices. Moreover, our work challenges the assumption that malicious insiders find new employment and bring the IP of other organisations unknown to that organisation (Cappelli *et al.*, 2012; Collins *et al.*, 2013). Our study also uniquely revealed that insiders work hard to find buyers for their stolen IP, sometimes

travelling several times overseas to sell the organisation's IPs. These findings provide new insights into preventing and discovering IP theft before it is too late.

The BSA addressed *RQ3*. This analysis highlighted that multiple and complex pathways (which include physical and cyber events) are involved in insider IP theft and that not all paths are linear. Akin to previous research (Cappelli *et al.*, 2012; Maloof *et al.*, 2007; Shaw and Stock, 2011), we found that the pathway of data stored to physical (i.e. printed out) led to misused systems, which further led to unauthorised access (probably to acquire IP the insider did not have access to). This path then returns to the storing of data on digital devices. This finding highlights the importance of detecting unauthorised access, which many organisations already undertake (Liu *et al.*, 2020), but also demonstrates that once this is identified, there are additional physical indicators to monitor in IP theft, such as employees approaching competitors and travelling overseas. Notably, in many of these cases, the employee remained in the organisation after the initial IP was stolen, and then they continued to steal IP. This contradicts previous research, which suggests that once IP is stolen, the employee abruptly leaves that organisation (Cappelli *et al.*, 2012; Nurse *et al.*, 2014; Shaw and Sellers, 2015; Whitty, 2021). The BSA also revealed that some IP insiders join an organisation intending to steal IP, which is consistent with previous research (Cappelli *et al.*, 2012; Nurse *et al.*, 2014; Shaw and Sellers, 2015; Whitty, 2021).

The BSA highlighted some unique and recurrent pathways not identified in previous research. For example, we found that communications related to offending led down various pathways to eventually communicate with rival organisations (that the insider sought, or organisations sought them), travel overseas, and conduct presentations. Whilst some of these behaviours may be difficult to detect, if earlier suspicious digital behaviours are observed combined with travel, an organisation might be concerned that they have an IP theft insider.

Taking the Grounded Theory and the BSA findings together, our work confirmed the importance of some indicators already used in detection, such as unauthorised access and downloading data. We also revealed new indicators (e.g. communications with externals to sell the IP). These variables are essential in any anomaly detection. However, in contrast to previous work, our findings provide strong evidence for using rule-based solutions for known attacks. It is important to go beyond seeking out stand-alone events and consider sequences of events. Based on our findings, algorithms may be refined to incorporate cyber indicators; however, without including physical events (e.g. travel, photographs), the prediction will be undeniably weaker.

When addressing *RQ4*, we contend that it is helpful to consider the Situational Crime Prevention Theory described earlier in this paper (Clarke, 1980). As a reminder, this theory suggests that crime may be prevented by removing opportunities for offending, increasing the perceived effort and the risk of being apprehended, reducing anticipated rewards and provocations, and removing excuses (Clarke, 1980). Our study identified multiple opportunities that could be closed down to prevent IP theft, and organisations may wish to be up-front about the tools they use and the monitoring carried out to detect this attack. Pointing this out may increase the perceived risk of stealing and selling on IP.

Notably, our paper highlighted technical and physical behaviours of concern that could help reduce the risk of an IP theft attack. Some of the technical behaviours that occurred on digital devices owned by the insider (e.g. communications, downloads, taking photographs of the IP) were most likely conducted to avoid detection. If organisations are very concerned about IP theft, they may decide to create policies around personal devices in the workplace. Some physical actions could be considered in policy to help prevent IP theft. For example, we learnt that insiders travelled overseas to meet potential rival organisations and conduct presentations. As stated above, policies may be developed around travel (e.g. travelling with co-workers and restricting countries employees might travel around for work). This might remove opportunities for insiders to meet potential buyers of the IP they have stolen.

Furthermore, our research revealed a cluster of insiders who deliberately joined an organisation to steal IP. Organisations concerned about IP theft may use more stringent vetting procedures to help prevent malicious insiders from entering their workplaces. Although this may be an additional cost to an organisation, it may well prevent much higher costs.

5. Conclusions

This paper's contribution to the field is more than a set of findings. We offer a new framework for understanding and studying insider threats. The work has elucidated aspects of the IP theft insider's personality. Moreover, scholars and organisations may no longer approach these threats as a simple linear pathway. The attacks can be multiple. As the analysis showed, numerous attempts were made in arguably non-subtle ways to steal and sell IP.

Contrary to what is generally accepted, many IP insiders sometimes sell portions of IP over time and/or to multiple buyers. This paper demonstrates the need for a multidisciplinary approach to investigating IP theft. It highlights the importance of considering psychological behaviours and methods (Taylor and Whitty, 2023) to examine these threats.

Practically speaking, the current research has important implications for designing systems that monitor malicious behaviour within organisations. Our findings align with previous frameworks of malicious insider threat that focus on a range of socio-technical indicators and integrate such data continuously (e.g. Greitzer *et al.*, 2018; Whitty, 2021). However, the attention to detail in our work – combining grounded theory analysis with BSA – has identified many more previously unknown variables in predictable patterns.

The monitoring of variables cannot be limited to log analysis of information security (IS) system behaviour, where the focus is on events such as policy violations, abnormal search behaviours and the modification, deletion or inappropriate access to files on the network (Costa *et al.*, 2016). Our research demonstrates that monitoring user behaviour to predict insider risk must include personnel security (Lang, 2022) and staying abreast of emerging technologies that insiders may exploit. Our research highlights the importance of personnel vetting, which includes aspects such as reporting suspicious behaviours and changes of circumstances and capturing data unavailable through log analysis and, which, as mentioned above, play a role in the sequences of behaviours of the IS attacks. As outlined in our data, this included behaviour such as overseas travel, particularly when this involves presentations to competitors or at venues when competitors are present. Such data needs to be integrated with traditional log analysis to identify the kinds of sequences of behaviours uncovered in this study that serve as indicators of impending insider attacks.

Contrary to typical vetting approaches, personnel vetting must also be continuous rather than solely reliant on scheduled security reviews of an individual (e.g. annual security appraisals). This approach, known as continuous evaluation, includes reviews of individuals at any time during the period of eligibility and involves monitoring the output from a range of business rules, automated checks and assessments (Luckey *et al.*, 2019). The results of our study showed that because time is crucial in the analysis of insider behaviour, more than annual appraisals may be needed to detect insiders intending to steal IP. Having passed the initial vetting process and without continuous monitoring, such actors may be able to operate relatively unchecked until the next security appraisal is due.

There are a few significant limitations to note. Firstly, this is one sample of IP theft cases, all discovered by the organisations that went to court. Many IP theft cases are potentially undiscovered, and of those that do, not all go to court (especially for organisations who believe it is a risk for the public to learn about their stolen IP). In addition, our study only focused on one aspect of personality, Machiavellianism; further analyses may reveal other indicative traits. Also, our work did not consider the psychological profiles, psychological

concerns (e.g. stressors) and organisational stressors examined in previous studies (Sarkar, 2010; Shaw and Stock, 2011; Whitty, 2021).

Despite the limitations, the methods used should be considered by scholars in their research and employed in organisations to improve the detection and prevention of IP insider threats. The work presents a new way of considering pathway models for insider threats. It proposes a new theoretical understanding – that insider threats may be (at least for IP theft) non-linear and complex.

References

Al-Mhiqani, M.N., Ahmad, R., Abidin, Z.Z., Abdulkareem, K.H., Mohammed, M.A., Gupta, D. and Shankar, K. (2022), "A new intelligent multilayer framework for insider threat detection", *Computers and Electrical Engineering*, Vol. 97, pp. 1-23, doi: 10.1016/j.compeleceng.2021.107597.

Appelbaum, S.H. (1997), "Socio-technical systems theory: an intervention strategy for organizational development", *Management Decision*, Vol. 35 No. 6, pp. 452-463, doi: 10.1108/00251749710173823.

Cappelli, D.M., Moore, A.P. and Trzeciak, R.F. (2012), *The CERT Guide to Insider Threats: how to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)*, Addison-Wesley, Upper Saddle River, NJ.

Ciuriak, D. and Ptashkina, M. (2021), "Quantifying trade secret theft: policy implications", *SSRN Electronic Journal*, Vol. 253, pp. 1-18, doi: 10.2139/ssrn.3706511.

Clarke, R.V. (1980), "Situational crime prevention: theory and practice", *The British Journal of Criminology*, Vol. 20 No. 2, pp. 136-147, doi: 10.1093/oxfordjournals.bjc.a047153.

Collins, M.L., Spooner, D., Cappelli, D.M., Moore, A.P. and Treciak, R. (2013), "Spotlight on: insider theft of intellectual property inside the United States involving foreign governments or organizations", Software Engineering Institute, CERT Division, Carnegie Mellon University, MA, doi: 10.1184/R1/6584291.v1.

Colwill, C. (2009), "Human factors in information security: the insider threat – who can you trust these days?", *Information Security Technical Report*, Vol. 14 No. 4, pp. 186-196.

Costa, D.L., Albrethsen, M.J., Collins, M.L., Perl, S.J., Silowash, G.J. and Spooner, D.L. (2016), *An Insider Threat Indicator Ontology*, Carnegie-Mellon University, Pittsburgh PA.

Greitzer, F.L., Purl, J., Leong, Y.M. and Becker, D.S. (2018), "Sofit: sociotechnical and organizational factors for insider threat", IEEE Symposium on Security and Privacy Workshops, pp. 197-206, doi:10.1109/spw.2018.00035.

Ji, Y., Wu, W., Zheng, H., Hu, Y., Chen, X. and He, L. (2023), "Is ChatGPT a good personality recognizer? A preliminary study", arXiv preprint arXiv: 2307.03952, doi: 10.48550/arXiv.2307.03952.

Keatley, D. (2018), *Pathways in Crime: An Introduction to Behaviour Sequence Analysis*, Springer, Tunbridge Wells, doi: 10.1007/978-3-319-75226-6.

Keatley, D.A., Sheridan, L. and Whitty, M.T. (2019), "'The road not taken': understanding and mapping complexity in threat assessment", *Journal of Threat Assessment and Management*, Vol. 6 Nos 3/4, pp. 198-201, doi: 10.1037/tam0000132.

Lang, E.L. (2022), "Seven (science-based) commandments for understanding and countering insider threats", *Counter-Insider Threat Research and Practice*, Vol. 1 No. 1, available at: https://citrap.scholasticahq.com/article/37321-seven-science-based-commandments-for-understanding-and-countering-insider-threats (accessed 2 April 2023).

Liang, N., Biros, D.P. and Luse, A. (2016), "An empirical validation of malicious insider characteristics", *Journal of Management Information Systems*, Vol. 33 No. 2, pp. 361-392, doi: 10.1080/07421222.2016.1205925.

Liu, M., Li, M., Sun, D., Shi, Z., Lv, B. and Liu, P. (2020), "Terminator: a data-level hybrid framework for intellectual property theft detection and prevention", CF'20: Proceedings of the 17th ACM International Conference on Computing Frontiers, pp.142-149, doi: 10.1145/3387902.3392329.

Luckey, D., Stebbins, D., Orrie, R., Rebhan, E., Bhatt, S.D. and Beaghley, S. (2019), "Assessing continuous evaluation approaches for insider threats", RAND Corporation, available at: www.rand.org/pubs/research_reports/RR2684.html (accessed 2 April 2023).

Maloof, M.A., Stephens, M. and Elicit, G.D. (2007), "A system for detecting insiders who violate need-to-know", *Recent Advances in Intrusion Detection, 10th International Symposium, RAID, Gold Coast, Australia, September 5-7, 2007*, Proceedings 10, pp. 146-166, doi:10.1007/978-3-540-74320-0_8.

MITRE (2023), "ATT&CK matrix for enterprise", available at: https://attack.mitre.org/matrices/enterprise (accessed 2 April 2023).

Neumann, C.S., Jones, D.N. and Paulhus, D.L. (2022), "Examining the short dark tetrad (SD4) across models, correlates, and gender", *Assessment*, Vol. 29 No. 4, pp. 651-667, doi: 10.1177/1073191120986624.

Nurse, J.R., Legg, P.A., Buckley, O., Agrafiotis, I., Wright, G., Whitty, M., Upton, D., Goldsmith, M. and Creese, S. (2014), "A critical reflection on the threat from human insiders – its nature, industry, perceptions, and detection approaches", *International Conference on Human Aspects of Information Security, Privacy, and Trust*, pp. 270-281, doi:10.1007/978-3-319-07620-1_24.

O'Boyle, E.H., Forsyth, D.R., Banks, G.C. and McDaniel, M.A. (2012), "A meta-analysis of the Dark Triad and work behavior: a social exchange perspective", *Journal of Applied Psychology*, Vol. 97 No. 3, pp. 557-579, doi: 10.1037/a0025679.

Paulhus, D. and Williams, K.M. (2002), "The Dark Triad of personality: narcissism, Machiavellianism and psychopathy", *Journal of Research in Personality*, Vol. 36 No. 6, pp. 556-563, doi: 10.1016/S0092-6566(02)00505-6.

Pfleeger, S.L., Predd, J.B., Hunker, J. and Bulford, C. (2010), "Insiders behaving badly: addressing bad actors and their actions", *IEEE Transactions on Information Forensics and Security*, Vol. 5 No. 1, pp. 169-179.

Rao, H., Leung, C. and Miao, C. (2023), "Can ChatGPT assess human personalities? A general evaluation framework", arXiv preprint arXiv:2303.01248, doi: 10.48550/arXiv.2303.01248.

Sarkar, K.R. (2010), "Assessing insider threats to information security using technical, behavioural and organization measures", *Information Security Technical Report*, Vol. 15 No. 3, pp. 112-133, doi: 10.1016/j.istr.2010.11.002.

Shaw, E.D. (2023), *The Psychology of Insider Risk: Detection, Investigation and Case Management*, CRC Press: Taylor & Francis Group, Boca Raton, doi: 10.1201/9781003388104.

Shaw, E.D. and Sellers, L. (2015), "Application of the critical-path method to evaluate insider risk", *Studies in Intelligence*, Vol. 59, pp. 1-8, available at: https://cyberwar.nl/d/fromCryptome/cia-cpm-insider-risks.pdf

Shaw, E.D. and Stock, H.V. (2011), "Behavioral risk indicators of malicious insider theft of intellectual property: misreading the writing on the wall", White Paper, Symantec, Mountain View, CA.

Shaw, E.D., Post, J.M. and Ruby, K.G. (1999), "Inside the mind of the insider", *Security Management*, Vol. 43, pp. 34-44, available at: link.gale.com/apps/doc/A58451092/AONE?u=monash&sid=bookmark-AONE&xid=77dc0fb7

Shaw, E., Payri, M., Cohn, M. and Shaw, I. (2013), "How often is employee anger an insider risk I? Detecting and measuring negative sentiment versus insider risk on digital communications", *Journal of Digital Forensics, Security and Law*, Vol. 8 No. 1, pp. 39-71, doi: 10.15394/jdfsl.2013.1140.

Sriman, B., Silviya, S.H.A., Anitham, R., Pandithural, O., Shriram, S.K. and Sathishkumar, R. (2023), "Combatting counterfeit currency: the power of EURion constellation and other anti-fraud measures", *International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI)*, pp.1-7, doi: 10.1109/ACCAI58221.2023.10200363.

Strauss, A. and Corbin, J. (1988), *Basics of Qualitative Research: Grounded Theory Procedures and Technique*, Sage, London.

Taylor, J. and Whitty, M. (2023), "An exploration of the awareness and attitudes of psychology students regarding their psychological literacy for working in the fields of psychology and cyber security", *Psychology Learning and Teaching*, Vol. 23 No. 2, pp. 298-314, doi: 10.1177/14757257231214612.

Tomazin, F. (2023), "Global intelligence chiefs last China's 'sanctioned' theft of intellectual property", The Sydney Morning Herald, 18 October, available at: www.smh.com.au/world/north-america/global-intelligence-chiefs-lash-china-s-sanctioned-theft-of-intellectual-property-20231018-p5ed3f.html

Walker-Roberts, S., Hammoudeh, M. and Dehghantanha, A. (2018), "A systematic review of the availability and efficacy of countermeasures to internal threats in healthcare critical infrastructure", *IEEE Access*, Vol. 6, pp. 25167-25177, doi: 10.1109/access.2018.2817560.

Warren, M. (2015), "Modern IP theft and insider threat", *Computer Fraud & Security*, Vol. 2015 No. 6, pp. 5-10, doi: 10.1016/s1361-3723(15)30056-7.

Wei, Z., Rauf, U. and Watcher, F.E. (2024), "E-watch: insider threat monitoring and detection for enhance security", *Annals of Telecommunications*, doi: 10.1007/s12243-024-01023-7.

Whitty, M.T. (2021), "Developing a conceptual model for insider threat", *Journal of Management and Organization*, Vol. 27 No. 5, pp. 911-929, doi: 10.1017/jmo.2018.57.

Whitty, M.T., Ruddy, C. and Keatley, D.A. (2023), "To catch a thief: examining socio-technical variables and developing a pathway framework for IP theft insider attacks", in Furnell, S., Clarke, N. (Eds). *Human Aspects of Information Security and Assurance*, *HAISA 2023*, IFIP Advances in Information and Communication Technology, Springer Nature, Cham, Vol. 674, pp. 377-390, doi: 10.1007/978-3-031-38530-8_30.

Further reading

Ahmad, A., Maynard, S.B., Desouza, K.C., Kotsias, J., Whitty, M.T. and Baskerville, R.L. (2021), "How can organizations develop situational awareness for incident response: an exploratory case study and process model of situation awareness", *Computers and Security*, Vol. 101, pp. 1-15, doi: 10.1016/j.cose.2020.102122.

Ahmad, A., Desouza, K., Maynard, S.B., Whitty, M., Kotsias, J. and Baskerville, R.L. (2020), "Situational-awareness in incident response: an in-depth case study and process model", *ICIS 2020 Proceedings*, Vol. 1, pp. 1-9, available at: https://aisel.aisnet.org/icis2020/cyber_security_privacy/cyber_security_privacy/1/

Frishammar, J., Ericsson, K. and Patel, P.C. (2015), "The dark side of knowledge transfer: exploring knowledge leakage in joint R&D projects", *Technovation*, Vols 41/42, pp. 75-88, doi: 10.1016/j.technovation.2015.01.001.

Knerler, K., Parker, I. and Zimmerman, C. (2022), "11 Strategies of a World-Class Cybersecurity Operations Centre", MITRE, MA, available at: mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf (accessed 2 April 2023).

Nguyen, M.T., Truong, L.H., Tran, T.T. and Chien, C.-F. (2020), "Artificial intelligence based data processing algorithm for video surveillance to empower industry 3.5", *Computers and Industrial Engineering*, Vol. 148, pp. 1-15, doi: 10.1016/j.cie.2020.106671.

Willison, R. and Siponen, M. (2009), "Overcoming the insider: reducing employee crime through situational crime prevention", *Communications of the ACM*, Vol. 52 No. 9, pp. 133-137, doi: 10.1145/1562164.1562198.

Corresponding author
Monica Therese Whitty can be contacted at: Monica.Whitty@monash.edu