Parliamentary Joint Committee on the Australian Crime Commission

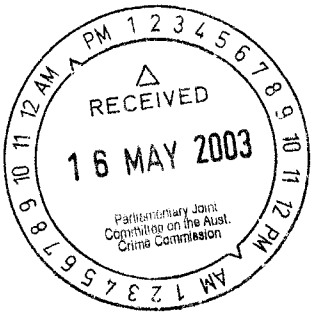
Inquiry Into Cybercrime

Submission No:17
Received 14 May 2003
Mr G.R. Morgan APM
Assistant Commissioner State Crime Command
NSW Police
Level 4, Prince Alfred Park Building
219-241 Cleveland Street
STRAWBERRY HILLS
NSW 2012
☎02 9384 6139 🖹02 9384 6687

NSW Police
www.police.nsw.gov.au ABN 43 408 613 180

OFFICE OF THE COMMANDER
STATE CRIME COMMAND
Level 4
Prince Alfred Park Building
219-241 Cleveland Street
Strawberry Hills NSW 2012
Ph. (02) 9384 6139 / 46139
Fx (02) 9384 6687 / 46687
TTY 9211 3776 (Hearing/Speech impaired only)

Maureen Weeks
Committee Secretary
Parliamentary Joint Committee
Parliament House
Canberra ACT 2600



13 May 2003

Dear Ms Weeks

On behalf of the NSW Police Commissioner I would like to thank the Parliamentary Joint Committee (PJC) on the Australian Crime Commission (ACC) for the invitation to present a submission to your enquiry.

Cybercrime is likely to have a steadily growing significance to NSW Police in the crime detection sphere. In addition to the specified areas, leading technology issues will increasingly become part of the investigation of crimes such as kidnapping, extortion, robbery, homicide and drug offences. Successful investigation of these matters will routinely require e-mail, SMS, and internet chat interception as well as forensic examination of a large array of consumer electronic devices and networked computers.

In preparing this contribution, relevant SCC Crime Squads along with Counter Terrorism Coordination Command were requested to respond with information that fitted the criteria. This submission should be considered as preliminary with relevant Squads and units in a better position to elaborate on these topics if required.

1. Child pornography and associated paedophile activity

SCC's Child Exploitation Internet Unit (CEIU) was established within the Child Protection Squad to investigate child exploitation and serial sexual abuse committed through or linked to the internet.

The CEIU has identified shortfalls in current NSW legislation. At this stage the unit is unable to provide information on novel or emerging trends apart from what is already known to most law enforcement agencies. Many Internet offenders have a good knowledge of police approaches and are constantly advising co-offenders on the best

approaches to minimise detection. However, the Child Protection Squad suggests the following legislative and operational changes that, while specific to the NSW context, have wider relevance:

- Amendments to telephone interception legislation that would include offences connected with child pornography and enticement. At present these offences are not class 2 and do not carry a seven year penalty as required by current telephone intercept legislation

- Making the current summary offences section under section 578B(2), Possess Child Pornography, and 578C(2A), Publish Child Pornography, indictable with increased penalties. These offences are currently summary offences while in some states they are indictable and carry penalties of more than five years

- Establishing an offence for enticing children by online luring and grooming to engage in a sexual act.

2. Banking, including credit card fraud and money laundering.

SCC's Fraud Unit has identified new modus operandi and potential risks to the financial services sector from e-crime.

A recent scam has been the establishment of rogue internet sites that look like genuine bank sites by using copies of the source code for the true site. Spam email invitations are sent to customers requesting them to make contact and supply information to update security. A small number of people were recently deceived resulting in losses of $200,000 from one bank and $4,000 from another. NSW Police prevented losses in another case due to an arrest. It is difficult to judge how much of a future risk this type of fraud poses. The technique is a type of social engineering security compromise rather than an electronic attack. However, some potential attacks could be:

- Compromise of domain name servers - for example, allowing rerouting of internet traffic to a bank. While this may be technically possible the likelihood cannot be ascertained at this stage. A few hours data diversion would be capable of compromising a significant number of accounts. Small personal accounts usually have daily transaction limits but some larger corporate or government accounts may have no such limits. Compromise of these accounts could have a significant impact on the financial services sector

- Spyware compromise - where passwords are captured through "Trojan" programs on customers' home (or business) computers. Where automated, this might have the potential to compromise large numbers of smaller accounts. Again, the actual risk is difficult to quantify. No incidents of this type have been reported to NSW Police.

Credit Card Fraud:

The Fraud Squad has dedicated an investigative team to credit card fraud in co-operation with major banks. At this point the issue of CPP (Common Purchase Point) credit card fraud may have plateaud or even be in decline. However, there is a significant body of credit card fraud that cannot be accounted for by CPPs and is possibly derived from one or more of the following:

- The definition of CPP being too narrow
- Credit card data compromised at sources other than CPP, eg, within the bank/card provider or a third party such as a card printer
- Compromise of data by unlawful physical interception of telephone lines carrying data
- Hacking into servers containing data, either through the Internet, direct dialup or wireless access points.

3. Threats to National Critical Infrastructure

The threats here are similar or perhaps identical to threats to the financial sector. One of the major obstacles to investigations in these areas is the collection of overseas evidence. Methods of gathering and presenting evidence in a cost effective way will need to be developed if law enforcement is expected to prosecute these types of offences. The Mutual Assistance Regime is not suitable for e-crime where evidence needs to be to be acquired promptly. Prosecuting e-crime offences may require different ways of presenting evidence in Court including:

- Accepting video link evidence
- Accepting overseas affidavit evidence, especially with respect to facts that are not reasonably disputable (eg, cardholder evidence of compromise)
- Disclosure of contested evidence by the defence
- Payment of costs by the defence for unnecessary disputed evidence.

Limitations on the capabilities of law enforcement are also a potential threat to the national infrastructure. It needs to be stressed that these types of restrictions, whatever their positive intention, come at a price to law enforcement. For example, the power to monitor Internet or other e-crime activity is firmly regulated by the telephone interception legislation. TI warrants cannot be sought for hacking incidents which are offences under NSW legislation. This is also the case in other states. In some cases, at least, this can be overcome with co-operation from the Commonwealth. The power to remotely access a computer is also not available to law enforcement agencies but it is acknowledged that this is a delicate area.

Other limiters common to all law enforcement agencies include the financial ones that curtail expenditure on alternative investigation techniques and the inability to enforce particular laws. Certainly a key risk to the future law enforcement response to cybercrime is the availability of staff trained in the specialist techniques that this area may increasingly demand.

In conclusion, it is pleasing that the ACC have had the foresight to identify the need for a cybercrime investigation capability. It is essential the ACC Cybercrime unit work in close co-operation with other law enforcement agencies and that, as far as

possible, there is no legislative impediment to this. The Australian Hi Tech Crime Centre is acknowledged to be the correct body to facilitate this co-operation.

The SCC looks forward to further developing a responsive partnership with the ACC and other stakeholders on these issues and thanks the Parliamentary Joint Committee for the opportunity to present a submission.

Yours sincerely

Peter Dein
Detective Chief Superintendent

FOR:
G.R. Morgan APM
Assistant Commissioner
State Crime Command