PCUG

10 NOVEMBER 2009

JOHN BROOME

CYBERSPACE AND CRIME

Overview

- Definitions
- Computers –the common link
- Legal framework
- Types of cybercrimes
- Some case studies
- Technology as friend and foe
- Investigating cybercrime
- Global Financial Crisis
- Money Laundering and why it matters

What is Cybercrime?

- Criminal activity which uses or takes place through communications technology, including the Internet, telephony and wireless technology (JC on ACC 2004).
- Offences where a computer is used as a tool in the commission of an offence, as the target of an offence, or used as a storage device in the commission of an offence (Australian Centre for Policy Research).
- Technology enabled crimes (Aust. High Tech Crime Centre)
  - E-Crime
  - Internet Crime
  - Net Crime
  - Computer Crime
  - High Tech Crime

What Do I Mean By “Computers”

- Obviously we need to distinguish between single PCs and networks of various sizes
- Short hand for present purposes
  - Single computer
  - A home network
  - A business network (retailers or large businesses)
  - A piece of national infrastructure (Bank or electricity grid)
  - An international system (SWIFT)

Using Computers to Commit Crime

- Computer as **target** (e.g. computer intrusion, data theft, techno-vandalism, techno-trespass)
- Computer as the **instrumentality** of the crime (e.g. credit card fraud, telecommunications fraud, theft or fraud)
- Computer as **incidental** to other crimes (e.g. drug trafficking, money laundering, child pornography)
- Crime associated with the **prevalence** of computers (e.g. copyright violation, software piracy, component theft
- Computer as a means of **storing** material related to a crime

Legal Framework

- Too many laws or too few?
- Specific and general
- *Cybercrime Act 2001* (Cwlth), which details offences against computer data and systems.
- *Criminal Code Act 1995 (Cwlth)*, Part 10.7 - Computer Offences, legislates against activities such as:
  - Computer intrusions (e.g. malicious hacking).
  - Unauthorised modification of data, including destruction of data.
  - Denial-of-Service (DoS) attacks.
  - Distributed Denial of Service (DDoS) attacks using botnets.
  - Creation and distribution of malicious software (e.g. viruses, worms, trojans).

Legal Framework

- Each state and territory in Australia has its own legislated computer-related offences
- And then ....
- All the specific laws relating to
  - Offences (fraud, theft, terrorism etc)
  - Privacy
  - Data Protection
- Internationally there is a wide range of laws, conventions and directives - Council of Europe's *Cybercrime Treaty*

Who is Protecting You?

- AFP and State and Territory Police
- High Tech Crime Centre (AFP)
- Australian Crime Commission (ACC)
- Australian Competition and Consumer Commission (ACCC)
- Australian Securities and Investment Commission (ASIC)
- Australian Communications Authority (ACA)
- Attorney- Generals Department (policy and MLA)
- Various state and territory agencies
- ISPs

Types of Cybercrime

- Fraud
- Insider trading
- Identity theft
- Pump and dump
- Intellectual property theft
- Racial vilification
- Phishing (bank or credit details)
- Mule recruitment
- Hacking
- Extortion
- Harassment
- Grooming
- Paedophilia
- Denial of Service
- Virus, Trojan attacks
- Spam
- Espionage
- Terrorism
- And many more

Types of Cybercrime

- Old Crimes using New Medium (e.g. frauds, racial vilification, insider trading, pump and dump, paedophilia)
- New Crimes sing New Medium (e.g. Virus and Trojan attacks, Denial of Service, Phishing
- Criminals will ALWAYS reinvent themselves and the way they operate and utilise new opportunities because we are SLOW to respond

Case Studies

- But ..... It does not stop the cybercriminal
- Pump and Dump - put false information on the net and sell when stock rises
- Sometimes this is done publicly but may be hard to stop – investment news letters
- Nigerian Letters
- Ponzi schemes (Bernie Maddoff)
- The greedy and the gullible

New Technologies

- Electronic Payment systems
  - Software (virtual currency used in on line games)
  - Hardware (Mondex, NETS cashcard or NTT's NCash
  - Online (BPay)or offline (prepaid cards like Mondex)
  - Picopayment, micropayment or macropayment systems (security features depends on size of payment)

New Technologies

- Electronic Cash (just like the real thing)
  - *untraceability*: offers users unconditional anonymity
  - *unlinkability* of payments: it is not possible to identify whether payments originated from a particular customer account
  - *unforgeability* of e-cash
  - *protection against double spending* (to different payees and to the same payee
  - But can provide wonderful opportunities for criminals

New Technologies

- Electronic purses and Prepaid cards
  - Usually have a maximum value
  - Used for small transactions
  - Anonymous
  - Can be abused
- Mobile Phone payments
  - Can be used for small payments (Dial a Coke)
  - Increasingly being used in developing countries (Philippines and Pakistan)

Global Financial Crisis (GFC)

- The result of greed, incompetence, negligence, stupidity, staggering failures of governance and crime
- How did a bank in Australia buy a ‘product’ which was the debt owed by unemployed home buyer in the US?
- Many products were deliberately misrepresented

Global Financial Crisis (GFC)

- Some of the major problems involved fraud
  - Lehman Bros
  - AIG (American Insurance Group
  - Fanny Mae and Freddie Mac (Government established mortgage sellers)
- Breakdown in regulation
- Products traded electronically and repackaged and on sold electronically
- Failure to understand products but also conflicts of interests (rating agencies)

Investigating Cybercrime

- In theory just like other crimes
- Crimes can be simple or complex
- Investigative challenges come from
  - The level of complexity
  - Skill and knowledge of the criminals
  - Skills and knowledge of the investigators and prosecutors
  - Location of evidence
  - Adequacy of laws (are we playing catch up)
  - Availability of witnesses
  - Preparedness of victims to speak up
  - Capacity to explain and prove the offence

Money Laundering

- Crime pays .... It always has and it always will
- Many crimes are committed to make money
- Many crimes make a great deal of money
- Criminals need to hide the link between the crime (predicate offence) and the resultant money (proceeds of crime)
- They use simple or complex methodologies
- Small amounts do not need to get laundered but large amounts do
- In many countries large amounts do need to be hidden

Money Laundering

- Hiding the criminal origins of money
- Predicate offence
- Placement
- Layering
- Integration
- Simplistic but useful framework
- Started as aid to investigation but has become (wrongly) end in itself
- Drugs, people smuggling, gun running, corruption, and fraud, fraud, fraud

Money Laundering

- Stock exchanges here and overseas
- Use of credit cards
- Funds transfers
- Hawala, Hundi, Chit, Door to Door
- False invoicing –trade based money laundering
- Use of commodities – diamonds, gold,
- Airport movements (e.g. Vietnam pilots)

Cyberspace and Crime

- We face enormous problems and the threats are real
- We are addressing and we are having some success
- As usual we tend to be slow, under resourced, overwhelmed and outwitted
- Awareness is important and hopefully we are all now a little more aware

Cyberspace and Crime

QUESTIONS