Australian Government
Australian Institute of Criminology

Cyber Crime Research

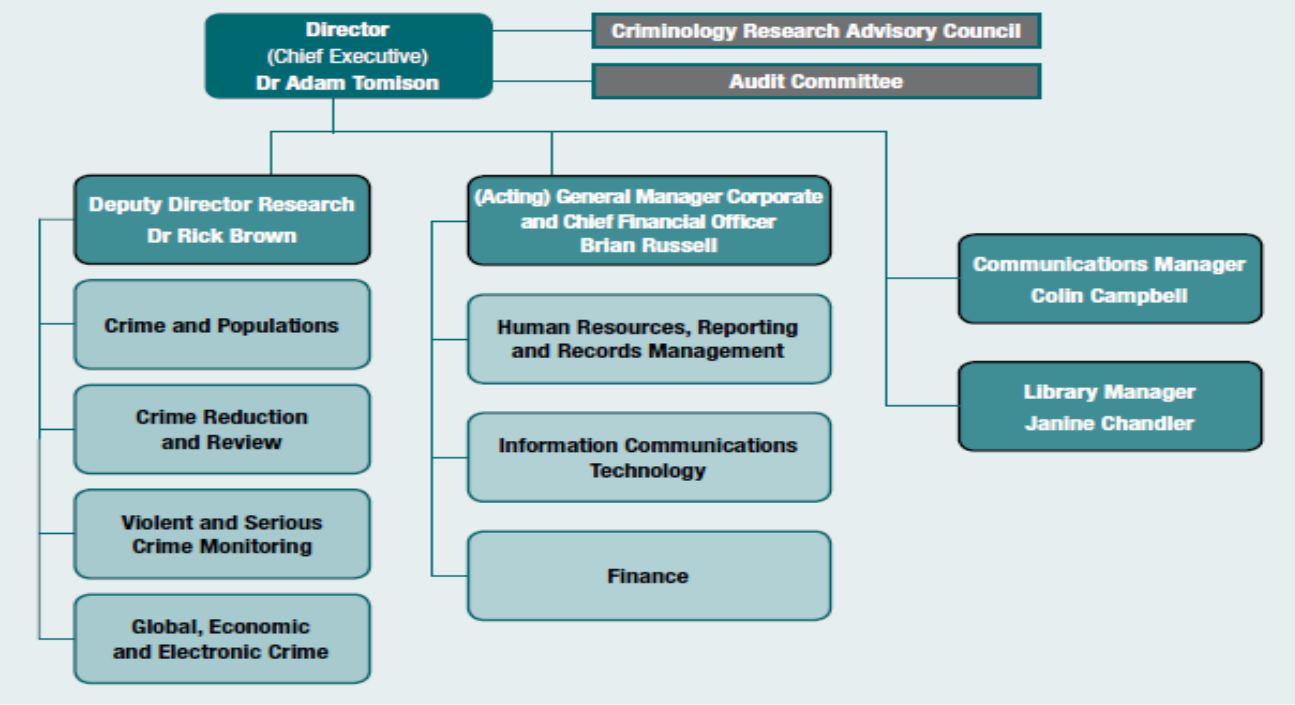
Presentation by the Australian Institute of Criminology

Dr Russell G Smith
Principal Criminologist

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 30 academic researchers and 25 support staff – total 55



Cyber crime research

Research questions

- How are cyber crimes committed (e.g. credit cards, internet)?
- How many crimes are committed and what are the crime trends?
- Who commits them and why do people commit them?
- How much money is at stake, lost and recovered?
- How can such crime be reduced – by prevention or punishment?

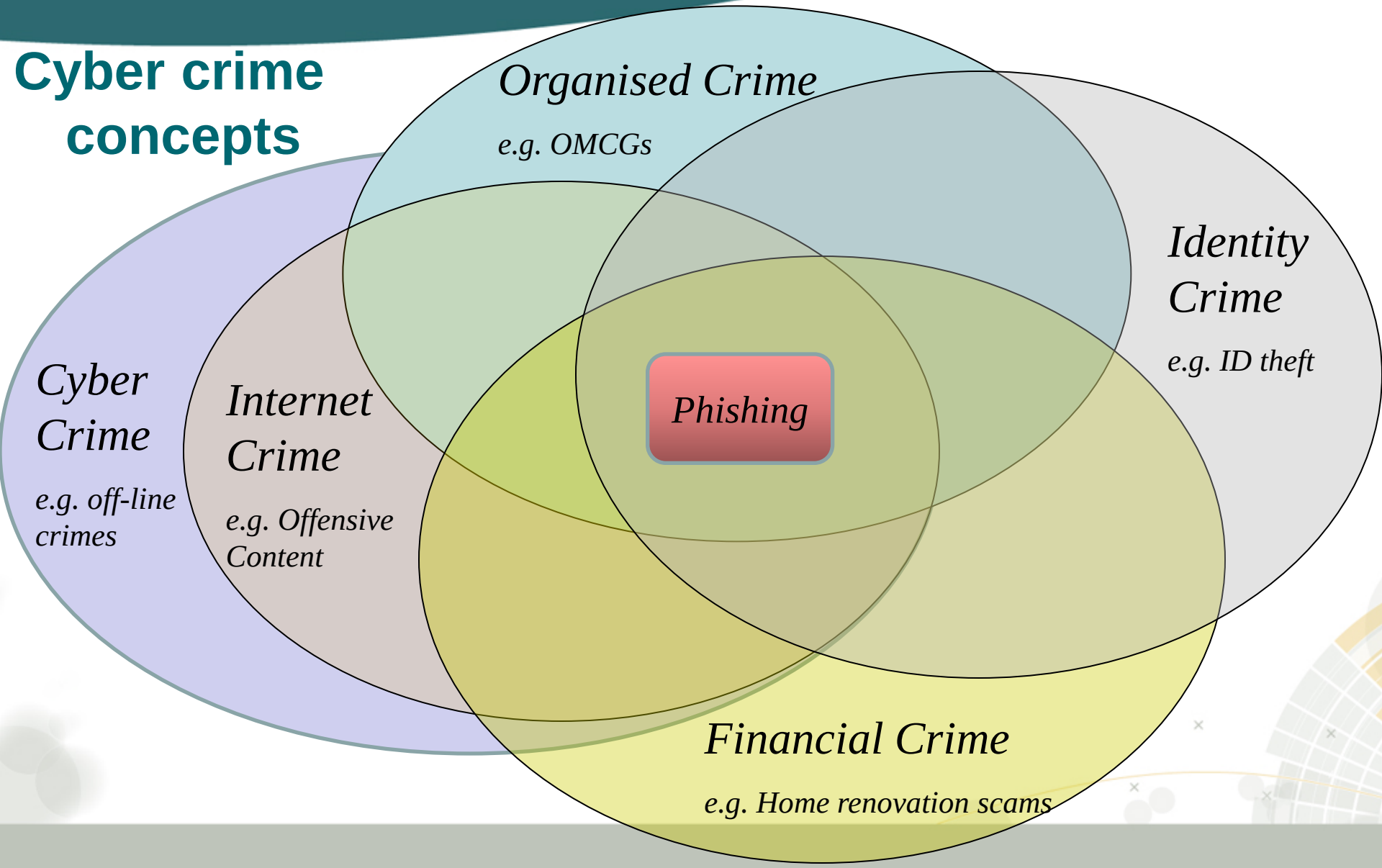
Research methods

- Online and desk-based reviews of books, reports and articles
- Legislative and case-law analysis, including sentencing research
- Consultations with business, government and the community
- Surveys of households, businesses, offenders and victims
- Analysis of media reporting of crime

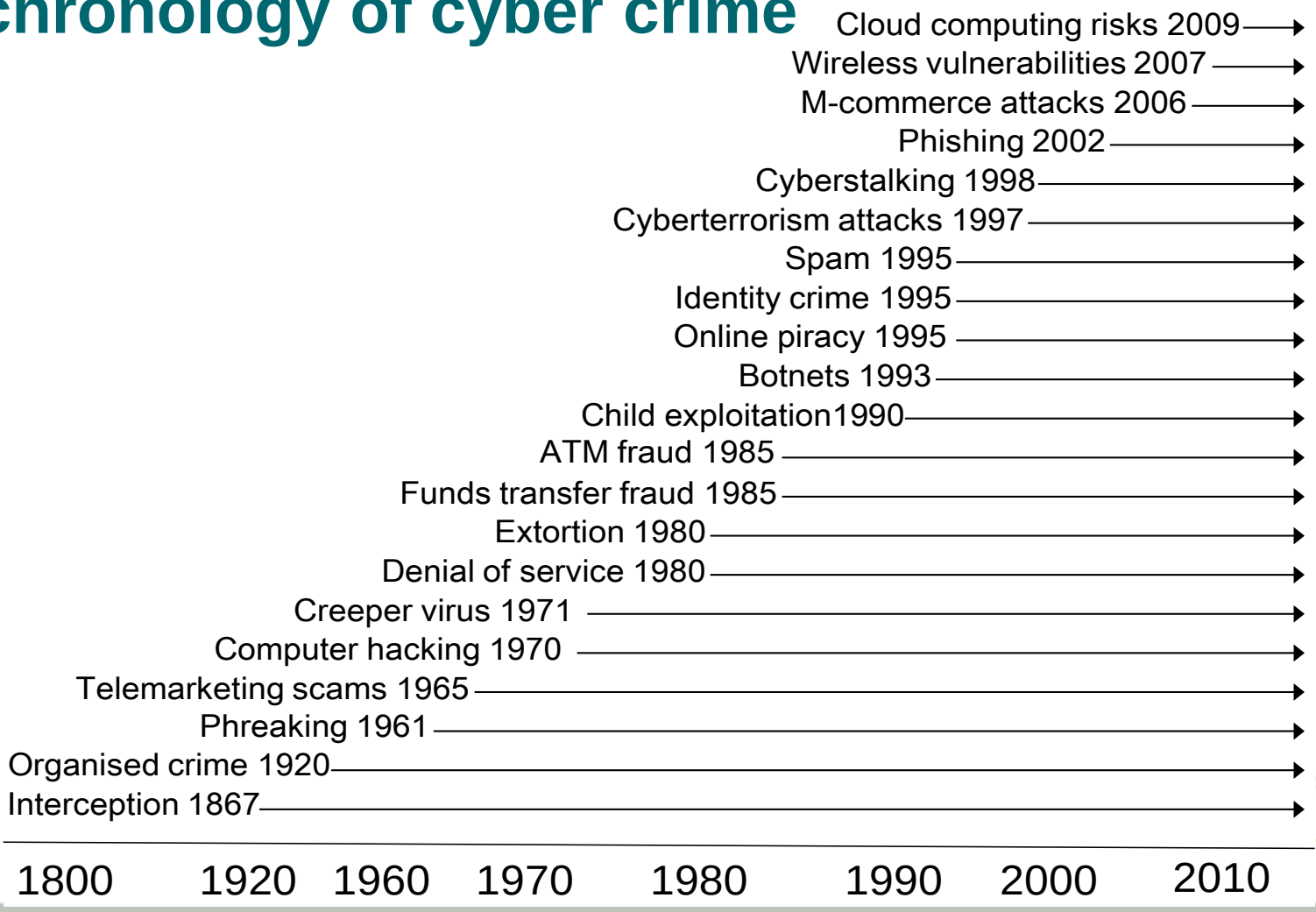
Dissemination of findings

- Reports, books, articles, conference papers, roundtables, online, media

Cyber crime concepts



A chronology of cyber crime



Changes in the motivations of offenders

Curiosity and self-education

- Early geeks and hackers
- Early “phreakers” (Cap’n Crunch in the 1970s)

Fame-seeking

- Risk-taking acts (Kevin Mitnick in the 1980s)
- High impact crime and targets (defence departments and banks)

Personal motivations / revenge

- Cyber-stalking, child exploitation, vandalism, employee revenge

Financial gain

- Scammers and phishers, organised economic criminals (e.g. ID crime)

Political and ideological change

- Cyber-terrorists and attacks on critical infrastructure

Drivers of change in the 21st century

Globalisation

- Increasing risks from the new and developing economies

User profile

- Integration of technology into personal and business life
- Increasing use of ICT in government

Technological development

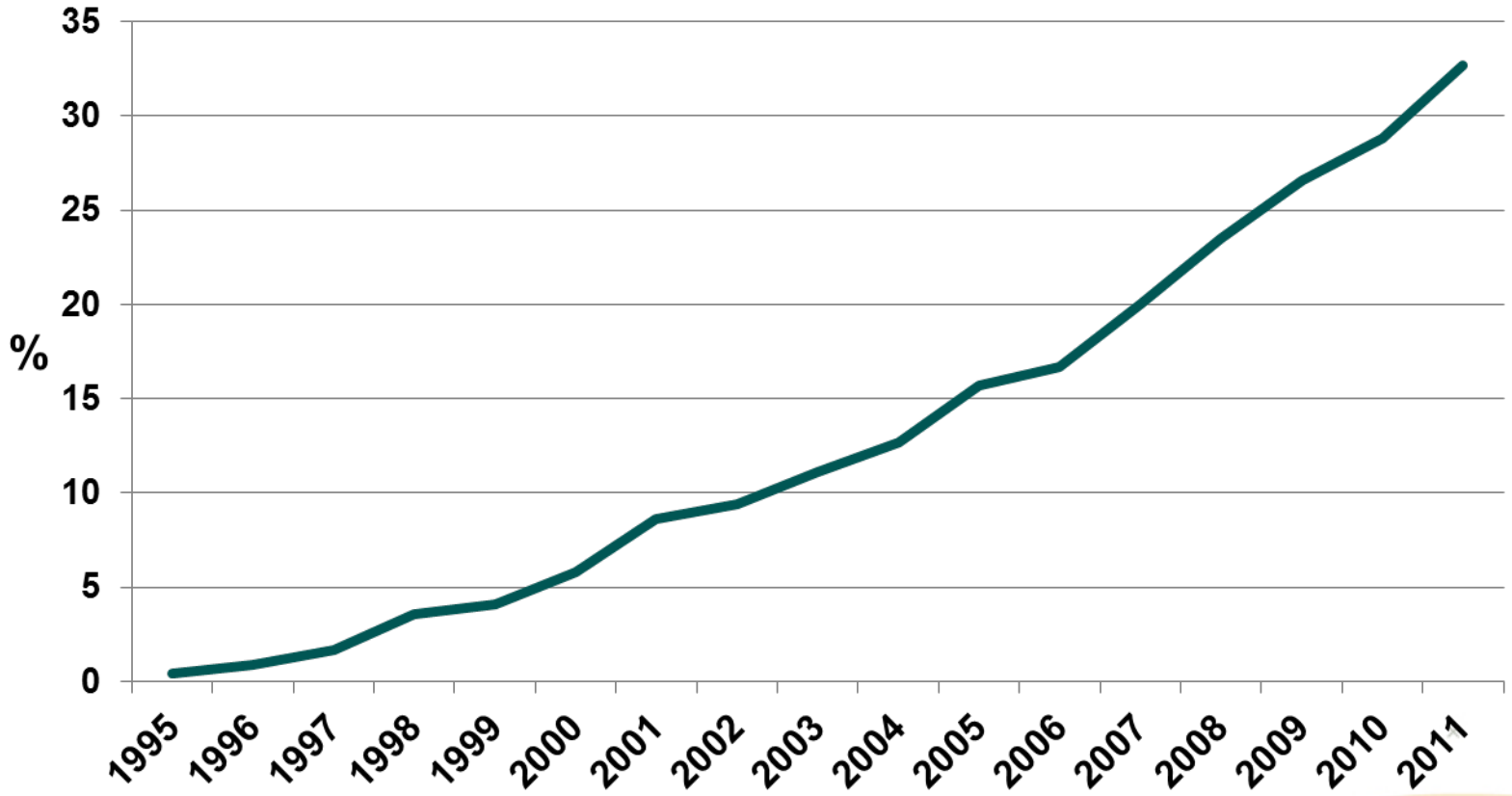
- Increasing use of broadband
- Increasing use of wireless technologies
- New methods of identification and verification
- New payment systems – SVCs, e-cash, gaming currencies, e-gold

Crime methodologies

- Movement from ‘syntactic’ to ‘semantic’ attacks

Internet growth statistics 1995-2011

Internet users as a percentage of world population



Source: http://www.internetworldstats.com

Online personal fraud risks

Syntactic attacks

- Exploitation of technical vulnerabilities to commit fraud
  (e.g. malware, plastic card skimming, illegal funds transfers, Wi-Fi)

Semantic attacks

- Exploitation of social vulnerabilities to gain personal information
  (e.g. scam solicitations, identity-related fraud, auction fraud)

Blended attacks

- Attacks using technical tools to facilitate social engineering

e.g. Phishing

- Using an unsolicited request to visit a counterfeit website in an attempt to trick users into disclosing personal banking information

Scam categories	Scam sub-categories
Advance fee schemes	Pyramid schemes, Ponzi schemes, chain letters, 'Nigerian' emails, business opportunities, prizes and lotteries, dating scams
Non-delivery and defective products and services	Online auctions, internet services, computer products, sexual services, credit and loan scams, health scams, educational qualifications
Unsolicited and unwanted goods and services	Spam, securities and investment fraud, bait advertising, inertia selling
Identity crime	Phishing, plastic card fraud, card skimming, un-authorised transactions, online banking fraud

Current and previous AIC 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

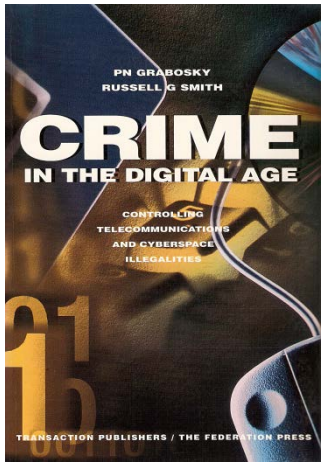
- *ABACUS – Aust Business Assessment of Computer User Security*
- Identity crime, e-banking, funds transfer fraud, business fraud
- Sharemarket manipulation / e-piracy / intellectual property theft
- Money laundering / financing of terrorism (SVCs, e-currencies, EFT)

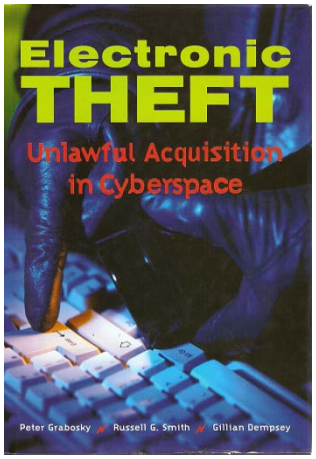
Personal cyber crime

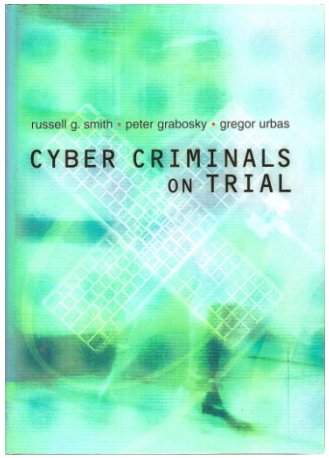
- *ACFT – Annual Online Scams Survey*
- Personal fraud / scams / Online child grooming / cyber-stalking

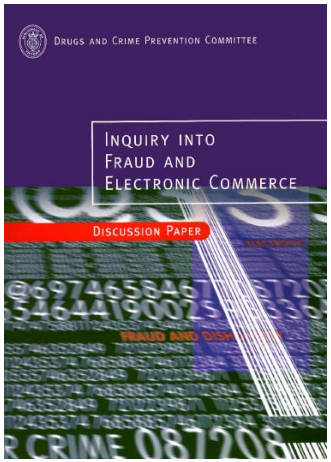
Australian Government
Australian Institute of Criminology

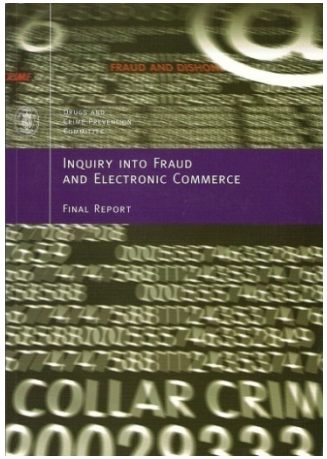
Principal AIC publications on cyber crime

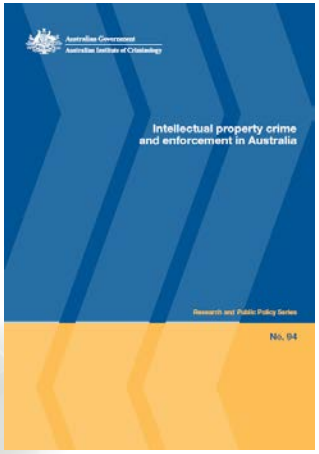


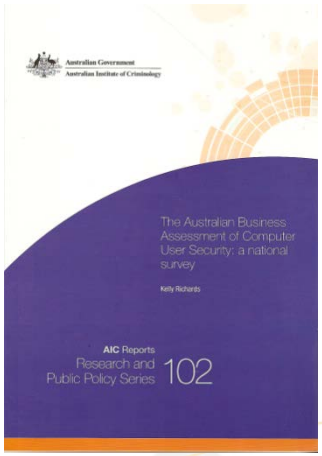












Quantifying the extent of identity crime

SIRCA (2003)

- Direct loss from identity fraud in Australia 2001-02 was $420 million
- Total cost of identity fraud $1.1 billion (including prevention & recovery)

Personal identity fraud (ABS)

- Total personal fraud in 2010-11 – 713,600 victims ($1.4b); 6.7% pop'n
- ID theft – 124,000, 0.8% (2007); 44,700, 0.3% (2010-11) [-64%]
- Card fraud – 383,300, 2.4% (2007) ; 662,300, 3.7% (2010-11) [+73%]

Official dishonesty offence statistics recorded by police

- 24% decline in offences; 35% decline in rate/100,000 pop'n since 2000

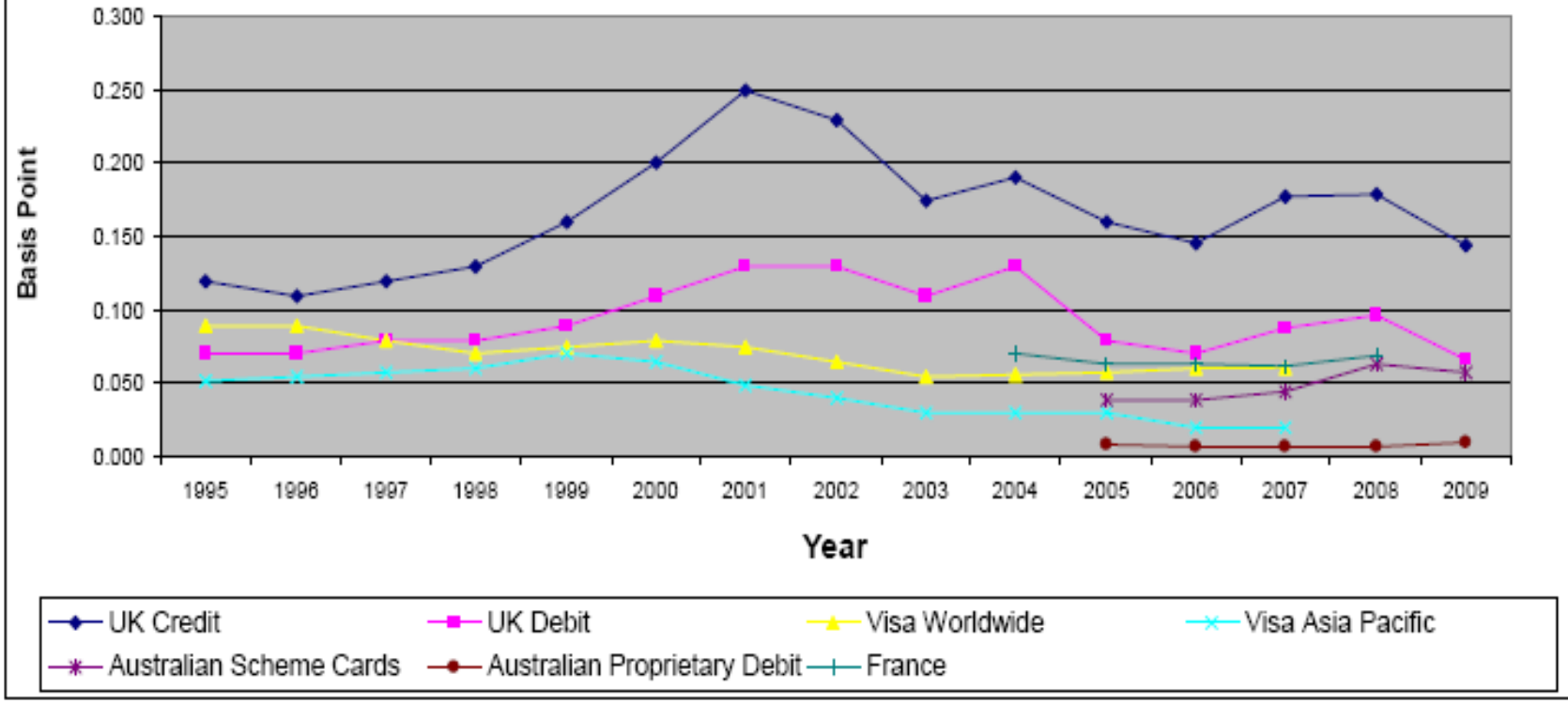
Plastic card fraud (APCA)

- 0.015% of card transactions fraudulent in 2006; 0.052% in 2011(Aust)
- Card-not-present fraud losses increased: $31.8m (2006) $198m (2011)
- Sept 2012 – 15,000 false cards worth $37.5m seized by police

Australian Government
Australian Institute of Criminology

Payment card fraud trends

Plastic card fraud losses in basis points for selected countries



Sources: APCA, UK Payments Association, Observatory for Payment Card Security (France) and Visa Inc.

Quantifying the extent of identity crime

SIRCA (2003)

- Direct loss from identity fraud in Australia 2001-02 was $420 million
- Total cost of identity fraud $1.1 billion (including prevention & recovery)

Personal identity fraud (ABS)

- ID theft – 124,000, 0.8% (2007); 44,700, 0.3% (2010-11) [-64%]
- Card fraud – 383,300, 2.4% (2007) ; 662,300, 3.7% (2010-11) [+73%]

Official dishonesty offence statistics recorded by police

- 24% decline in offences; 35% decline in rate/100,000 pop'n since 2000

Plastic card fraud (APCA)

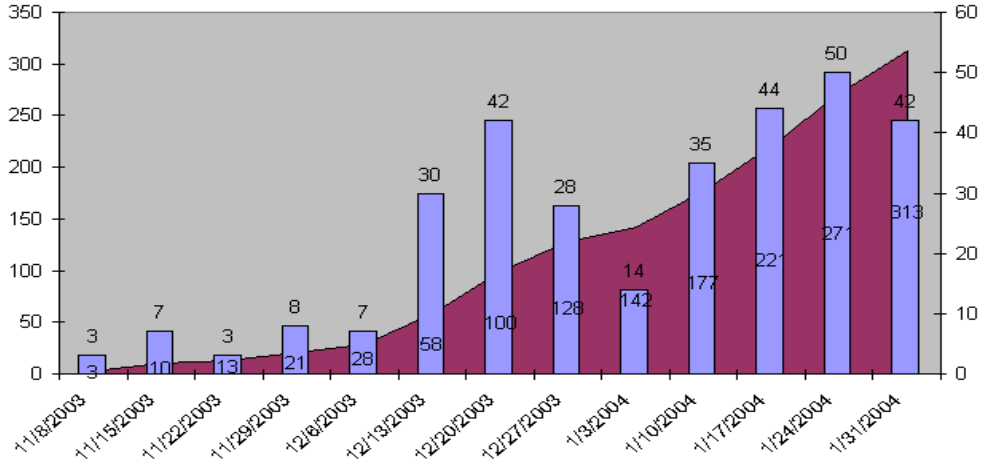
- 0.015% of card transactions fraudulent 2006; 0.052% in 2011(Aust)
- Card-not-present fraud losses increased: $31.8m (2006) $198m (2011)
- Sept 2012 – 15,000 false cards worth $37.5m seized by police

Cybercrime

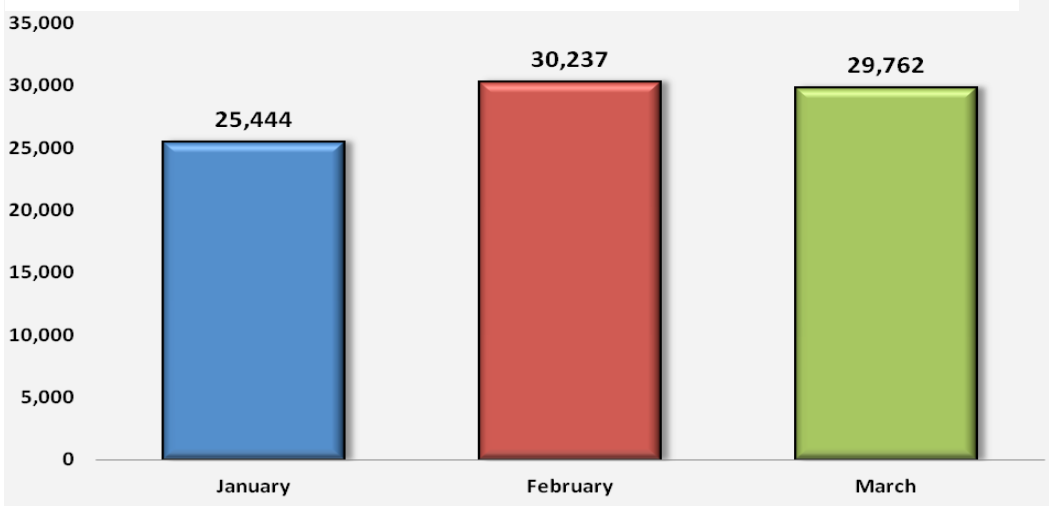
- Verizon (2011) – 855 data breaches involving 174 million records
- APWG – Phishing attacks – 176 (Jan 2004); 23,535 (Jan 2011)

Anti-Phishing Working Group Data

January 2004
- 176 unique attacks



January 2012
- 25,244 unique attacks



14,243% increase over 8 years

Source: http://www.antiphishing.org/phishReportsArchive.html

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 and online games

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, contactless)
- 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 between public and private sectors

Australian Government
Australian Institute of Criminology

Russell.Smith@aic.gov.au