SUBMISSION NO. 53

CHIEF MINISTER
MINISTER FOR POLICE, FIRE AND EMERGENCY SERVICES

Parliament House
State Square
Darwin NT 0800
chief.minister@nt.gov.au

GPO Box 3146
Darwin NT 0801
Telephone: 08 8901 4000
Facsimile: 08 8901 4099

The Honourable Belinda Neal MP
Email: coms.reps@aph.gov.au

Dear Ms Neal

Thank you for your letter dated 14 May 2009 with regard to the House of Representatives Standing Committee on Communications commencing an inquiry into cyber crime and its impact on consumers.

The issues for consideration by the Standing Committee are set out below (in bold). Comments are set out in relation to those issues of particular relevance to the Northern Territory Police.

a) Nature and prevalence of e-security risks including financial fraud and theft of personal information, including the impact of malicious software such as viruses and Trojans.

NT residents and businesses are frequently falling victim to various varieties of cyber crime and many have lost substantial sums of money which cannot be recovered.

Internet Banking Fraud

The NT Police receive regular complaints from victims who have had thousands of dollars (up to approximately $20,000) withdrawn out of their accounts via internet banking fraud. These generally seem to be operated by overseas crime groups harvesting bank account sign-on details via phasing or installing of malware or trojans on their computers. These 'stolen' sign-on details are used via internet banking to get into the victim's bank account and transfer funds out. Mostly the funds cannot be directly transferred overseas and need to be transferred first to a 'mule' account with the 'mule' given instructions to withdraw the money in cash and send it overseas via Western Union (WU). 'Mules' are recruited often via on-line job seeker sites.

To date, the banks have been reimbursing their customers who are victimised in this way. The banks are therefore bearing the cost of this type of crime. The only avenue open to police is the interview of the 'mule' to determine their criminal culpability. Targeting of the overseas crime groups running these frauds is extremely difficult.

Most internet bank fraud 'mules' are innocent parties however, NT Police has identified people that knowingly participate in this type of crime. NT Police has sought an opinion from the NT Director of Public Prosecutions regarding appropriate charges for a NT female who offered her services as a 'mule', but kept the money ($40,000) for her own use.

On-line Auction Fraud

NT Police receive frequent complaints regarding auction fraud occurring through sites such as eBay. On most occasions the offenders are located in another jurisdiction.

For police purposes, the jurisdiction where the offender is located and where they obtain the proceeds of the deception, is the jurisdiction that has primary responsibility for the investigation of the offence.

In order to assist victims making their complaint direct to the most appropriate jurisdiction, Queensland Police Fraud and Corporate Crime developed and host an on-line auction fraud reporting site. This practical facility was developed in consultation with all Australian Police jurisdictions.

NT Police has successfully investigated and prosecuted three on-line auction fraud offenders in this jurisdiction. Each had numerous interstate victims and all three offenders received terms of imprisonment.

On-line Scams

Nigerian 419 scams

The NT has many victims who have paid money to Nigeria or other West African Countries for several years, including one victim who has paid over $350,000 in relation to a 'deceased estate' scam. Despite a number of approaches by Police to persuade him to stop sending money, the victim continues to engage in this activity even though he has given away his life savings.

Deceptive advertisements

NT Police receive frequent complaints from victims who have responded to deceptive advertisements through on-line classifieds and other sites, in relation to items such as cars, caravans, jewellery, pets and the like which are purported to be located in Australia. The victims were deceived into sending money (up to $30,000) overseas (mostly via WU) to offenders who have no intention of providing the item in exchange.

There is little Australian law enforcement can do for these victims other than trying to target harden them so they do not fall victim to further scams. The offenders use false names, public domain emails and are overseas. The money, once sent via WU can be picked up immediately from any WU outlet in the destination country, usually by 'runners' carrying false identification.

Stolen or compromised Credit Card Numbers used by overseas offenders to obtain goods/cash from NT businesses

Bulk numbers of credit card details have been compromised in the last few years, particularly from firms in the United States of America. These credit card details are used by overseas offenders, often from West Africa or Asia, to make on-line orders of goods from NT businesses. The business bears the loss when the genuine cardholder's bank charges the transaction back. NT Police receive regular complaints of these transactions.

Credit Card Skimming/ATM Skimming

Despite two recent media articles claiming that skimming machines were installed on a number of Darwin Automated Teller Machines (ATM), this is not the case. The NT was not hit by the recent spate of ATM skimming in the country.

Similarly, while there is no known incidence of credit card skimming in the NT, the NT was visited by 'shoppers' associated with an organised crime group from Malaysia, carrying counterfeit credit cards cloned in New South Wales and Victoria from credit card data skimmed in Malaysia. Four offenders were arrested by NT Police in relation to this matter, successfully prosecuted for forgery and deception offences and sentenced to imprisonment.

To date there are no incidents of skimming or possessing of skimming equipment or counterfeit credit card making equipment in the NT.

Fraud facilitated by the on-line environment

In 2008 NT Police investigated and prosecuted a New South Wales man for obtaining $95,000 by deception from the Territory Insurance Office under a work cover policy, and a further attempt deception on a second local insurance company. The offender used his computer to manufacture documents and certificates sufficient to identify himself under various assumed names. He registered companies and opened bank accounts under those names. He then applied on-line with numerous insurance companies around the country for work cover policies on behalf of each of those companies, each of which he claimed had only one employee (whichever false name he was using).

Shortly after each policy was accepted the offender would purport that he was injured, manufacture medical certificates, and forward his claim to the insurance company. His claims were almost always accepted. This fraud could not have worked except that the offender was able to deal with the insurance companies almost entirely via computer. Using this methodology over a three year period the offender was able to obtain approximately $1 million from insurance companies around Australia. He is presently serving 21 months of a three year five month sentence in the NT. Queensland Police will seek to extradite him at the conclusion of his NT sentence.

Malicious Attack on Computer Network

In 2008, the NT Police investigated and prosecuted an offender for maliciously remotely hacking into the NT Government computer system, shutting down several servers, deleting 10,000 user accounts, and adversely impacting on the provision of government services, in particular those of Royal Darwin Hospital, Darwin Prison and the Supreme Court. Attempts were also made to attack servers of the PowerWater Corporation and NT Police, Fire and Emergency Services. The offender had been recently dismissed by the company contracted to provide computer services to the NT Government. The offender was sentenced to three years and four months imprisonment with a 12 month non-parole period.

b) The implication of these risks on the wider economy, including the growing economic and security impact of botnets.

c) Level of understanding and awareness of e-security risks within the Australian community.

Despite repeated warnings issued by NT Police and other agencies through the media, the level of awareness of the general public remains low. People seem to lose objectivity when dealing with people on-line, and have no qualms about sending money to people they do not know as a result of an on-line transaction.

People and businesses have difficulty keeping their virus/spyware protection up to date on their home and business computers.

d) Measures currently deployed to mitigate e-security risks faced by Australian consumers.

i) Education initiatives.

NT Police regularly provides media releases, often in conjunction with the NT Office of Consumer Affairs.

ii) Legislative and regulatory initiatives.

The NT needs to look at current legislation regarding various aspects of credit card skimming and cloning as there are currently some deficiencies.

iii) Cross-portfolio and inter-jurisdictional coordination.

Inter-jurisdictional Police coordination and liaison is vitally important in relation to cyber crime. The regular meeting of the Heads of State and Territory Fraud Units and the High Tech Crime Managers Group is imperative to foster close and efficient liaison and cooperation between the jurisdictions.

iv) International co-operation.

International co-operation is problematic. Obtaining a police response from another country in a timely manner can be difficult.

It was hoped when the Australian High Tech Crime Centre (AHTCC) was established in 2003 that it would provide a liaison with international police and help coordinate offences from the Australian end and refer them overseas. From an NT Police perspective the AHTCC appears to be focussed primarily on internet banking fraud and is not in a position to offer substantial assistance in the other areas described above.

e) Future initiatives that will further mitigate the e-security risks to Australian internet users.

f) Emerging technologies to combat these risks.

Yours sincerely

PAUL HENDERSON

7/3/9