Computer Crime in New Zealand

by Nigel Hanson

The use of computers in New Zealand businesses is increasing. Therefore it makes sense that there will also be an increase in the number of cases of computer crime being reported to the police. This assumption, which I made in November 1992, led me to the decision to write my fourth year university dissertation (in 1993) on computer crime in New Zealand. This article describes some of the findings from the cases I analysed, along with methods and policies that I believe could have been used to prevent the crimes occurring in the first instance. Also described is the response I received from both the police and banks in New Zealand when I contacted them for cases to study.

The Search for cases

From the articles I have read and common sense, I knew that obtaining cases to study would be difficult. The numerous requests that I sent out over a six month period (November 1992 - May 1993) stated that measures could be taken to secure sensitive information if this was desired or required.

Letters were sent to the Dunedin, Christchurch, Wellington and Auckland Criminal Investigation Bureaus (CIBs). Both the Dunedin and Wellington CIB stated that they had not received any complaints of computer fraud through their offices. A detective from the Christchurch CIB admitted that he did have knowledge of cases of computer crime that had occurred in New Zealand banks. However, although he would have liked to assist, he felt that disclosing information about previous cases may jeopardise the level of co-operation received from the banks in future cases. To date the Auckland CIB have not replied.

The New Zealand Serious Fraud Office, the Security Intelligence Service, and the Government Communications Security Bureau (GCSB), were also contacted, but once again they were all unable to assist. However, Malcolm Shore from the GCSB did supply a number of overseas cases to study and numerous security related articles, which proved to be very helpful.

From the replies I received, I reached two important conclusions. Firstly, businesses in New Zealand appear to be reluctant to report instances of computer crime to the police. Loss of confidence with their shareholders and customers is possibly a major reason for the low reporting rate. The second conclusion was that even if the police did have knowledge of cases of computer crime that have occurred, they were very reluctant to tell anyone even the barest details. I assume that this is because their investigations are based on the understanding that information given to the police by complainants will remain confidential. It is understandable that the police cannot betray this trust.

Five banks were sent requests for cases to study, four of which replied. Two banks made it quite clear that it was against company policy to release any information regarding cases of computer crime that have occurred in their organisations. The other two claimed that '... we have not experienced computer crimes of consequence...' and '... problems tend to be of a petty clerical nature'. It seems unusual that two banks obviously have had trouble with computer crime in the past, and the other two have not. Either way it was obvious that the banks contacted did not want anyone to know whether there have in fact been any cases of computer crime in their organisations. This could be because they feel that if they admit that a computer crime has occurred in the past, then they could be a target for further attack from people checking to see if the security has been updated.

New Zealand cases

A total of 17 cases of computer crime were identified after several months of research. The cases were reproduced in my dissertation with permission from the New Zealand Computer Society from a paper titled '*Computer Fraud: Prevention and Detection of Fraud in a Computing Environment*'. The paper was present by Mr Peter Doone and Mr Phil Royal during March and April 1990.

After studying the 17 cases, I was able to make a number of generalised conclusions about computer crime in New Zealand. These are described below.

- The size of the companies that were involved in the cases varied, but it appears that large financial companies such as banks are more susceptible to computer crime. A possible reason for this is the size of the potential gain if the perpetrator is successful. The sheer size of an organisation such as a bank also means that small discrepancies would be more difficult to trace.
- None of the crimes described in the cases involved very inventive

methods to carry out the crime. The perpetrators often used flaws in the security of the computer systems to their advantage. This also highlights the fact that nearly all of the crimes were an 'inside job'.

- The majority of offenders were either managers or senior staff within their company. Management and senior staff are usually the last to be suspected, but are in fact the people in the best position to commit a computer crime.
- The time until the crime was discovered varied tremendously. The fact that some of the crimes managed to survive a number of audits indicates that computer crimes may not be being actively looked for by auditors. In one case, where a 14 year old boy committed an Automatic Teller Machine (ATM) fraud, it wasn't until the boy confessed to his school teacher that the bank even knew that the crime had been committed.
- Probably the most startling fact has been left until last. Where the estimated loss was given, the average loss to the company or organisation was more than $480,000.

Preventing the Crimes

Nearly all of the documented New Zealand crimes could have been prevented, often by having simple policies in place. Below are some general recommendations which I believe *may* have prevented the crimes from occurring.

- Access to the source code for computer programs should be tightly controlled. Changes to programs should be automatically logged and the details of changes should be clearly documented by the programmer involved.
- Financial systems such as payroll records should be regularly audited to check for discrepancies, such as fictitious employees or excessive payments to staff members.
- In the case of banks or other organisations where employees can have credit or investment accounts, it should not be possible for an individual to access or operate their own account. Any dealings with their account should only be able to be done through a senior member of staff. This restriction should be implemented both at an administrative and technical level.

> *"Nearly all of the documented New Zealand crimes could have been prevented, often by having simple policies in place"*

- Fictitious suppliers or employees are often entered into databases in order to obtain payments dishonestly. Restricting who can enter data can help reduce the risk of this happening. Although authenticating every employee or supplier may be time consuming, it would be advantageous to do this.
- When employees have their employment terminated, they should be escorted off the premises. Measures such as invalidating their user code should be undertaken prior to their dismissal. Once dismissed, they should not be permitted anywhere near the computer system.
- When confronting a person suspected of a computer crime/ fraud, the element of surprise should be used. It is preferable that the suspect is nowhere near the computer when he or she is confronted. The person should not be pre-warned as it only takes a split second for evidence stored in magnetic form to be destroyed.
- Call-back verification and a limit on the number of unsuccessful logins should be standard on all computer systems that have dial-up access. Call-back verification automatically disconnects a user after the person has logged in, and then calls the user back at the telephone number that the computer system has recorded for that user. Limiting the number of unsuccessful logins means that if somebody repeatedly tries to break into a computer system, they will soon find that the modem will not answer the phone.
- Where procedures are in place to prevent security breaches, corresponding penalties should also be in place. Employees should be warned of the penalty of breaking a procedure, and should not be let off with a warning. There is no point having procedures if they are not actively enforced.
- When transferring funds, whether it be from one branch to another or across the world, both the sender and receiver should be authenticated and their financial status assessed. Once the money is transferred, it is nearly impossible to retrieve the money if it is intercepted before it reaches the rightful receiver.

Conclusions

The management of many New Zealand companies are realising that timely and accurate information is a necessity in today's business world. What they must also realise is that they must protect their information just like they would any other asset. Computer security should be looked at as an investment and not as a cost.

The current level of reporting computer crime and fraud is very low in New Zealand. This may give companies a false sense of security. Companies may believe that if computer crime and fraud are not being reported, either to the police or through the media, then it does not exist. It is time that companies realised just how much they can potentially lose if they do not protect themselves.

Overseas experience indicates that New Zealand is not unique in having a low rate of reporting of computer crimes. My final conclusion regarding computer crime is quite simple: Everyone wants to prevent it - but nobody wants to talk about it. Hopefully articles such as this one will highlight the fact that Computer crime is occurring in New Zealand and should be addressed more seriously. ✍

Nigel Hanson, ANZCS, is a systems analyst with the Southern Regional Health Authority (SRHA), Dunedin. This is an abstract from his dissertation which has been submitted for his Bachelor of Commerce degree with honours in Information Science at the University of Otago, Dunedin, New Zealand.

Proceedings
of the New South Wales Society for Computers and the Law

PAST COPIES OF THE PROCEEDINGS ARE NOW AVAILABLE.
THIS IS YOUR CHANCE TO COMPLETE THE SET!

Volume	Year	Cost ($)	Please ✓ if required
Volume 1	1983	20	
Volume 2	1984-5	20	
Volume 3	1986	20	
Volume 4	1987	20	
Volume 5	1988	20	
Volume 6	1989	20	
Volume 7	1990	20	
Volume 8	1991	20	
SPECIAL Volumes 1-8		80	
Volume 9	1992	25	

Please make all cheques payable to:
NSW Society for Computers & the Law

Please send your cheque and the completed
form to Diana Gould,
The Proceedings Editor,
NSW Society for Computers & the Law,
c/- Clayton Utz,
No 1 O'Connell St, SYDNEY NSW 2000,
DX 370

NAME: ______________________ POSITION: ______________________

FIRM/COMPANY: ____

ADDRESS: ____

______________________ POSTCODE: ________ STATE: ________ DX: ________

SIGNED: ______________________________________ DATE: ____________