Australian Government
Australian Institute of Criminology

29th Cambridge Symposium 2011

Penetration of Financial and Commercial Organisations by Criminals and Terrorists

Dr Russell G Smith
Principal Criminologist

Penetration typologies

Overt penetration

- ***Remote*** – Ram-rading *(e.g. ATM attacks)*
- ***Proximal*** – Taking cash, documents and information *(e.g. insider theft)*

Covert penetration

Remote penetration

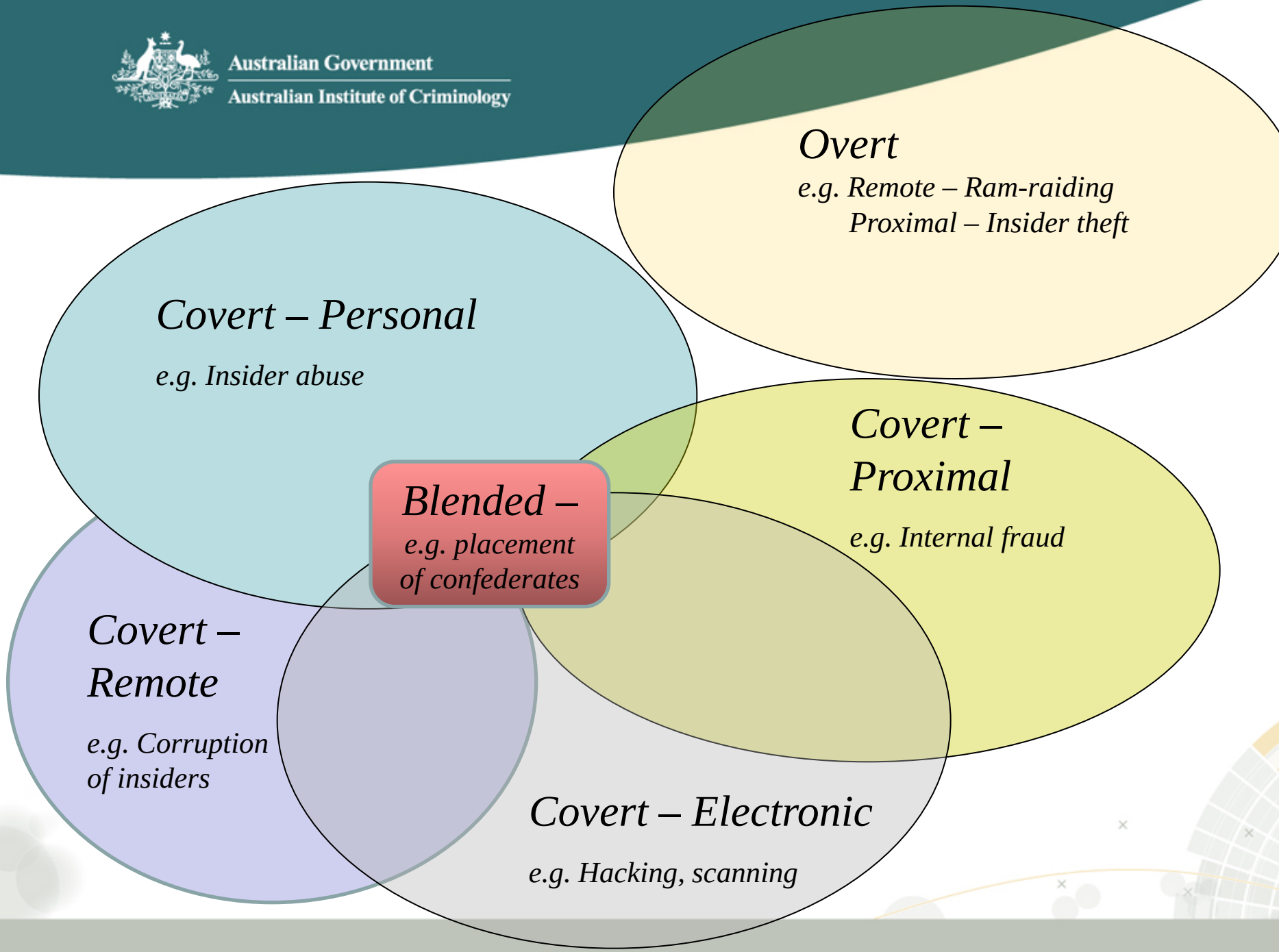
- Personal – corruption of insiders *(e.g. bribery, kickbacks)*
- Electronic – remote scanning; hacking into networks *(e.g. scanning PINs)*

Proximal penetration

- Personal – insider abuse *(e.g. employee fraud, contractor fraud – World Bank)*
- Electronic – misuse of access privileges *(e.g. password abuse)*

Blended penetration

- Personal – placement of confederates within banks *(e.g. ANZ Bank case)*
- Electronic – placement of trojans *(e.g. malware, keylogging)*


Overt
e.g. Remote – Ram-raiding
Proximal – Insider theft
Covert – Personal
e.g. Insider abuse
Covert – Proximal
e.g. Internal fraud
Blended –
e.g. placement of confederates
Covert – Remote
e.g. Corruption of insiders
Covert – Electronic
e.g. Hacking, scanning

Criminological explanations

Crime is 'where the money is' (Willie Sutton)

- *Internal* – cash, account information, internal security weaknesses
- *External* – electronic banking, customer information, staff weaknesses

Routine activity theory

- Cohen & Felson (1979) – predatory crime depends on the presence of (*financially*) motivated offenders, suitable targets (*banks*), and the absence of capable guardians (*regulators*)
- Assumes that offenders undertake 'rational choice decision-making'

Displacement risks

- *. . . A change in offender behaviour, along illegitimate means, which is designed to circumvent either a specific preventive measure or more general conditions unfavourable to the offender's usual model of operating* (Gabor 1990)
- If security is perceived to be an effective barrier, then corruption of insiders and placement of confederates will be employed

Australian Government
Australian Institute of Criminology

Operation Hickey

Identity Security Strike Team Operation

- Multi-agency investigation starting in February 2006
- 20 offenders arrested for organised identity fraud syndicate activities

Modus Operandi *(personal, remote, covert penetration)*

- Forgery of 7,000 identification documents
- Take-over of individual and corporate identities
- Transactions resulting in > A$1 million exposure for banks
- Corruption of bank officers to gain confidential client data –

Sentences

- 13 offenders pleaded guilty - longest head sentence of 6 years
- 2 bank officers sentenced: one to 2 Years with 18 month non-parole; the other received a suspended sentence of 12 months' imprisonment

ANZ Bank Case

Modus Operandi *(personal, blended, covert penetration)*

- Between August and September 2004, the ANZ Bank was defrauded of A$650,000 with an eventual actual loss of A$140,000 though the illegal transfer of money from Equity Manager Accounts of customers of the bank to outside accounts held in the names of various persons
- Unauthorised funds transfers were undertaken by Melissa Jennison, a bank employee, who transferred A$650,000 from four customer accounts into the accounts of her accomplice Robert Schaefer
- Jennison also transferred funds to the business account of Tran, whose account was used to launder the illicit funds for a Ms Van

Sentences (R v *Schaefer & Tran* [2007] VSCA 36)

- Jennison – 3 years, 12 months non-parole period & confiscation order
- Schaefer – 15 months, 6 months to be served, 9 months suspended
- Tran – 2½ years, 12 months non-parole period & confiscation order

Environmental crime preventive strategies

Overt penetration

- ***Remote*** – Ram-rading – *target hardening (bollards, security screens)*
- ***Proximal*** – Taking cash & documents – *target removal, document security / monitoring, physical access control, entry-exist screening*

Covert penetration

Remote penetration

- Personal – corruption of insiders – *internal controls and monitoring*
- Electronic – hacking and scanning – *e-security and TEMPEST controls*

Proximal penetration

- Personal – insider abuse – *surveillance and personnel monitoring*
- Electronic – misuse of access privileges – *enhanced access controls*

Blended penetration

- Personal – Placement of confederates – *enhanced recruitment checks*
- Electronic – Placement of trojans – *enhanced e-security*

Australian Government
Australian Institute of Criminology

Russell.Smith@aic.gov.au