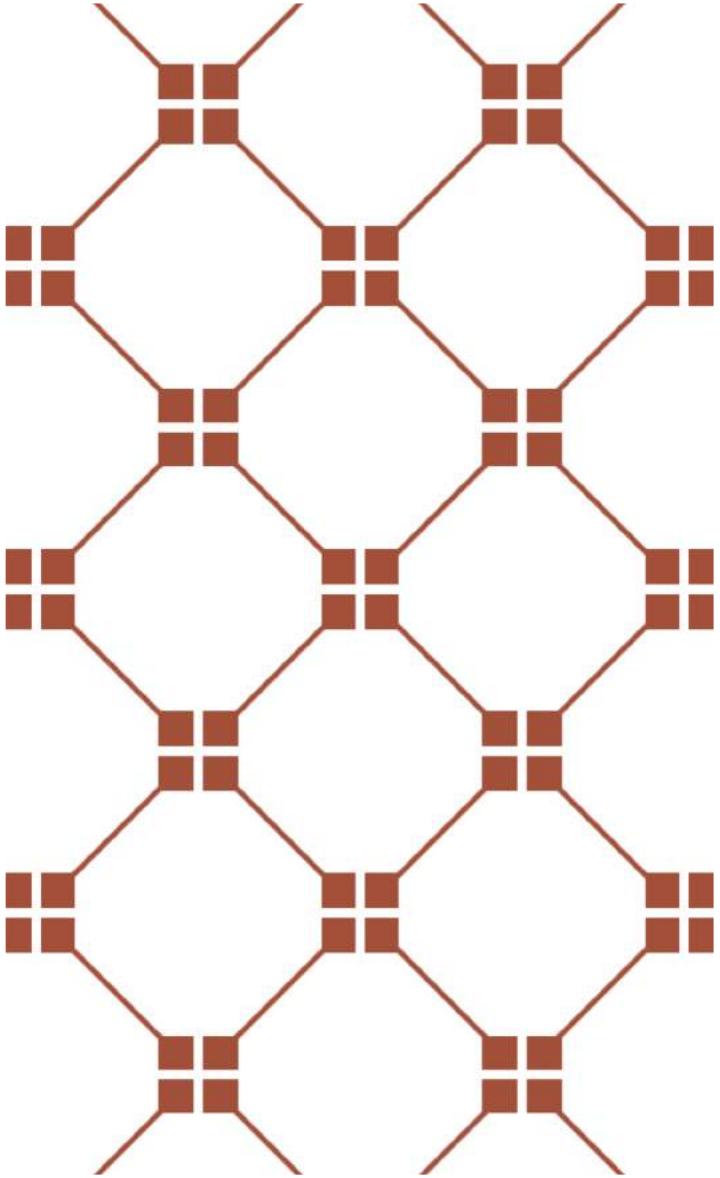
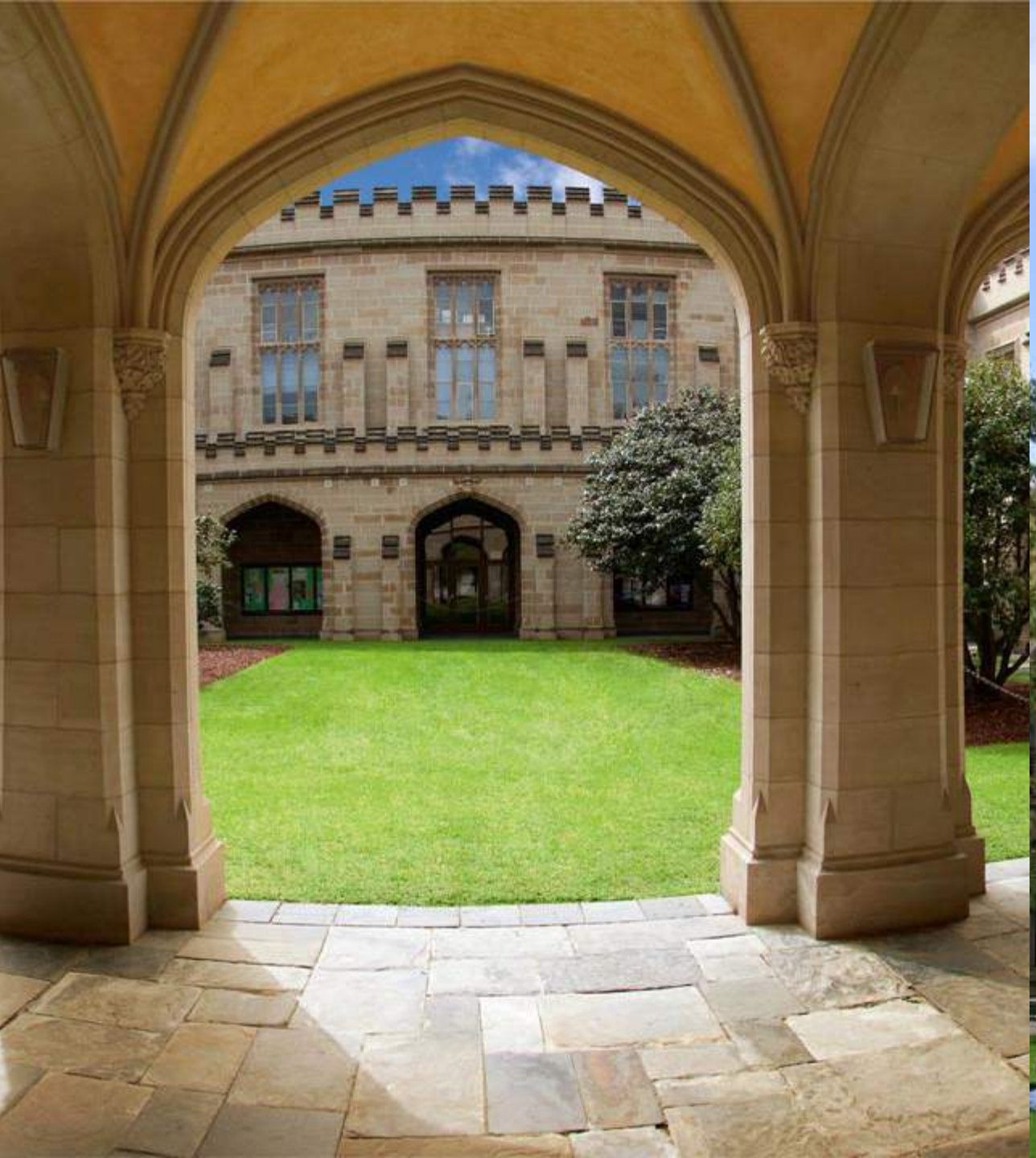


DEVELOPING A CONCEPTUAL MODEL FOR INSIDER THREAT

Monica Whitty
University of Melbourne



DEFINITION OF AN INSIDER

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

- Theft
- IP theft – e.g., 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
- Password cracking

HARM CAUSED BY INSIDER THREAT

- Loss of monies
- Reputational harm
- Harm to employees
- Harm to clients
- Security to individuals/organisations/society
- National Infrastructure

CHELSEA (BRADLEY) MANNING, JULIAN ASSANGE, EDWARD SNOWDEN

Whistleblower or insider threat?

DEMOGRAPHIC DETAILS

- Men – 20-45 years
- Full-time permanent staff (88%, CPNI, 2013)
- Customer facing (20%, CPNI, 2013)
- Financial (11%, CPNI, 2013)
- Security staff (11%, CPNI, 2013)
- University graduates (58%, CPNI, 2013)

Job roles:

- Managerial (45%, CPNI, 2013)
- Non-managerial (49%, CPNI, 2013)

INSIDER THREAT, FRAUD

- Average insider = 30 years
- Age range 21-20 years.
- Men/Women = 60/40 split (akin to working population)

cifas
Leaders in fraud prevention

SHAW & STOCK (2011): IP THEFT

- Average age = 37 years
- Employed in technical positions
- 65 % who committed an insider attack had already accepted a new job

Difficult to detect on demographic details alone!

DISPOSITIONAL INDICATORS

- Self-centredness, arrogance, risk-taking, manipulative, coldness, narcissism, self-deception and defensiveness (Turner & Gelles, 2003).
- 120 cases: 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 (CPNI, 2013).
- IP theft: antisocial traits, difficulties getting along with others, being above the rules, impulsivity, tendency to blame others, ambitious, and greedy (Shaw & Stock, 2011).

IP theft: Volume of printing (Malood & Stephens, 2007).

Emotional state, such as depressed, stressed (e.g., Shaw & Stock, 2011; Turner & Gelles, 2003).

Hypothetical situations – language change + negative affect (Taylor et al., 2013)

Difficult to pick up alone!

BEHAVIOURAL INDICATORS

RESEARCH OBJECTIVES

1. Examine which psychological, behavioural, and social variables (in both the physical and cyber realms) are important when identifying potential insider attackers.
2. Examine the potential pathways that might lead to an attack.

METHOD

Case study methodology – 99 collected

Attack took place within the year prior to the interviews taking place

Semi-structured interview with – managers, fellow employees, HR personnel, heads of security and their teams, law enforcement officers.

Interviewed about: the job role of the insider; their general behaviour in the workplace, prior to and after the attack; their observations regarding the person's personality and behaviour; the person's circumstances prior to 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.

- Financial sector
- Retail sector
- Public sector
- Telecommunications providers
- High school
- Labourer business
- Insurance provider
- Courier business
- Nursery
- Warehouse
- Prison

ORGANISATIONS

TYPE OF INSIDER ATTACK

- Fraud (80%)
- Reputational damage (7%)
- Theft (7%)
- IP/data theft (6%)
- Identity theft (3%)
- Money laundering (2%)
- Procurement fraud (2%)
- Working illegally (1%)
- 10% of cases involved more than one type of insider attack

INSIDERS

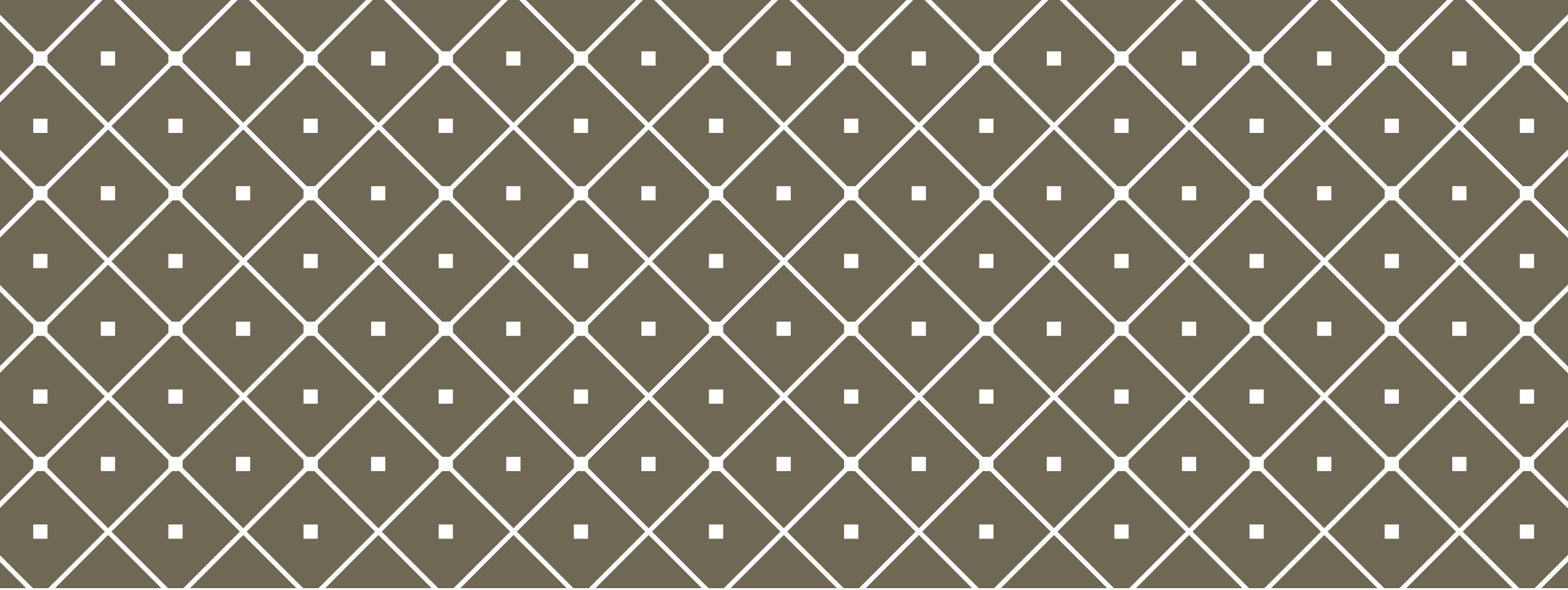
In most cases there was a person working in isolation (68%); however, 32% of the cases involved a group (some of which included outsiders).

In 50% of the cases the insider received a custodial sentence, 13% received a community service order and 15% received a suspended sentence.

Eighty-eight per cent of the insiders where dismissed and 3% resigned.

Sixty-two per cent of the insiders where male and 38% were female, with ages ranging from 19-62 years ($M = 31.39$ years).

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 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



DESCRIPTON OF INSIDER

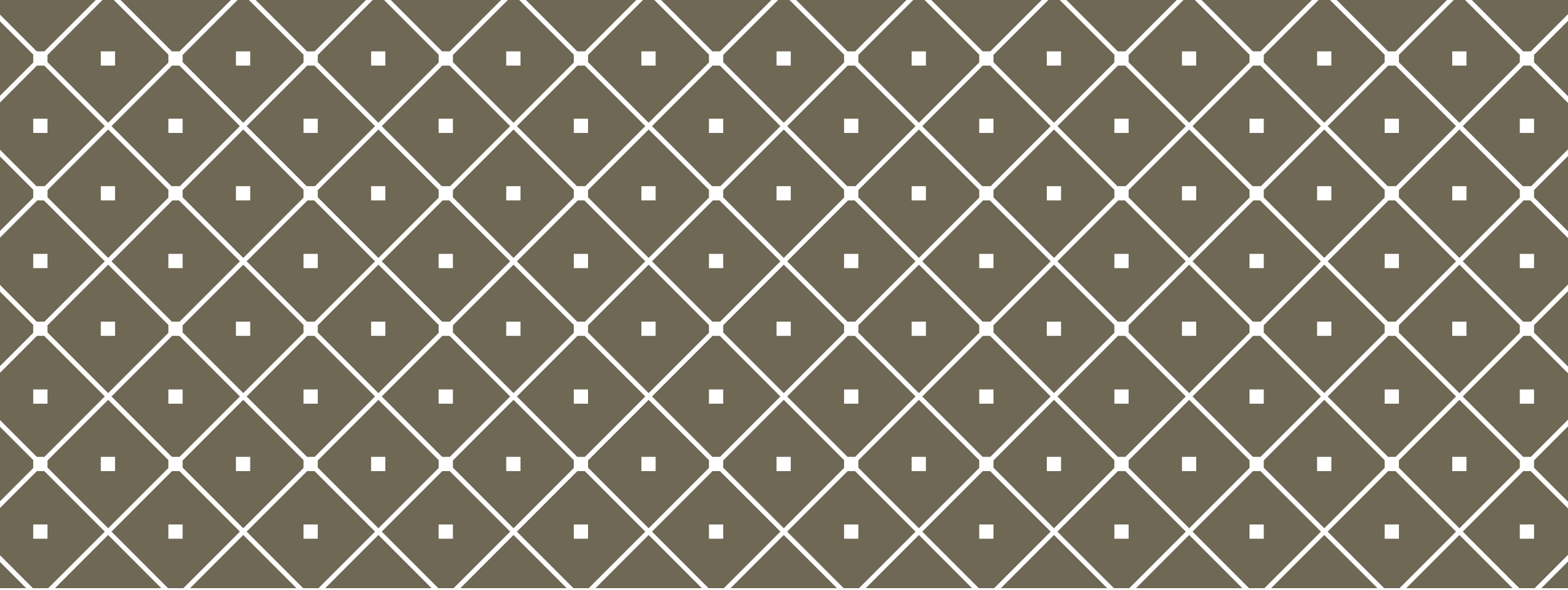
External locus of control	**Fatalist view of the world, believing that events that happen are out of their control.**	**2**
Open to flattery	Open to flattery and being coerced by others (e.g., conned into a romantic relationship).	2
Life circumstances and actions prior to employment		
Gang membership	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 prior to 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	Prior to 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 prior to 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**
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

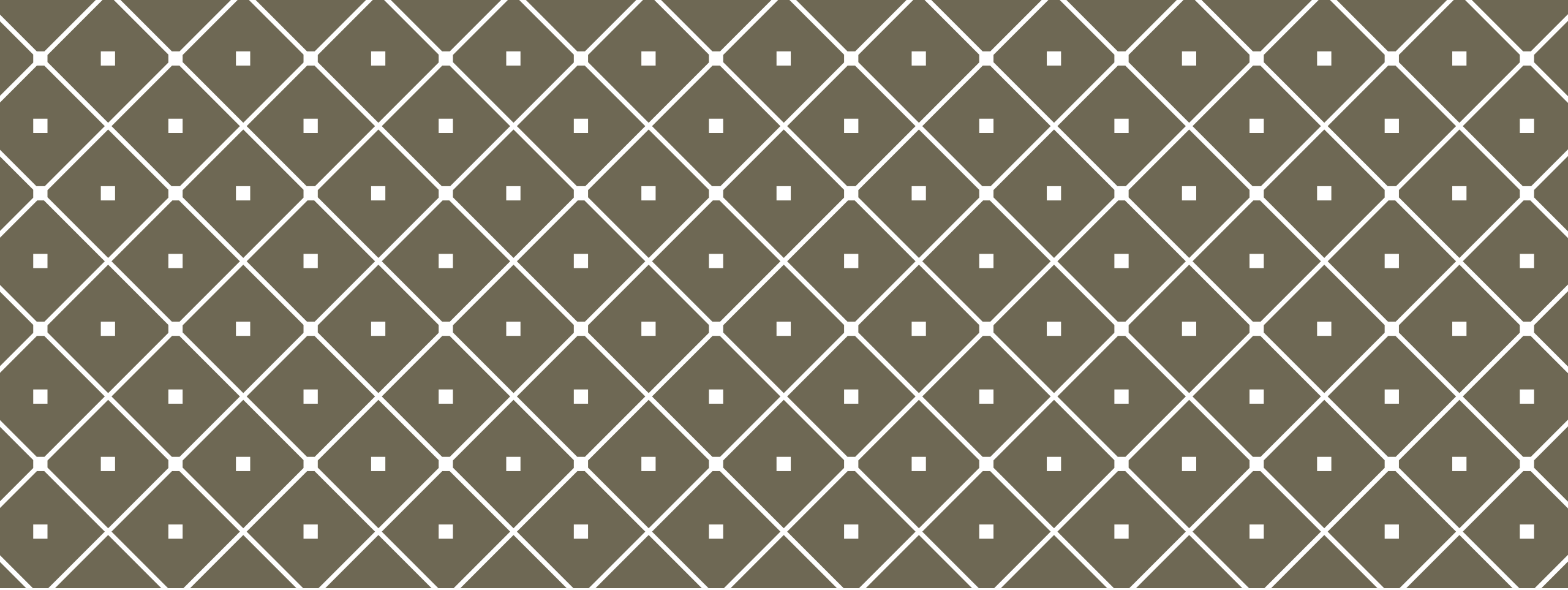
Unusual hours	**Turning up to work or leaving at times different to those required or expected and/or different compared with employees in similar roles. Taking longer breaks than permitted.**	**4**
Downloading large volumes of data	Downloading large volumes of data and/or emailing large volumes of data	3
Star employee – not meeting targets	A talented, well-regarded employee ceases to meet targets and displays signs of distress.	3
Absentee	Frequently taking time off work.	3



MOTIVATION

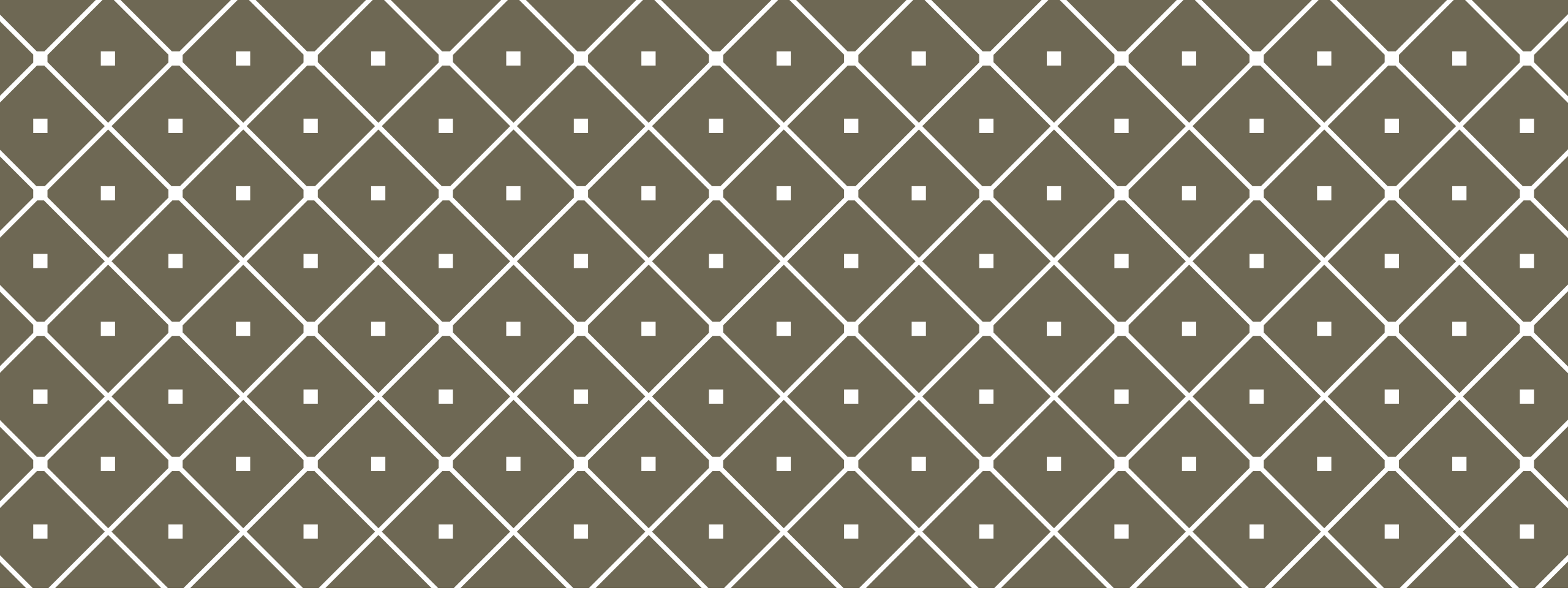
Motivation	Description	%
Greed/Living beyond their means	Intense and selfish desire to acquire wealth. Need money to support their lifestyle and pay-off debts (not acquired from addiction).	55
Need to support an addiction	Money needed to support addiction and/or pay-off insurmountable debt accrued from 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



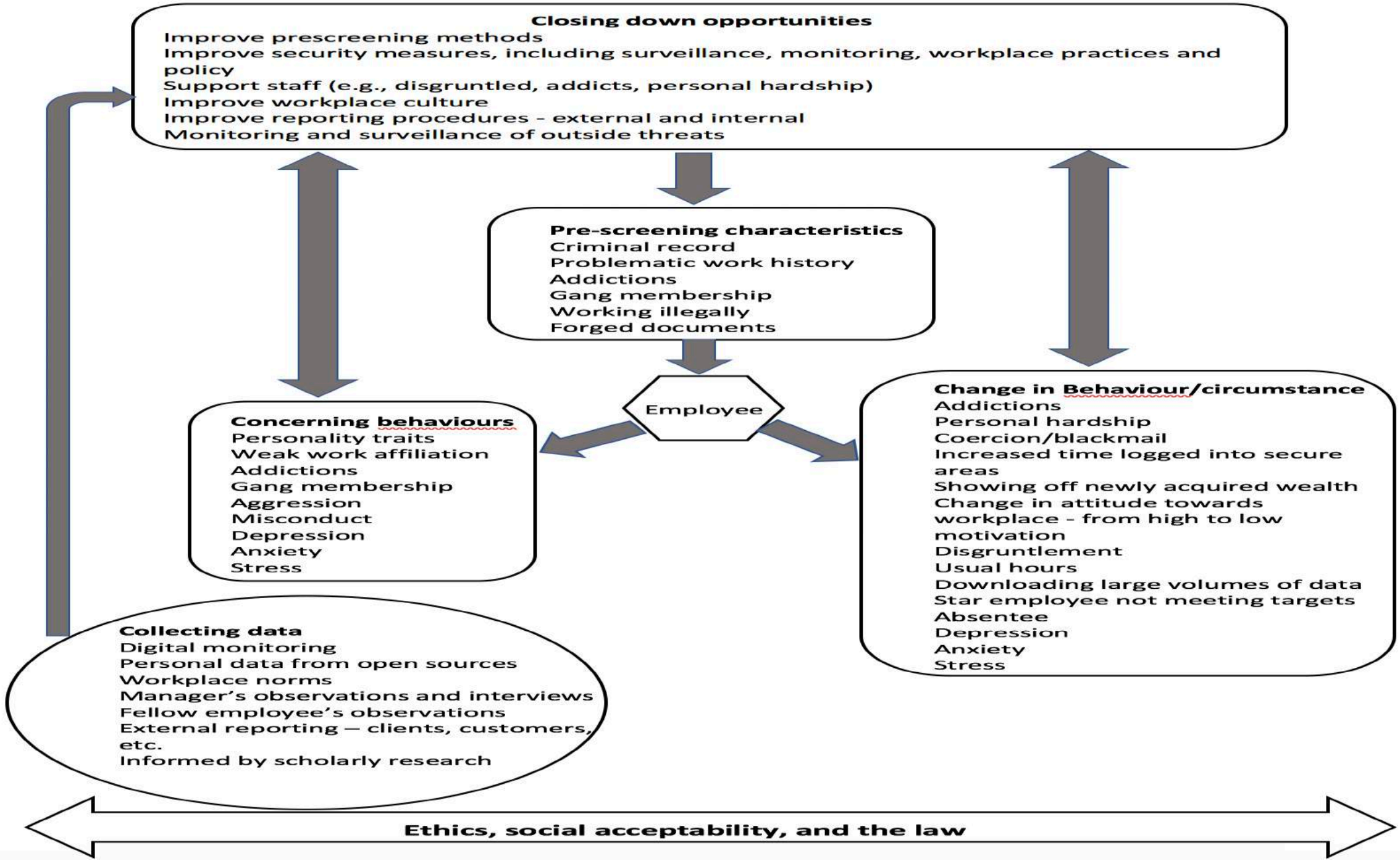
OPPOTUNITY

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



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


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

REFERENCE

Whitty, M. T. (in press). Developing a conceptual model for insider threat. *Journal of Management & Organization*.