Australian Government
Australian Institute of Criminology

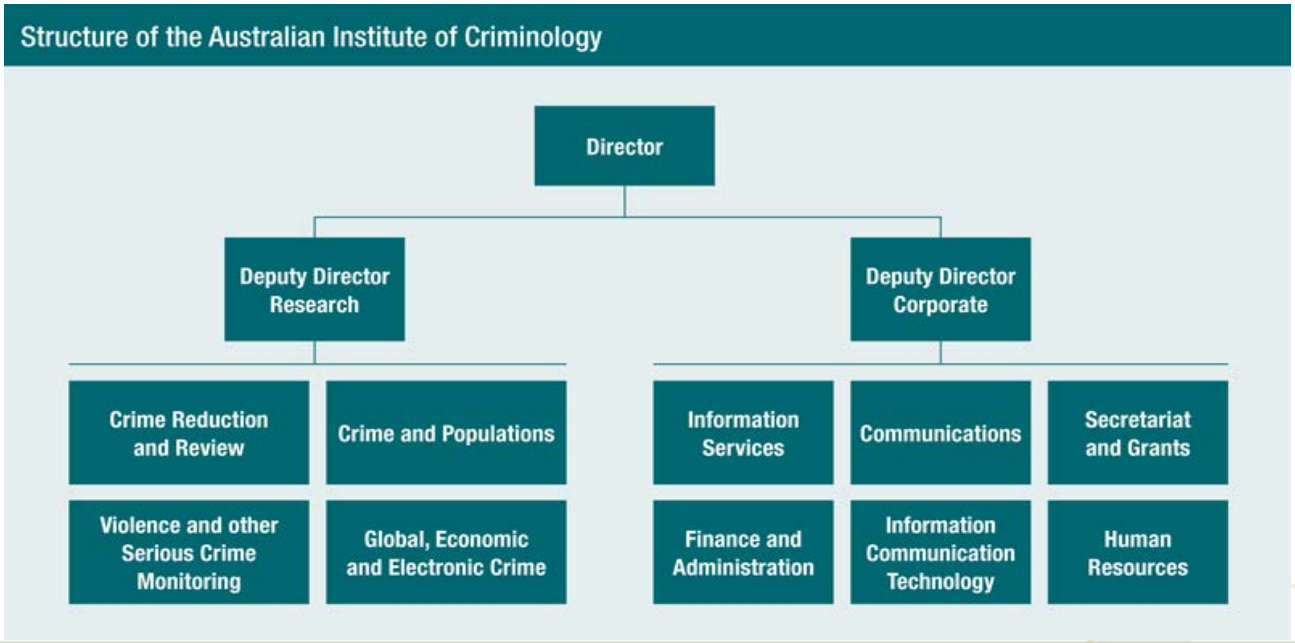
Cyber Crime Research

Presentation by the Australian Institute of Criminology

Australian Government
Australian Institute of Criminology

The Australian Institute of Criminology

- Australia's national research and knowledge centre on crime and justice
- Core funding from the Australian Government, with income for contract research from public and private sectors
- Criminology Research Advisory Council representing all jurisdictions
- Staff of 29 academic researchers and 23 support staff – total 52



Current and previous cyber crime research

Public sector

- *Fraud against the Commonwealth annual survey*
- Electronic funds transfer fraud
- E-tax fraud, electronic voting fraud risks
- Electronic Medicare / Centrelink (welfare) fraud

Private sector

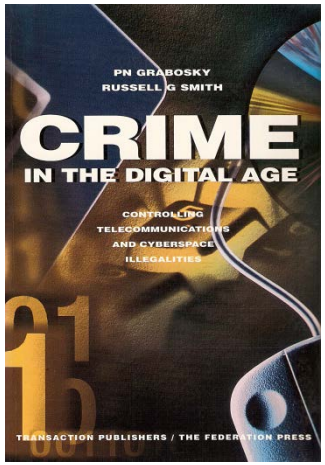
- *ABACUS – Aust Business Assessment of Computer User Security*
- Identity crime, e-banking, funds transfer fraud, business fraud
- Sharemarket manipulation / e-piracy / intellectual property theft
- Money laundering / financing of terrorism (SVCs, e-currencies, EFT)

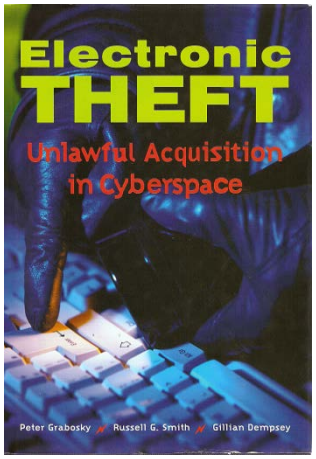
Personal cyber crime

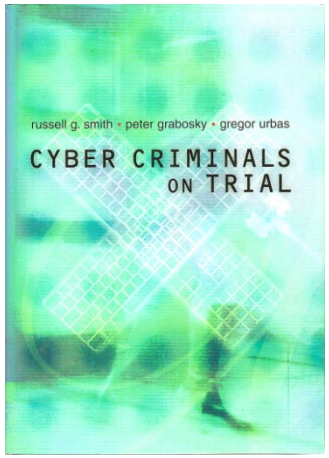
- *ACFT – Annual Online Scams Survey*
- Personal fraud / scams / Online child grooming / cyber-stalking

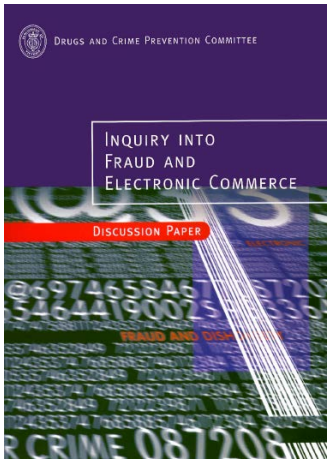
Australian Government
Australian Institute of Criminology

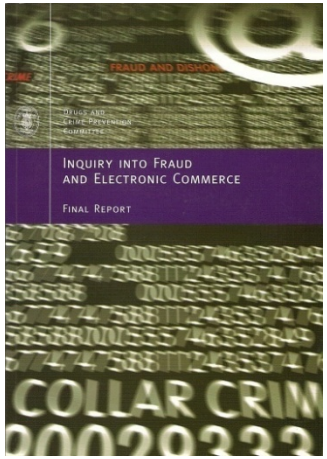
Principal AIC publications on cyber crime

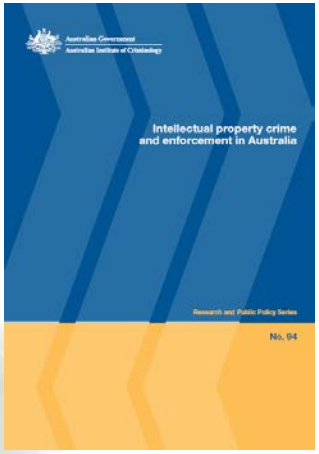


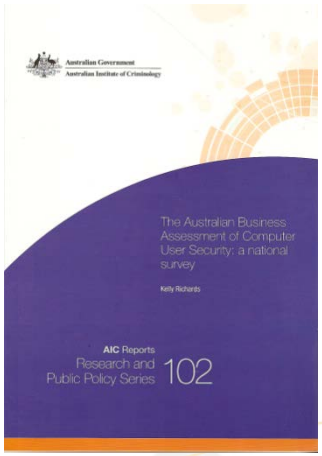












Developing risk areas

Computer-facilitated fraud and money laundering

- Focussed personal spam attacks (whale phishing, spear phishing)
- Click frauds to defraud online advertisers
- Phishing leading to Vishing and SMiShing / context-aware phishing
- Money laundering using Stored Value Cards

Unauthorised access

- Access to disable security systems
- Embedded malicious code installed by corrupt insiders / consultants
- Displacement risks of violence to obtain access codes

Evolution of malware

- Malware able to avoid detection by filters
- Vulnerabilities from user-generated web content
- Botware moving to peer-to-peer networks / file-sharing

Developing risk areas

Intellectual property infringement and industrial espionage

- Electronic theft of trademarks and patents
- Enhanced reverse engineering of code relating to inventions
- Hacking into unencrypted commercial-in-confidence communications
- Risks from insecure outsourcing / placement of confederates

Exploitation of younger people

- Cyber-bullying and cyber-stalking
- Theft of devices with data and personal information
- Theft of virtual property from 3D Virtual Environments

Offensive content / cyber-terrorism

- Use of cryptography to prevent access to images
- Live streaming of images of child abuse in chat rooms / sexting
- Use of ICT to organise racially motivated attacks / terrorism

Ongoing / proposed cyber crime research areas

Cyber crime trends

- Cost and impact of cyber crime
- Patterns of prosecution activity; analysis of prosecution policy
- Impact of smartcard technologies on fraud (Chip/PIN)
- Spoofing biometric identification systems
- Data leakage; mobile and wireless fraud; crime risks of cloud computing

Patterns of victimisation

- Why do people respond to consumer scam invitations?
- What online fraud risks face small business?
- What risks face older people – superannuation fraud; online banking?

Responses to cyber crime

- Sentencing of cyber criminals – local and comparative research
- Criminal justice sanctions – electronic monitoring; internet restrictions
- Policing – data access and sharing (*Cybercrime Amendment Bill 2011*)

Australian Government
Australian Institute of Criminology

Russell.Smith@aic.gov.au