Australian Government

Australian Institute of Criminology

IBAC corruption, prevention and integrity conference

Corruption in the digital world

Dr Russell G Smith
Principal Criminologist
04/10/2017

www.aic.gov.au

The relationship between ICT and corruption

ICT as a target of corruption

- Theft and misuse of devices for the data they contain
- Trading in digital information taken from the workplace
- DDoS attacks as a means to extort money or information from agencies

ICT as a tool for committing corruption *(as an enabler)*

- Allowing access to data held in storage – personal information
- Hacking into unencrypted data streams – email, text, voice, SMS

ICT as a tool for committing corruption *(as an enhancer)*

- Theft of personal information for use in identity crime
- Theft and sharing of digital intellectual property
- Counterfeiting and altering documents
- Facilitation of unauthorised electronic transactions (from overseas)
- Allowing secure and anonymous communications between co-offenders

Source: Smith & Jorna in *Handbook of Global Research and Practice in Corruption* (2011)

The drivers of digital corruption

e-Government

- Digital government services – tax, health, voting via Internet / NBN
- Remote working – offices networked to agencies via VPNs

Opportunity theory *(Cohen & Felson’s routine activity theory)*

- Technological changes produce new crime opportunities
  - – motivated offenders (trained in IT, unemployed, networked)
  - – suitable targets (personal information, e-funds, infrastructure)
  - – absent capable guardians (legal & policing barriers, poor training)
- New technologies – wireless, mobile, biometrics, social networks
- Data overload and complexity of systems impede investigations

Tactical displacement

- Blocking of opportunities through enhanced e-security
- Reversion to personal crime and corruption of insiders

An example of tactical displacement – *Estrada case*

Fidencio Estrada

- Allegedly involved in organised drug trafficking in 2000
- Wanted access to Treasury Enforcement Communications System (TECS) database of law enforcement intelligence & customs watch list

Rafael Pacheco

- US Customs agent in Florida bribed with US$18,000 to access TECS
- Provided information on warrants, police operations & visa applications

Charges

- *Estrada*: conspiracy to bribe a public official, money laundering
- *Pacheco*: receiving a bribe, accessing database, obstructing justice

Sentences

- *Estrada*: 41 months' imprisonment and 36 months' supervised release
- *Pacheco*: 87 months' concurrent on another sentence of 60 months

Corruption within the World Bank

Chief Information Officer’s conflict of interest

- IT contractor allegedly involved with World Bank’s CIO
- CIO awarded IT contractor a major contract to supply IT to World Bank
- CIO alleged to have then purchased stock options from IT contractor
- IT contractor became the World Bank’s global IT services provider

Allegations of illegal and corrupt conduct by IT contractor

- Allegedly installed key-logging software on Bank employees’ computers
- Allegedly bribed bank officials by providing improper benefits to staff

Outcomes – Department of Institutional Integrity

- Chief Information Officer dismissed
- IT contractor became insolvent
- Criminal charges laid against IT contractor’s managers and auditors
- Bank established ‘International Corruption Hunters Alliance’

Future risks of ICT-related corruption

UK intelligence assessment of risks

- Police identifying themselves as officers on social networking sites
- Leaking confidential electronic information from police networks

Global State of Information Security Survey

- Survey of 12,840 senior IT managers in 135 countries
- 77% had not established security policies that addressed social networks or Web 2.0 technologies
- 60% had yet to implement security technologies supporting Web 2.0

Cloud computing-related risks

- External monitoring or theft of data held in cloud infrastructure

e-Procurement

- Corrupt electronic access to tender information and bribery of employees to manipulate procurement procedures and outcomes

Conclusions

Prevention strategies to consider

- Ensure that CEOs and managers are ICT literate and understand the risks
- Educate staff on how to use ICT securely (e.g. encryption, ID security)
- Publicise ICT policies and the consequences of non-compliance
- Limit or monitor the use of personal ICT services and devices (email, SMS, social networking, USB devices) for work in the public sector
- Monitor ICT usage (IP addresses, logon-logoff times, data usage)

Australian Government

Australian Institute of Criminology

Russell.Smith@aic.gov.au

www.aic.gov.au