



90  
"Australian attitudes  
towards  
computer crime."

Paul John Sullivan  
B. Comm. (Newcastle)



Submitted as full requirement for an award of  
**Master of Business**  
within the Faculty of Business  
and the Department of Business Computing  
of Victoria University of Technology.

FTS THESIS  
364.1680994 SUL  
30001004467751  
Sullivan, Paul John  
Australian attitudes towards  
computer crime

**Declaration**

This thesis does not incorporate, without acknowledgment, any material previously submitted for a degree in any University, College of Advanced Education, or other educational institution and to the best of my knowledge and belief it does not contain any material previously published or written by another person except where due reference is made in the text.



Paul J SULLIVAN

**Acknowledgments**

I would like to acknowledge the support and assistance of Assistant Commissioner Christine Nixon (NSW Police Service), Mr David Bradley (Dean, NSW Police Academy) and Sgt Bob Marquet (NSW Police Academy) regarding access to data. Further, I would like to thank Mr Ian Hayward (Department of Business Computing, VUT) and Dr Roger Coldwell (Visiting Professor, ACARB-RMIT) for their supervision and help. In turn, I would like to thank Dr Jo Coldwell (University of Newcastle) for her advice regarding statistical analysis methods used in this research and Mr Alan McFarlane for the sponsorship of the GIO regarding computer hardware and software. Most importantly, I would like to thank my wife, Karen, and my children, Emma, Bethany and Sean, for helping me to concentrate on the task and providing the opportunity for me to do so.



Paul J Sullivan.

**Table of Contents**

i	<b>Title Page.</b>
ii	<b>Declaration.</b>
iii	<b>Acknowledgments.</b>
iv	<b>Table of Contents.</b>
viii	<b>List of Appendices.</b>
x	<b>List of Tables.</b>
xi	<b>Abstract.</b>
1	<b>1.00 Introduction.</b>
2	Origins of information technology.
2	Life with Computers.
6	Security problems with Computers.
8	What is Computer Crime?
10	Computer Fraud.
11	Software Piracy.
12	Credit card fraud.
13	Hacking.
14	Motivation for Hacking.
17	Ramifications of computer crime.
21	Organised Crime and Computer Crime.
22	Confidentiality.
24	The Incidence and Cost of Computer Crime.

27		The Global Situation.
28		How does one identify a hacker?
31		Computer criminals attitudes.
31		Research into Australian attitudes.
36		Hypotheses to be tested.
37	<b>2.0</b>	<b>Methodology.</b>
38		Background.
39		The population.
40		Objectives.
40		Limitations.
41		Sample size.
42		The hypotheses being tested.
43		Contingency tables.
43		Chi-squared tests.
44		The questionnaire.
47	<b>3.0</b>	<b>Results</b>
48		Respondents' ranking of computer of computer fraud against other offences.
48		Respondents' ranking of credit card fraud against other offences.
49		Respondents' ranking of hacking against other offences.
50		University respondents' ranking of hacking as a crime according to sex.

50		Male university respondents' ranking of hacking as a crime according to academic status.
51		Female university respondents' ranking of hacking as a crime according to academic status.
51		University staff's responses to copying software as a crime according to sex.
52		University students' responses to copying software as a crime according to sex.
52		University students' responses to copying software as a crime according to user status.
53		University staff's responses to copying software as a crime according to user status.
59		Overview.
61	<b>4.0</b>	<b>Discussion</b>
62		Findings and discussion of hypothesis one and hypothesis two.
67		Findings and discussion of hypothesis three.
69		Findings and discussion of hypothesis four.
70		Findings and discussion of hypothesis five and hypothesis six.

72		Findings and discussion of hypothesis seven and hypothesis eight.
73		Findings and discussion of hypothesis nine and hypothesis ten.
73		Reporting of offences to police.
75	<b>5.0</b>	<b>Conclusions</b>
77	<b>6.0</b>	<b>Further research.</b>
78	<b>7.0</b>	<b>Bibliography and References.</b>

**List of Appendices**

- |    |                    |  |
|----|--------------------|--|
| 86 | <b>Appendix 1</b>  | A questionnaire.   |
| 87 | <b>Appendix 2</b>  | A questionnaire.   |
| 88 | <b>Appendix 3</b>  | Respondents' ranking of computer fraud against other offences.                             |
| 89 | <b>Appendix 4</b>  | Respondents' ranking of credit card fraud against other offences.                          |
| 90 | <b>Appendix 5</b>  | Respondents' assessment of hacking.  |
| 91 | <b>Appendix 6</b>  | University respondents' ranking of hacking as a crime according to sex.                    |
| 92 | <b>Appendix 7</b>  | Male university respondents' ranking of hacking as a crime according to academic status.   |
| 93 | <b>Appendix 8</b>  | Female university respondents' ranking of hacking as a crime according to academic status. |
| 94 | <b>Appendix 9</b>  | University staff's responses to copying software as a crime according to sex.              |
| 95 | <b>Appendix 10</b> | University students' responses to copying software as a crime according to sex.            |
| 96 | <b>Appendix 11</b> | University students' responses to copying software as a crime according to user status.    |
| 97 | <b>Appendix 12</b> | University staff's responses to copying software as a crime according to user status.      |
| 98 | <b>Appendix 13</b> | Survey by Coldwell of teachers re hacking according to sex.                                |
| 98 | <b>Appendix 14</b> | Survey by Coldwell of teachers re hacking according to discipline.                         |

99	<b>Appendix 15</b>	Survey by Coldwell of teachers re hacking according to age.
99	<b>Appendix 16</b>	Survey by Coldwell of teachers re hacking according to faculty.
100	<b>Appendix 17</b>	Survey by Coldwell of social science students and their responses to the ethics of hacking.

**List of Tables**

- 29 **Table 1** Summary: The number of computer crime incidents in the United States of between 1988 and 1993 (see Chapt 1).
- 33 **Table 2** ACARB's perpetrator classifications (see Chapt 1).
- 54 **Table 3** Respondents' ranking of computer fraud against other offences (See Chapt 3).
- 54 **Table 4** Respondents' ranking of credit card fraud against other offences (see Chapt 3.0).
- 55 **Table 5** Respondents' assessment of hacking (see Chapt 3).
- 55 **Table 6** University respondents' ranking of hacking as a crime according to sex (see Chapt 3.0).
- 56 **Table 7** Male university respondents' ranking of hacking as a crime according to academic status (see Chapt 3).
- 56 **Table 8** Female university respondents' ranking of hacking as a crime according to academic status (see Chapt 3).
- 57 **Table 9** University staff's responses to copying software as a crime according to sex (see Chapt 3).
- 57 **Table 10** University students' responses to copying software as a crime according to sex (see Chapt 3).
- 58 **Table 11** University students' responses to copying software as a crime according to user status (see Chapt 3).
- 58 **Table 12** University staff's responses to copying software as a crime according to user status (see Chapt 3).
- 66 **Table 13** Summary of estimates of crime and justice. (see Chapt 4)

**Australian attitudes towards computer crime****Abstract**

This investigation compares the responses of university staff and students of a Faculty of Business with those of the staff and students at the New South Wales Police Academy, in Goulburn. The research tested the attitudes of the respondents to computer fraud, credit card fraud, copying software and hacking into computer systems. The research found, from questionnaire responses, that computer crimes are considered to be insignificant compared with other crimes which have far less impact on society in financial terms. Hacking, in particular, which costs Australian society an increasing amount each year, was ranked at a very low level of significance. Further, the research found a significant difference between the university and police responses to whether or not hacking and copying software are considered to be criminal activities.

From this thesis arise other matters which need to be addressed in the future, particularly the origins of these attitudes. It asks whether we should address the problem that is posed, earlier in the educational lives of our children. With this in mind, it asks whether we should address the problem earlier than at a tertiary education level. Whereas political indoctrination has worked in a number of extreme cases elsewhere in the world, we do not seem to contemplate using anything like these draconian methods in the case of combating crime.

## 1.0 INTRODUCTION

Origins of information technology.  
Life with computers.  
Security problems with computers.  
What is computer crime?  
Computer fraud.  
Software piracy.  
Credit card fraud.  
Hacking.  
Motivation for hacking.  
Ramifications of computer crime.  
Organised crime and computer crime.  
Confidentiality.  
The incidence and cost of computer crime.  
The global situation.  
How does one identify a hacker?  
Computer criminals attitudes.  
Research into Australian attitudes.  
Hypotheses to be tested.

## **Origins of information technology.**

In 1820, Charles Babbage began a project to create a machine that would solve long and complicated mathematical calculations. If he succeeded in creating such a machine, it would eventually re-define our way of life thereby altering many aspects of our existence. Fifty-years after commencing this project, he had not yet achieved his goal. However, when he died in 1871, little did he realise that he probably laid the foundation for a computer age. His successors continued his work and, before the end of the nineteenth-century, several calculating machines had been developed. Vindication of all of Charles Babbage's work came in 1943, some seventy two years after his death, when Harvard University switched on the Mark I digital computer and a computer age was upon us. However, within several decades computers were being used for a more macabre purpose, namely in the commission of crime.

## **Life with Computers.**

Computer technology has changed our lives over the last fifty years, the way that we think and the way that we live with it. Computers are now viewed as an essential part of western civilisation and we have become largely dependent upon them. We can only imagine the capacity and the horizons for current and future development of computer technology but, with the affordability of personal

computers, the simplification of computer languages and the education of computer users, our dependence on computers will continue to develop. Already, our banking and financial sectors rely heavily upon computers for the electronic transfer of funds between organisations and individuals. Marriott (1988) estimated that about thirty billion dollars is turned over each day on the Australian foreign currency market alone. Marriot (1988) estimates that a modern bank cannot survive for more than two or three days without using its data processing system. He uses the example of Westpac when it accidentally lost the use of its ATN network. He also highlights the turnover of Electronic Funds Transfer (EFT) networks in the world which, he estimated, transfers about five thousand billion dollars per day.

Sessions (1991) quotes figures of well over eighty per cent of all American daily financial transactions taking place via electronic funds transfers. Australia is obviously moving in this direction. It is not only the commercial sectors of our society which are computer dependent. Computers control an increasing number of aspects of our lives from point switching and scheduling of buses and trains to the control and monitoring of traffic lights and air travel, from telecommunications to credit, from the maintenance, collection and dissemination of domestic and international intelligence to the execution of military campaigns. From my personal experience it is difficult to

buy a home delivered pizza without divulging all of one's private details for entry onto pizza supplier's database. Some of that information is then analysed for marketing purposes however, the bulk of the confidential and personal information is retained for the use of the employees. Such information as the purchaser's telephone number, name and address are stored on a private database. Further, it is difficult to enter a competition without divulging details of what products one purchases. Have you ever applied for a loan and had a total credit reference check? Many private and public institutions have a database which contains private and confidential information which is valuable to them and possibly to others. Further, the nature of this situation offers a very tempting avenue for abuse by criminals. This was seen in an investigation by the New South Wales Independent Commission Against Corruption (ICAC) who recommended for prosecution a number of New South Wales public servants who accessed and sold confidential information to interested parties which included major banks and international corporations, Roden (1992).

When a computer system becomes unreliable it only emphasises its vulnerability. Such was the case in 1994 when the telephone system and data storage systems at the Australian Security Intelligence Organisation (ASIO), Australia's internal intelligence organisation, were compromised (Anon, 1994a). All of ASIO's activities were totally paralysed and shut down after it was found that the internal telephone

system and the computer and data storage systems may have been penetrated by possibly hostile persons. To restore the reliability and confidence in its systems, ASIO had to replace its system totally at an incredible cost to Australian taxpayers.

An accidental cut in the lines of communication between the central computer system and bank automatic teller machines in France (Anon, 1993d), caused chaos when people could not access their funds or obtain credit. It resulted in the collapse of their credit card system when forty per cent of France's automatic teller machines were cut off and isolated from the central computer system.

In the future, we can look forward to direct electronic purchasing, new electronic information systems for banking, communications satellites, communicating with consumers, home communications and domestic computerisation. But at what cost to society at large? It is the realisation of this total dependence on computer technology that generates questions like "What would happen if we could no longer depend upon the reliability of computers" and "What would happen if this vulnerability was exploited by the criminal world?" I believe that the realisation of these problems is with society now. The credibility of society's computer systems is being jeopardised.

## Security Problems with Computers.

As highlighted by Johnston (1991), "The scope of computer related crimes is restricted only by the ingenuity of the criminal" (see also Bequai, 1987). As computer technology races ahead, so increases the number of people who are computer literate and, therefore, the number of computer related crimes. As computers have become essential household and office fixtures, the vulnerability of computers has increased considerably and left a door open for people who would capitalise on society's weaknesses for their own benefit. It is not that society has a new breed of offender. My Police experience reveals that in some instances, the ever adaptive criminal has moved away from traditional offences to an easier target (See Eysenck, 1977). I believe that the victims of computer related crime are reluctant to report the commission of the offence preferring to keep the matter confidential rather than risk embarrassment and scorn. This is an ideal scenario for criminals with the attraction of a low risk of detection and an apathetic attitude of potential victims. The very nature of computing assists criminals in its exploitation.

Some of the features which give rise to its exploitation are:

- a. A computer will execute all given instructions no matter how illegal.
- b. It is difficult to anticipate what a computer

is doing with the data that it holds.

- c. Because of the speed of a computer, infiltration of the operation can be carried out equally quickly.
- d. Whatever security systems have been implemented, certain people must have unlimited access to it.
- e. Haphazard key presses - even by a child - can be accepted by a computer.
- f. Because of a computer's accuracy and speed, the results from the computer are more readily believed than if that same information came from another source.
- g. A computer often allows an offender to commit a crime in complete anonymity. If offenders instruct a computer that they are a particular person by using another person's password or features, it will assume that you are that person and allocate to them all of that person's access rights.
- h. Many people in upper management are computer illiterate and, therefore, do not understand the need for, and the intricacies of computer security. Many have been trained pre-computer and therefore they do not have the necessary appreciation of its uses and abuses.
- i. People at a corporate level in organisations are not particularly concerned about computer security which has to compete with other

aspects of their corporate budget (see Coldwell & James, 1993)

### **What is Computer Crime?**

The term computer crime has been used as a broad term for the combination of a number of offences, some of which are computer fraud, hacking, and software piracy. In this context, a computer can be viewed as either the tool which is used to be able to commit the offence, as in the case of an embezzler, or as the means by which the offence takes place. This would be the case where unauthorised access is gained to data processing systems. One of the most widely read documents on the topic of computer crime is a report of the Scottish Law Commission on Computer Crime which was published in 1987, Marriott (1988). Out of that document came eight categories of computer crimes:

- a. Erasing or falsifying data or programs to obtain a pecuniary or other advantage.
- b. Obtaining unauthorised access to a computer.
- c. Eavesdropping on a computer.
- d. Copying of information without its physical removal.
- e. Unauthorised borrowing of computer discs or tapes.
- f. Making unauthorised use of computer time or facilities.
- g. Malicious or reckless corruption or erasure of

data or programs.

**h.** Denial of access to authorised users.

Kamay (1992) has extended the above definition to include the following elements of computer abuse, in Australia, by identifying:

- a.** Unauthorised manipulation of computer input and/or output.
- b.** Unauthorised access to the system through terminals or micro-computers.
- c.** Unauthorised modification or use of application programs, operating systems or computing equipment.
- d.** Trespass on data processing installation, theft of equipment, files or output.
- e.** Sabotage of computer installation, files, application programs or operating systems.
- f.** Unauthorised data interception.

In the Criminal Law Journal, Roden (1991) refers to the *International Handbook on Computer Crime* which was produced in 1986. In that document, there are three categories which give a broader explanation of the variety of computer offences. These categories and sub-categories are:

*Category One*

*Computer Related Economic Crimes*

- a.** Fraud by computer manipulation.

- b. Computer espionage and software piracy.
- c. Computer sabotage.
- d. Theft of services.
- e. Unauthorised access to data processing systems and hacking.
- f. The computer as a tool for traditional business offences.

*Category Two*

*Computer Related Infringements of Privacy*

- a. Use of incorrect data.
- b. Illegal collection and storage of correct data.
- c. Illegal disclosure and misuse of data.
- d. Infringements of formalities of privacy laws.

*Category Three*

*Further Abuses*

- a. Offences against state and political interests.
- b. The extension to offences against personal integrity.

**Computer Fraud.**

Computer fraud is merely a new term for an old offence. From my experience, rather than erasing or falsifying data which is recorded on hardcopy and other records, offenders

have now adapted to the computer age and falsify and erase data which is stored within a computer system.

What could also be included within this category is the use of stored information for the pecuniary advantage of the offender. Offences which would fall within this category are insider trading and tender rigging.

### **Software piracy.**

Software piracy is an endemic social problem which seems to be here to stay. In general, software piracy is a term used to describe any unauthorised copying of software. Software is the set of instructions which tell a computer what to do and how to do it. It is created and owned by people who expect the users of their creation to pay through a licensing agreement for that right to do so.

As the cost of computer hardware, which includes the computer, printer and visual units, has declined, the importance and monetary value of software, which is the operating instructions to the computer, has increased. As a consequence, copying computer software illegally has become a major concern within the industry. Within our education system Coldwell (1990a) believes that it is acceptable for both students and teachers to copy and distribute software.

Morrison (1990) advises us that, in commerce, education and

government departments, there is mounting evidence of the mass copying of software. He goes further to say that there are few individuals who can say honestly that they have never used a program for which the developer has not been properly compensated.

Unfortunately, software is being copied and distributed to computer users without the consent of the owner of the software who gains nothing from the transaction, for the years of financing research and the development of the product. Large scale piracy became a recognisable phenomenon with the demand and availability of affordable personal computers and, ever since, the producers of software have battled to stem the flood of illicit copies of their product which is running into the millions - if not billions - of dollars, Fleming (1993).

#### **Credit card fraud.**

Society's reliance on *plastic money* is probably only equalled by our reliance on computers. What was once thought of as a much safer method of transaction between vendor and purchaser, when compared with cash and cheques, is now seen as a lucrative avenue for criminals, Fleming (1993). The availability and affordability of the necessary technology to criminals has given them an ability to produce high quality forgeries of legitimate credit cards which is,

according to the Australian Federal Police, costing the card industry millions of dollars, Confidential (1993).

Credit cards were once viewed as the answer to the major problems experienced with cheques, such as dishonoured cheques and the lack of knowledge by the recipient regarding the solvency of the drawer. However, the technology that is available to criminals has made use of this once foolproof card turning it into a burgeoning criminal industry. The confidence that society has in credit cards and our reliance upon them has enabled criminals to utilise this dependence to their advantage.

### **Hacking.**

Hacking, the unauthorised accessing of a computer and the unauthorised accessing of data processing systems, is but one element of computer related crime and, according to Police, it is by far the most difficult to detect, deter and prosecute. The popular press has devoted much publicity to the many cases of unauthorised use of computer systems by outsiders, commonly called *hacking*. Hacking into computer systems is believed to have emerged in the late 1950s at the Massachusetts Institute of Technology (MIT) among a group of young male students. In Europe, hacking is thought to have started in the mid-1960's in Italy and it has since spread world wide. According to a survey conducted in 1980 by the predecessor of the *Australian Computer Abuse Research Bureau*

(ACARB), which was then known as the *Computer Abuse Research Bureau* (CARB) the earliest cases of computer abuse in Australia occurred in 1967 (see Kamay, 1992).

Computer abuse, as defined by Kamay & Adams (1992), includes the unauthorised manipulation of computer input or output, the unauthorised access to the system through a terminal, the unauthorised modification or use of application programs, operating systems or computing equipment, trespass on data processing installation, theft of equipment, files or output, the sabotage of computer installation, files, application programs or operating systems and unauthorised data interception. Put simply, a hacker is a person who gains unauthorised access to another's computer systems without their consent through the use of computer equipment. Why, then, do an increasing number of people seek to access another's computer system illegally?

#### **Motivation for Hacking.**

A former hacker, Powell (1992), wrote in the *Sydney Morning Herald* that the reason that hacking into computer systems is rife is that it is so easy to do. He advised us that, in his opinion, companies are lax and careless with their computer security. He advised too that, even when computer security is good, cracking them is simple with inside help. He stated that we can always find the complex code written

on a piece of paper somewhere as users cannot remember complex codes and, hence, they want them to be easily accessible. A general rule is that, the more secure that computer systems are made against hackers, the more difficult it is for ordinary users to work with them which, in turn, depletes real computer security considerably. (This argument is given in greater detail by James and Coldwell (1993) regarding the lack of influence of closed systems like 4GLS). Even attempts to strengthen security, by maintaining audit trails and logging incoming telephone numbers, is unsuccessful as there exist various computer programs which allow hackers to access and manipulate those numbers.

In the *FBI Law Enforcement Bulletin*, Sessions (1991) stated that there are two major types of computer crime. The first is a crime in which a computer is the vehicle or the tool of a crime and the second is a crime in which a computer and the information stored in it are the targets of the criminal. In the former instance, he refers to more traditional crimes such as embezzlement, fraud and larceny. A criminal must use a computer as a vehicle to perpetrate an offence as this technology is the current mode of handling data.

The latter class of crime is unique to computers and it can be either committed internally by employees or externally by other criminals (see Kamay and Adams, 1992). The external

threat usually involves the use of telecommunications to gain unauthorised access to a computer system and it is this type of offence that involves penetration by a hacker.

There appears to be three types of computer hacker. The first, and probably the largest group, is people who break into computer systems for a combination of intellectual and egotistical reasons. They break into systems for no other reason than to see if they are capable of doing it. While having access to the system, they explore and then depart without deliberately stealing, erasing, altering or destroying data.

The next group of hackers is those which access computer systems illegally to steal, erase, alter, destroy, disrupt and interrupt the system. Their motivations are usually malicious by nature without being, necessarily, for financial gain.

The last, and probably the most serious, group of hackers is by far the most dangerous. This group of people pose a very real threat to the financial sector, commerce and national and international security. They are professional criminals who use specialised skills to steal information, manipulate data and, so, cause major disruption to the system. By so doing, they have a potential for damaging the function and potential of society's information systems, simply by making it unreliable.

## The Ramifications of Hacking.

Although the *explorer* class of hacker does not access a computer system with an intention of causing damage or disruption, their desire to explore randomly can, by its sheer nature, inadvertently lead to major problems within a system. Normally, these hackers only look around to satisfy their curiosity and then depart from the system. Unfortunately, things do not always develop as planned.

Such was the case highlighted in the *Daily Telegraph Mirror* (Anon, 1993a) when hackers penetrated a Commonwealth Scientific and Industrial Research Organisation (CSIRO) system thereby threatening the organisation's reputation. Only one of the computer systems at eleven CSIRO research sites had adequate security procedures according the Australian National Audit Office (ANAO).

The first of the security breaches was detected in 1991 followed by others in 1992 and 1993. In a report to the Senate, the ANAO stated that they believed that these breaches were enacted by hackers who trespassed for fun rather than for material gain. Other similar incidents are an intrusion into the computer system of NASA in 1993, causing them to shut down for twenty-four hours after an unnamed hacker accessed the system using a correct password. On his arrest, a former university student also admitted intruding as a hobby into the systems at the CSIRO and

universities' computer systems at Wisconsin, California and Indiana (Anon, 1993b).

Robert Morris caused six-thousand computer systems to crash when he *accidentally* released a worm into the Arpanet network (Powell 1992). Robert Schifreen and Steve Gold hacked into British Telecom and, finding the passwords for their subscribers, they hacked into the electronic mail box of the Duke of Edinburgh (Powell 1992). Paul Bedworth was arrested after using a four-hundred dollar computer bought as a birthday present to hack into the computer systems at the White House, the Tokyo Zoo and the *European Organisation for the Research and Treatment of Cancer*. The latter's computer networks broke down because of his activities. Other victims included major banks and a Swedish Telephone system which crashed because its network became overloaded (Anon, 1993c).

The next group of hackers are *vandals* whose objective is to cause chaos rather than to achieve financial gain. These people, who usually have some past association with their victims, often have a score to settle with them and their actions are an attempt to gain revenge. Retribution by the hacker can be achieved either internally, by introducing a virus into a computer system, or by erasing, altering or deleting data. It can also be achieved externally, through telecommunications mode after access to the computer system has been gained. This situation is highlighted by Raethal

(1994) who refers to a virus, which has a potential to erase computer files, that was being circulated to unsuspecting Higher School Certificate students through a bogus study guide available on various Sydney bulletin boards. The file passes scan tests for viruses but, once it was installed, it generated at least nine other corrupt files which had the potential to cause a considerable loss of data. The study guide was written by an anonymous person who posed as a past examination marker and it is believed that the virus was both, directed at children, and created by children.

A final group of hackers might be called *professionals* as their main motivation is monetary gain. Their aims include terrorism, blackmail, national and international espionage, military action, commercial rivalry and theft to name but a few. Foreign powers, organised crime, the financial and industrial sectors and various interest groups are but a few who resort to the use of hacking for these purposes (see Bequai, 1987, and Coldwell, 1987). Typical of this is an incident reported in the *Daily Telegraph Mirror* (Anon, 1994b) where a hacker obtained thousands of secret telephone numbers including those of the British Royal Family and the British Prime Minister, Mr John Major, by penetrating a database of *British Telecom*.

It was cited by the *Daily Telegraph Mirror* (Anon, 1994c) that the *Independent Newspaper* reported a hacker obtaining sensitive information about *British Intelligence* from a

database at *British Telecom* and sending the numbers out on a global Internet network making them available to millions of others. The hacker, who was not identified, possessed telephone numbers and addresses for secret defence installations, counter intelligence personnel and details about a United States defence communications centre. The telephone numbers, which were divulged, included the private lines for the Prime Minister's London residence, Buckingham Palace, Princess Diana's home at Kensington Palace and information about a bunker that the Government would use in the event of a nuclear war. *British Telecom* had failed to find any evidence of hacking and it is believed that access was obtained through lax security and access to employee's passwords. Private information relating to Lady Diana Spencer and the costs associated with her marriage to Prince Charles were published in European magazines after this information was illegally gained by a hacker.

Other more sinister examples of the use and scope for hacking are that a hacker was arrested and charged with stealing Air Force secrets that included a list of planned targets in a hypothetical war (Robotham, 1994).

Three West German hackers were discovered providing the Soviet *KGB* with information from military and industrial computers in the USA, UK and ten other countries (Lane, 1989). An investigation was initiated by ASIO and the Defence Signals Directorate after it was alleged that a

foreign power sabotaged a system within the Department of Immigration. Information was received of a possible high level computer breach which led to valuable details on suspected terrorists being erased. This severely hampered ASIO's investigation into a 1992 attack on the Iranian Embassy, in Canberra, and the movements of suspected foreign spies. The sabotage took place moments before a list of possible suspects in the embassy raid could be retrieved from the Immigration Department's computer (see Miranda, 1994).

#### **Organised crime and computer crime.**

Both Federal and State Police believe that organised crime will move towards computer crime, credit card fraud and hacking in particular, not only because of its ease but because of the potential rewards and the low risk of being detected. The rapid pace of computing technology, the availability of the equipment and the reduction in cost of essential equipment has given rise to an emerging area of fraud, namely, credit card fraud. New technology has given the criminal element the means to tap into a rich avenue to exploit.

The Australian Federal Police and the New South Wales Police have both highlighted the involvement of international organised crime in the areas of credit card fraud, particularly that of counterfeit cards. They believe that

to date, overseas law enforcement agencies have commented that the impact of credit card fraud upon Australia is small in comparison to Asian countries. However, as these countries intensify their efforts to reduce credit card fraud, it forces the criminals to look elsewhere, and, consequently, organised criminals find Australia as an attractive target.

The United States Secret Service has warned Australia that it is a target for a massive international counterfeit credit card operation (Warnock, 1994). They believe that Australia has been trialled and this has been substantiated by the arrest of persons by the New South Wales Police Fraud Section. With other government and non-government institutions utilising the plastic card to provide credit services, health cover, identification, security facilities to name but a few, it will be only time that delays these industries from being subjected to credit card fraud and plastic card crime.

With public apathy and the ignorance of the plastic card industry, the potential for lost revenue and instability is immeasurable.

### **Confidentiality.**

The potential for using and abusing confidential and embarrassing information was highlighted by Coldwell (1987)

regarding the use of a database by brothels in the USA which networked with other brothels via a modem and then pooled the information. This potentially volatile information could be used to extort monies from brothel users by blackmail.

To a lesser extent on the scale of terror, but no less legally and ethically incorrect, are those who trade in information. There are people who access and sell confidential information to various interested groups about individuals and companies for pecuniary gain. Typical of this situation is the ICAC exposure of the New South Wales Government's lack of security regarding government-held confidential information regarding individual Australians, Roden, (1992).

The ICAC exposed a multi-million dollar trade in confidential information involving various arms of the Public Service. Their investigation revealed a total disregard, by those who are trusted with this information, who then used this access to information for their own financial benefit. The investigation found that one hundred-and-fifty-five people and organisations, which included many of the major commercial forces in Australia, had engaged in corrupt conduct and that a further one-hundred-and-one people and organisations had engaged in conduct liable to allow or cause corrupt conduct. It was recommended to the Director for Public Prosecutions that

charges be laid against one-hundred-and-eight people.

### **The Incidence and Cost of Computer Crime.**

Australia, like much of the rest of the world, lacks accurate computer crime statistics due mainly to the reluctance of victims to come forward and report the offences. Another reason for the lack of available statistics is that both State and Federal government bodies will not make them available to the public. ACARB provides data related to *known* computer crimes, in Australia, but it can only estimate the true extent of this type of crime. The figures that are publicised by ACARB represent those crimes that are *reported* and they don't represent the number of offences that go undetected and unreported, Coldwell (1991). The reasons for the reluctance of victims of computer crime to report the matter to Police are varied but it seems to be due to a desire to avoid adverse publicity which could affect consumer and shareholder confidence and possible repercussions against their management.

We, in Australia, can only estimate the extent and cost of computer crime. But, when a survey conducted by Griffin, Rowe and Associates (Stephens, 1990), a legal firm specialising in fraud, reports that up to 25% of the workforce from board level down, are actively seeking opportunities to defraud on a regular basis, and that between 2% and 5% of the gross turnover that disappears each

year would be a normal fraud factor, it would be fair to say that accurate and reliable computer crime statistics would be very useful.

There appears to be at least two schools of thought regarding the existence or otherwise of hacking. For example, some would have us believe that hacking is only a minor problem and that the alleged epidemic proportions, reported in newspapers, are a figment of the imagination of journalists, who are whipping the public into a frenzy so that they can sell papers, thereby sensationalising the situation. They would also have us believe that hacking exists among a small group of people who intrude into systems for no apparent reason other than to satisfy their curiosities. They acknowledge that it occurs but not with the frequency or degree that others would have us believe. One such person is Tapper (1989) who feels that there is a very real difference between the amount of computer crime that occurs and that which potential victims anticipate occurring. He quotes figures from the Ontario Police for a survey where 5% of respondents reported being a victim and 42% who regarded it as a problem (Morrison, 1990).

In the United Kingdom in 1986, the accounting firm of Ernst and Whinney surveyed businesses about the existence of computer crime and about a third regarded it as a serious problem although only 3% admitted that they had experienced it (Morrison, 1990). However, Tapper (1989) does relent and

admit that, by its very nature, there is a very real difference between the actual reporting of offences and the data in the survey. The other side of the story is represented by a group of people who believe that computer crime is the crime of the present and the future and that urgent attention is required to stem the tide of computer crime generally.

Probably the most reliable statistics, in Australia, are again from ACARB which has collected data on computer crime from surveys, past studies of companies, from the police and from the media. Between June 1990, and October 1991, there was a total of one-hundred-and-eighty-four incidents of computer abuse that they reported. The monetary value of twenty-nine of these incidents was known and valued at \$1,694,975.00 with an average being \$58,447.00. Of these, one-hundred-and-fifty-five cases involved viruses which had an incalculable loss. Up to the beginning of 1992, there was a total of four-hundred-and-ninety-seven cases reported with an approximate value of \$16,908,000.00 from one-hundred-and-eighty assessable cases with an average of \$93,933.00 per incident. Of these, three-hundred-and-seventeen cases had an unknown loss, Kammay (1992).

ACARB's statistics also reveal that the largest sector for financial losses belongs to the banking and financial industries which amounts to 61.6%. Their statistics also reveal that the greatest number of cases, over that period,

involved viruses which represented 65% but less than 1% of the financial losses. Theft of information increased but only fifty-three cases occurred with nineteen-cases being assessable at \$42,940.00 in total.

### **The global situation.**

Again using statistics from ACARB and Kamay (1992), a survey of one-thousand-five-hundred public and private firms in the United Kingdom, conducted over three years, revealed one-hundred-and-eighty incidents costing more than one-million pounds. Fraud accounted for seventy-three of those crimes with theft accounting for twenty-seven, hacking for twenty-six and viruses for fifty-four incidents.

Statistics from Germany, in 1987, show that there were two-thousand-seven-hundred-and-seventy-seven incidents of fraud, one-hundred-and sixty-nine due to forgery, sabotage accounting for seventy-two and hacking for seventy-two. In the *European Economic Community*, (EEC), there were one-thousand-two-hundred computer abuses worth 3,210 million francs and, in Japan in 1982, computer crime amounted to ten-million yen.

In the United States, information has been gleaned from a Department of Defence workshop, where there were thirty interest groups from eighteen United States Federal Agencies, who discussed computer crime. Captain David

Christy, a member of the Federal Computer Investigations Committee (Christy 1994), quotes figures relating to the incidence of computer hacking rising from 1.3 per 100 computers in 1989 to 1.6 per 100 computers in 1991. The total monetary damage grew from \$US81.6 million, in 1989, to \$US164.3 million in 1991. He then makes estimates and shows the number of incidents between 1988 and 1993 (See table 1).

All of these statistics are estimates, however, but it is believed (NSW Police, 1992) that only 10% of computer crime, generally, is actually reported. The cost of virus attacks is difficult to estimate due mostly to the difficulties arising from estimating the value of information lost as a result of the attack. Regrettably, an important feature is that computer crime is difficult to detect and, therefore, the arrest figures are not representative of the totality of the crime.

#### **How does one identify a Hacker?**

Powell (1992), a self-confessed former hacker, writes that a successful hacker must possess four essential qualities which, he believes, university and college students do possess. These relate to their *time*, *computer knowledge*, the *need to know* and their *access* to a network.

Table 1. Summary: Number of reported computer crime incidents in the United States of America between 1988 and 1993.

YEAR	NUMBER	PERCENTAGE OF TOTAL
1988	6	0.176
1989	132	3.864
1990	252	7.377
1991	406	11.885
1992	900	26.347
1993	1720	50.351
<b>Total</b>	3416	100

**Note:** Reproduced data from Christy (1994). Note that half of the incidents, for the period 1988 to 1993, in fact, occurred in 1993.

*Time.*

Time is needed for cracking a code and breaking into a computer network. It may take numerous attempts before a hacker succeeds in accessing a computer system and Powell believes that university and college students have the time.

*Computer Knowledge.*

Powell (1992) states that the computer skills, that are required of a hacker, are much lower than what is generally believed. As a minimum he feels that a hacker needs to know about networks, how communications are set-up, how to access bulletin boards and the intricacies of the *MS-DOS* and *Unix* operating systems.

*A Need to Know.*

There must be a stimulus and motivation to hack into a system and, Powell believes that, if hackers can access the computer system of a university, there is a possibility that students could find information which would help them in their examinations or they could alter data relating to their grades.

*Access to a Network*

Most students of universities and colleges have access to the Internet which links them and other universities with government research facilities, commercial institutions and laboratories.

**Computer criminals' attitudes.**

At a seminar on Initiative Against Fraud in 1991, the, then, Director of the *Cash Transactions Reports Agency* (CTRA) said "For Australia to deal with white collar crime and corporate fraud, it is unsatisfactory for those in business, who deplore the existence of such activity, to merely cheer from the sidelines". He added further that "... We need a whistleblower", Stephens (1991).

For computer crime and hacking to be confronted and challenged, there needs to be a positive attitude amongst victims, potential offenders and possible investigators. If the current *status quo* is maintained with non-reporting and the casual approach maintained to deterring and investigating offenders, we seem to be merely encouraging future offenders and creating a monster for future generation.

**Research into Australian attitudes.**

The rapid acceleration of computing technology and the associated *information superhighway* has raised a number of questions about what is right and what is wrong with regard to computer intrusions, the availability and dissemination of data, privacy, copyright, software piracy and confidentiality to name but a few topics. It is an anomaly that professions such as law, architecture and medicine have

strict codes of conduct to which their members are obliged to adhere. If these codes of conduct are breached, their respective disciplinary boards are entitled to take action against the offending party which could ultimately lead to that person being excluded from working within that industry. There are few ethical standards set by either government or industry to police the use of computers and it is left to the discretion of individual users and managers to decide what *will* and what *will not* be done.

From my experience, most of the research to date, seems to concentrate on statistical data regarding incidents rather than ethical issues. If the standardisation of ethical codes and compulsory adherence to these codes were given higher priority, there may be less emphasis on statistical surveys, criminal profiles and the like.

ACARB is the most reliable source of statistical information regarding the type of offender, the cost of these types of crime to the community and industry, computer security and employee risks (see table 2). Benbow et al (1986) has researched the attitudes of large public and private organisations regarding data security among other things.

Table 2. ACARB's Perpetrator classifications.

Job Position	Total	Known value	\$ value of loss	% of value	Average loss \$
Programmer	34	19	989,154	7.28	52,061
Customer	16	11	855,496	6.30	77,772
Operator	15	9	13,700	0.10	1,522
Input Clerk	14	7	802,507	5.91	114,651
User Staff	6	1	600	0.00	600
Manager	7	6	4,690,500	34.54	781,750
Consultant	2	1	994,000	7.32	994,000
Student	16	4	1,600	0.01	400
Thief	11	9	34,700	0.26	3,856
Hacker	24	3	26,525	0.20	8,842
Other Unident.	111	61	5,171,027	38.08	84,771
<b>TOTAL</b>	<b>256</b>	<b>131</b>	<b>13,579,859</b>	<b>100</b>	<b>103,663</b>

See Kamay (1992)

While most research has concentrated on other aspects of computer related crime such as better computer security, very little research has explored people's attitudes towards various computer related crimes. Coldwell (1990a), however, has focused on the attitudes of various high-risk groups such as, students of various disciplines, such as schoolteachers, going one logical step further from the fundamental findings of ACARB. Kamay's (1992) findings suggest that the high-risk groups are internal, from employees such as management, programmers and consultants with lesser external threats from students and other unknown persons. It must be stressed that this data is derived from reported cases only.

To be in a managerial position of authority, or to be able to be employed on a consultancy basis, or to have programming skills draws a fair assumption that people in these groups could have tertiary qualifications and some of these are likely to be a product of our higher education system. Coldwell (1990a) found that first year undergraduates in the *physical sciences* were more likely to think that hacking into other people's computer systems is acceptable than those in even the *life sciences*. The former group included people in the computer sciences. In conclusion, he suggested that undergraduates, who he called *machine people*, fell at the opposite end of a continuum to those of others who he called *people people* regarding their responses. Later, Coldwell (1993a) reported another study

which indicated that the responses of *schoolteachers* in these fields confirmed the pattern in his original results. He had approached schoolteachers because of their significant role in influencing the ethical orientation of the children pre-university, who he had originally surveyed in the first year at university.

Therefore, an assessment of both the students and the educators within the education system would be useful to supplement the overall credibility of research into computer related crime. It would also give some insight into some possible deficiencies concerning ethical standards regarding the use of computers. To ensure that the entire scenario was researched, the attitudes of the investigators of these offences - in this case the New South Wales Police - were also tested to examine the training and education given to both new recruits and experienced detectives. The attitudes of this group are significant in the chain of events due to the fact that if the upholders of society's laws do not place a great deal of significance on computer related crime, the investigation, arrest and punishment of offenders will be given low priority.

The hypotheses which are to be tested and the findings which arise from these tests should provide an insight into ethical training which can be given at institutions of higher education whether they are police or university institutes.

**Hypotheses to be tested.**

1. University respondents and police academy respondents judge computer fraud similarly as insignificant compared with other crimes.
2. University respondents and police academy respondents judge credit card fraud similarly as insignificant compared with other crimes.
3. University respondents and police academy respondents judge hacking similarly as insignificant compared with other crimes.
4. Female and male university respondents judge hacking similarly as insignificant compared with other crimes.
5. Male students and male university staff judge hacking similarly as insignificant compared to other crimes.
6. Female students and female university staff judge hacking similarly as insignificant compared to other crimes.
7. Female and male academic staff are in general agreement about the acceptability of copying software.
8. Female and male students are in general agreement about the acceptability of copying software.
9. Student computer users are more likely to find copying software acceptable than are student computer non-users.
10. University staff computer users are more likely to find copying software acceptable than are university staff computer non-users.

## 2.0 METHODOLOGY

Background.

The population.

Objectives.

Limitations.

Sample size.

The hypotheses being tested.

Contingency tables.

Chi-squared tests.

The questionnaire.

## Background

This study compares the responses from two distinct but inter-related groups of people, police officers currently studying at the New South Wales Police Academy, at Goulburn in New South Wales and students from the faculty of Business at Victoria University of Technology at Footscray in Victoria.

These two groups were selected for testing on the basis that university students have attracted attention in the popular media to be the most likely group from which competent computer criminals emerge. They were also selected to assess whether or not students develop attitudes whilst at university in response to the attitudes of university staff. Police, on the other hand, have the obvious task of investigating computer related crime. It is important to test the attitudes of this group on the basis of the perceived importance and seriousness of these offences and therefore the quality of their subsequent investigations. The responses, conclusions and subsequent attitudes from these two groups could lay a foundation for the development of ethical standards for different disciplines in their use of computer technology. To be able to test a large a sample as possible as well obtaining accurate and confidential responses it was decided to examine these groups' attitudes by way of a self completing questionnaire.

**The Population.**

These two groups are further subdivided accordingly:

*University*

- a. Undergraduates from the Faculty of Business.
- b. Academic staff from the Faculty of Business.

The total sample size being one-hundred-and-eighty-nine (189) respondents.

*Police Academy*

- a. Student police officers.
- b. Detectives.

The total sample size being five-hundred-and-ten (510) respondents.

The selection of *university academic staff* and *detectives* was done on the basis that these sub-groups are seen to be more institutionalised than *university students* and *student police officers*. They have been employed and operational within their respective careers long enough to have definite attitudes and professional beliefs.

University students and student police officers have just commenced their respective careers and they are yet to be totally influenced by their institutional ideologies. Student Police officers are recruited from a broad cross section of society, trades people and university graduates and, therefore, their responses could perhaps be seen to be representative of the population at large. Undergraduates are mostly recent school-leavers and, therefore, their

responses and attitudes will reflect those of our secondary education systems too.

### **Objectives.**

The main objectives of this research are to:

- \* Statistically compare the responses of university students and lecturing staff, and, student police officers and detectives to aspects of computer related crime, namely computer fraud, credit card fraud, hacking and software piracy, when these offences are compared and included with a number of other crimes.
  
- \* To question whether or not the attitudes of undergraduate students and student police officers are formulated before entering institutions of higher education.
  
- \* To assess the need and development of ethical standards for the different disciplines.
  
- \* To examine the educational practices of different disciplines, through responses to a self-completed questionnaire.

### **Limitations.**

Part of this study was undertaken at the New South Wales Police Academy from recently recruited student police officers and experienced detectives. This institution has

its own distinct culture which should have permeated through to the detectives and may have done so with the student police officers. This culture may have influenced the responses from the student police officers in particular, who's academic achievement and behaviour has an effect upon their graduation.

### **Sample Size.**

The sample sizes are:

a.	Student police officers	482
b.	Detectives	28
	TOTAL	510
a.	University students	155
b.	University staff	34
	TOTAL	189

The writer expresses a concern regarding the small sample with both detectives and academic staff. Greater confidence could be placed in the findings and conclusions with a larger sample. However, the maximum number of detectives in training at the New South Wales Police Academy is a matter of departmental policy and therefore, beyond the control of the researcher. Academic staff numbers within the Faculty of Business at Victoria University of Technology is also a situation beyond the control of the researcher. With this in mind, the eventual conclusions should be viewed as the starting point of a more rigorous and detailed study

following the completion of this study.

**The hypotheses being tested.**

The foundation and the theory that is being tested overall is not only the attitudes of the respondents to various types of computer related crime, but indirectly the attitudes of our education system gained through responses from academic staff and students. Is the idea of a strict code of ethics to be taught to students of institutions of higher education a case of too little, too late? Should we be pursuing this education or indoctrination at a much earlier stage? I believe that history has shown society that young children are the target and logical starting point of any form of indoctrination such as communism, nazism or simply teaching the evils of drug abuse or the benefits of stranger danger.

This belief can be seen in the indoctrination of children in nazi Germany within the Hitler Youth. Adults, on the other hand, appear to be more *set in their ways* and this gives rise to the possibility that the university respondents and the Police respondents could follow a particular course of action or career path based on the attitudes which have been in place since early childhood. The hypotheses being tested may shed some light on the strength of these attitudes.

### **Contingency Tables.**

Contingency tables are used to compare the relationship between pairs of variables. They summarise data in such a way that they can be tested for the statistical significance of sets of responses (see the methodological recommendations regarding this in Moser and Kalton, 1989). The relationship between the data in the contingency tables is used, firstly, to compare the general responses of university respondents and New South Wales Police Academy respondents. Having established certain differences in responses between these two groups, those of the university respondents were probed further - using the variables nominated by Coldwell (1990b) - to assess the nature of the attitudes of the primary population, the staff and students of the Faculty of Business (see guidance given by Madge, 1981).

### **Chi-squared.**

Chi-squared tests are used, in response to the data in the contingency tables, to assess whether differences between sets of data were statistically significant (see Daniel 1986). A statement occurs at the bottom of each contingency table whether a *null hypothesis* was accepted or not. A null hypothesis is a provisional statement that, say, the opinions of university staff and university students would not differ significantly regarding a particular variable. A null hypothesis would be accepted, if there was no

difference, and rejected, if there was a difference (see contingency tables given as appendices for examples in this process). In some cases, the level of acceptable was taken to an extreme to indicate the high level at which the test was applied. In these cases - significant ones from the point of view of this thesis - the findings of this thesis is founded on these relationships.

### **The Questionnaire. (See Appendix 1 and 2)**

One of the objectives of this research is to compare the responses of undergraduates, academic staff, detectives and student police officers to the acceptability of different computer related crimes. The method by which these responses are obtained is by way of a self-completion questionnaire. The format for this questionnaire was designed with the hypotheses which were being tested in mind. The question of rank was introduced only to distinguish between experienced police and recent recruits.

The questions of sex, age and marital status were introduced to see if there is any difference in responses between the various people within those categories in accordance with the hypotheses. The question of the educational standard reached was introduced to compare the responses of police respondents with those obtained from the university respondents to highlight any differences. To enable a comparison of Coldwell's (1992) findings, the university

student's qualifications were requested to establish if there was any nexus between various academic persuasions and the acceptance of computer crime. Coldwell's findings showed that persons within various faculties had quite different attitudes towards computer crime. The question of prior occupation was directed more at the police to see if there was any common ground arising from various occupations.

The salient features of the questionnaire are question 13. and question 14 respectively. The former asks the respondent to prioritise 15 offences. The most serious offence was to be given the score of "1" with the least serious offence being given the score of "15". Most of the offences are of a similar nature apart from the crimes of murder, domestic violence and rape. These three serious crimes are violent and emotional when compared with the remaining crimes. It is a clear indication of a respondent's attitude and attention to detail within this questionnaire and these questions when the scores for these three serious offences are analysed. They would be given very low scores if the respondents viewed the offences objectively and not hastily. Question 14 confronts the respondent with a direct challenge of their personal views - specifically - about the rights and wrongs of *hacking* into computer systems. All of the responses to this questionnaire (see appendix 1) were statistically analysed according to age, sex, academic status and Police rank and then placed into contingency tables for further analyses

using a Chi-squared test.

### 3.0 RESULTS

Respondents' ranking of computer fraud against other offences.

Respondents' ranking of credit card fraud against other offences.

Respondents' assessment of hacking.

University respondents' ranking of hacking as a crime according to sex.

Male university respondents' ranking of hacking as a crime according to academic status.

Female university respondents' ranking of hacking as a crime according to academic status.

University staff's responses to copying software as a crime according to sex.

University students' responses to copying software as a crime according to sex.

University students' responses to copying software as a crime according to user status.

University staffs' responses to copying software as a crime according to user status.

Overview.

**Respondent's ranking of computer fraud against other offences.**

The responses from both university and New South Wales Police respondents are depicted in Table 3. Both university respondents and police academy respondents judge computer fraud similarly as insignificant compared with the other fourteen crimes which are highlighted in appendix 1. The majority of the responses from both groups of people fall within the ranking of greater than ten. Considering that the most serious offence is given the score of one and the least serious offence given the ranking of fifteen, it is significant that 66.57% of responses from university people and 60.59% of police indicated that computer fraud deserves a ranking greater than ten. *The null hypothesis that university respondents and Police academy respondents judge computer fraud similarly as insignificant compared with other crime was accepted.*

**Respondent's ranking of credit card fraud against other offences.**

The responses from the same groups of university and police respondents, are highlighted in Table 4. In this case, they are asked to rank the crime of credit card fraud against the same fourteen offences. University respondents and Police Academy respondents judge credit card fraud differently but agree that it is insignificant compared with other offences.

*The null hypothesis that university respondents and police academy respondents judge credit card fraud similarly as insignificant compared with other crimes was, however, rejected.*

#### **Respondent's assessment of hacking.**

Table 5 lists the responses from all university and police respondents when confronted with the acceptability or otherwise of hacking. From this table it can be seen that university respondents believe that hacking is acceptable in contrast with the beliefs of the New South Wales Police Academy respondents. A high level of 64% of university respondents believe that hacking into other people's computer systems is acceptable compared with only 4.31% of the police. Only 6.86% of university respondents believe that hacking is unacceptable compared with an extremely high level of 82.94% of the police. A further 29.14% of university respondents are unsure whether hacking is acceptable or not compared with only 12.75% of the police.

*The null hypothesis that university respondents and Police Academy respondents believe that hacking is acceptable is rejected at an extremely high level of 0.5%.*

**University respondents' ranking of hacking as a crime according to sex.**

Table 6 highlights responses which have been broken down according to sex, amongst only university respondents. The results indicate that female and male university respondents generally disagree about the insignificance of hacking. However, the statistical test does not support a strong disagreement. Male respondents appear to believe that hacking is a serious offence but less so than the female respondents. *The null hypothesis that female and male university respondents are in general agreement about the insignificance of hacking is, however, rejected.*

**Male University respondents' ranking of hacking as a crime according to academic status.**

Table 7 differentiates between the responses on the basis of academic status - namely student or staff member - to examine any difference in attitude and response when the offence of hacking is compared with fourteen other offences. Male students and male university staff are in general agreement about the insignificance of hacking as a crime. There does not appear to be any significant difference between the two groups. *The null hypothesis being tested, that male students and male academic staff are in general agreement about the insignificance of hacking is accepted.*

**Female university respondents' ranking of hacking as a crime according to academic status.**

Table 8 tests the hypothesis that female students and female academic staff both believe that hacking is insignificant when compared to the base group of fourteen other offences. *The null hypothesis, that female students and female university staff are in general agreement about the insignificance of hacking, is accepted.*

**University staff's responses to copying software as a crime according to sex.**

Table 9 gives the responses to the question of the acceptability of copying software. The hypothesis to be tested is that both female and male university staff are in general agreement about the acceptability of copying software. The result from this test indicates that the respondents agree that copying software is acceptable. This hypothesis was accepted. A high proportion of respondents, 50% female and 58.82% male, found the offence acceptable with a further 16.67% and 17.65% undecided. Only 33.33% of females and 23.53% of males found the offence unacceptable. *The null hypothesis that female and male academic staff are in general agreement about the acceptability of copying software is accepted.*

**University student's responses to copying software as a crime according to sex.**

Table 10 shows the responses from male and female students with regard to the acceptability or otherwise of copying software as a crime. The hypothesis tested was that both male and female students are in general agreement about the acceptability of copying software. A study of the responses revealed that male students are far more likely to find copying software acceptable than are female students. *This null hypothesis that female and male students are in general agreement about the acceptability of copying software was rejected at an extremely high level of 0.5%.*

**University students' responses to copying software as a crime according to user status.**

The acceptability or otherwise of copying software is further subdivided according to whether or not the respondents have a computer at their disposal. Table 11 gives the responses for students with computers and those without computers. The null hypothesis to be tested is that student computer users are more likely to find copying software acceptable than are student computer non-users.

It is shown that student computer users are more likely to find copying software acceptable than are student computer non-users, therefore *the null hypothesis that student computer users are more likely to find copying software*

*acceptable than are student computer non-users is supported although, this is not statistically reinforced.*

**University staff's responses to copying software as a crime according to user status.**

Academic staff have been divided into computer users and non-computer users to highlight any differences towards the acceptability of copying software as an offence. The null hypothesis to be tested is that university staff computer users are more likely to find copying software acceptable than are university staff computer non-users. Table 12 shows that university staff computer users are more likely to find copying software acceptable than are university staff non-users. *The null hypothesis is supported by the data although it is not statistically supported. Meanwhile, the size of the sample throws some doubt on the result in this case.*

Table 3. Respondent's ranking of Computer Fraud against other offences.

Ranking	University respondents	Police Academy respondents	TOTALS
1 - 5	10 (5.71)	29 (5.69)	39 (5.69)
6 - 10	59 (33.72)	172 (33.73)	231 (33.73)
> 10	106 (66.57)	309 (60.59)	415 (60.58)
Totals	175 (100)	510 (100)	685 (100)

Table 4. Respondent's ranking of Credit Card Fraud against other offences.

Ranking	University respondents	Police Academy respondent's	TOTALS
1 - 5	13 (7.43)	10 (1.96)	23 (3.36)
6 - 10	51 (29.14)	150 (29.41)	201 (29.34)
> 10	111 (63.43)	350 (68.63)	461 (67.30)
Totals	175 (100)	510 (100)	685 (100)

Table 5. Respondent's assessment of Hacking.

Acceptance	University respondent's	Police Academy respondent's	TOTALS
Acceptable	112 (64.00)	22 (4.31)	134 (19.56)
Not Acceptable	12 (6.86)	423 (82.94)	435 (63.50)
Don't Know	51 (29.14)	65 (12.75)	116 (16.94)
Totals	175 (100)	510 (100)	685 (100)

Table 6. University respondent's ranking of Hacking as a crime according to sex.

Ranking	Female University respondents	Male University respondents	TOTALS
1 - 5	7 (7.00)	4 (5.33)	11 (6.29)
6 - 10	18 (18.00)	27 (36.00)	45 (25.71)
> 10	75 (75.00)	44 (58.67)	119 (68.00)
Totals	100 (100)	75 (100)	175 (100)

Table 7. Male university respondent's ranking of hacking as a crime according to academic status.

Ranking	Male Students	Male University Staff	TOTALS
1 - 5	3 (5.17)	1 (5.88)	4 (5.33)
6 - 10	17 (29.31)	2 (11.77)	19 (25.33)
> 10	38 (65.52)	14 (82.35)	52 (69.34)
Totals	58 (100)	17 (100)	75 (100)

Table 8. Female university respondent's ranking of hacking as a crime according to academic status.

Ranking	Female Students	Female University Staff	TOTALS
1 - 5	7 (7.95)	1 (8.33)	8 (8.00)
6 - 10	29 (32.96)	3 (25.00)	32 (32.00)
> 10	52 (59.09)	8 (66.67)	60 (60.00)
Totals	88 (100)	12 (100)	100 (100)

Table 9. University staff's responses to copying software as a crime according to sex.

Acceptance	Female University Staff	Male University Staff	TOTALS
Acceptable	6 (50.00)	10 (58.82)	16 (55.17)
Not Acceptable	4 (33.33)	4 (23.53)	8 (27.59)
Don't Know	2 (16.67)	3 (17.65)	5 (17.24)
Totals	12 (100)	17 (100)	29 (100)

Table 10. University student's responses to copying software as a crime according to sex.

Acceptance	Female Students	Male Students	TOTALS
Acceptable	41 (46.59)	45 (77.59)	86 (58.91)
Not Acceptable	20 (22.73)	6 (10.34)	26 (17.80)
Don't Know	27 (30.68)	7 (12.07)	34 (23.29)
Totals	88 (100)	58 (100)	146 (100)

Table 11. University student's responses to copying software as a crime according to user status.

Acceptance	Student computer users	Student computer non-users	TOTALS
Acceptable	72 (60.50)	11 (40.74)	83 (56.85)
Not Acceptable	23 (19.33)	8 (29.63)	31 (21.23)
Don't Know	24 (20.17)	8 (29.63)	32 (21.92)
Totals	119 (100)	27 (100)	146 (100)

Table 12. University staff's responses to copying software as a crime according to user status.

Acceptance	University staff computer users	University staff computer non-users	TOTALS
Acceptable	14 (66.67)	1 (12.50)	15 (51.72)
Not Acceptable	4 (19.05)	4 (50.00)	8 (27.59)
Don't Know	3 (14.28)	3 (37.50)	6 (20.69)
Totals	21 (100)	8 (100)	29 (100)

## Overview

Of the ten hypotheses tested five were accepted at some level and five were rejected. The results of these tests are that:

1. University and police respondents both believe that computer fraud is *insignificant* when this offence is compared with fourteen other offences.
2. University and police respondents both believe that credit card fraud is *insignificant* when compared with fourteen other offences. University respondents place less significance upon the offence however, than police.
3. University respondents believe that hacking is *acceptable* whereas, the police do not believe that it is acceptable.
4. Female university respondents have less regard for hacking as an offence than do male university respondents.
5. Both male students and male academic staff agree about the *insignificance* of hacking as an offence.
6. Both female students and female academic staff agree about the *insignificance* of hacking as an offence.
7. Both female and male academic staff agree about the *acceptability* of copying software.
8. Male students are *less* likely to find copying software *acceptable* than are female students.

9. Student computer users are *more likely* to find copying software *acceptable* than are student computer non-users.
10. University staff computer users are *more likely* to find copying software *acceptable* than are university staff computer non-users.

#### 4.00 DISCUSSION.

Findings and discussion of hypothesis one and hypothesis two.

Findings and discussion of hypothesis three.

Findings and discussion of hypothesis four.

Findings and discussion of hypothesis five and hypothesis six.

Findings and discussion of hypothesis seven and hypothesis eight.

Findings and discussion of hypothesis nine and hypothesis ten.

Reporting of offences to Police.

**Findings and discussion of hypothesis one and hypothesis two.**

The results from the first and second hypotheses showed an acceptance of the belief that both university respondents and Police Academy respondents judge computer fraud and credit card fraud similarly as *insignificant* when compared with fourteen other offences. Indeed, if this response was accepted universally its ramifications would be significant indeed. If this sample of our society is typical, our educators - future decision makers and the upholders of our laws - believe that computer fraud and credit card fraud are insignificant crimes.

An obvious aside to these negative attitudes towards these aspects of computer related crime could be education in the area of ethics which could be introduced at various educational institutions. This education programme could be directed at potential computer users, abusers and accusers regarding the effects upon the community of various aspects of fraud and, more particularly, computer related crime. Hopefully, this will raise the status of computer related crime to the serious level it warrants.

In talking to both experienced and relatively inexperienced police about computer crime and fraud in general, they perceive computer related crime as an area which does not warrant serious investigation. The attitudes of many police

officers seems to be exuberance and ambition when it comes to aspiring to join the ranks of specialist homicide and armed robbery investigators and sections. The contrary is believed with regard to the investigation of fraud. It seems to be perceived as either a punishment or a misdirected career move to follow fraud investigation as one's chosen career path.

Chappell (1992) refers to the financial cost of fraud to the Australian community and he believes that cost to be much greater than all other forms of crime combined. This combines with the fact that offenders are at less risk of apprehension, they are at less risk of being convicted than other traditional types of offenders and, if they are convicted, he states that they are likely to incur a lesser penalty. Chappell compares the Victoria Police investigations of fraud in 1989 which totalled three-hundred-thirty-five million dollars as opposed to less than three million dollars for armed robbery for example.

Walker (1992) talks of the cost of various types of crime to the community and how these costs are shared between the different types of crime: violent crime, property crime and drugs. He also refers to the financial cost of preventing and prosecuting crime and how equitable the resource allocation is shared between the offences on the basis of seriousness.

He estimates the total cost of all types of fraud as being in the vicinity of one-billion-seven-hundred million dollars with computer related crime involving between three-hundred-million and seven-hundred-million dollars. He highlights the breakdown of the cost to the community (see table 13) and it can be clearly seen that fraud costs the community up to in excess of fifty per cent of the total cost of crime. With those figures and the obvious attitude of police officers to computer fraud and credit card fraud I believe there is more than sufficient information to warrant a review of how the police are educated regarding the seriousness of this type of crime.

Coldwell believes that it is accepted by educators that, in early life, there are three major influences on one's personal development. These are thought to be one's parents, one's teachers and one's peers (Coldwell, 1993b). If that tenet is to be believed, coupled with the results of testing the first two hypotheses, an obvious question arises. Are we as a society developing generations of potential offenders through the actions of our educational institutions? This is, perhaps the case. In 1985, the *Australian Computer Society* developed a Code of Practice by upgrading an earlier preliminary statement (ACS, 1985).

As Coldwell suggests, the *Australian Computer Society* was becoming sensitive to criticism from its public about the increasing incidence of computer crime (Coldwell, 1990a).

Even though few academic computer scientists belong to the developed educational modules on Australian Computer Society, some tertiary institutes have professional ethics. According to Coldwell (1987), a computing course at Royal Melbourne Institute of Technology (RMIT) as early as 1986 involved subjects such as social responsibility. But, are these examples the exception or the rule? Further research within this field may answer that question.

Table 13. Estimates of Cost of Crime and Justice.

Major Category	Cost Estimate in Millions of dollars.	% of Grand Total
Homicide	275 max'm	1.0 - 1.6
Assaults inc sex	331 min'm	1.2 - 2.0
Robbery & Extort.	93	0.3 - 0.6
Break & Enter	893	3.3 - 5.3
Fraud/forgery	6710-13770	39.9 - 51.1
Theft/steal m/veh	667	2.5 - 4.0
Shoplifting	20-1500	0.1 - 5.6
Other theft	545	2.0 - 3.2
Property dam.	525-1645	3.1 - 6.1
Drug offences	1200	4.5 - 7.1
<b>TOTAL CRIME</b>	<b>11259-20919</b>	<b>67.0 - 77.7</b>
Police & Law Enf.	2575	9.6 - 15.3
Courts	619-1030	3.7 - 3.8
Corrective Service	600	2.2 - 3.6
Other	500-550	2.0 - 3.0
<b>TOTAL CRIM JUSTICE</b>	<b>4294-4755</b>	<b>17.7 - 25.6</b>
Other	1250 min'm	4.6 - 7.4
<b>GRAND TOTAL</b>	<b>16803-26924</b>	<b>100.0</b>

**Note:** Survey from Kamay and Adams (1991).

**Findings and discussion of Hypothesis three.**

The result from testing hypothesis 3 was that university respondents believe that hacking is acceptable whereas, the police do not believe that it is acceptable. The null hypothesis that both groups of respondents would generate the same response was rejected at an extremely high level. Almost eighty-three per cent of the police respondents believed that hacking was not acceptable and, while this figure is quite reassuring in light of the findings of the first two hypotheses, this figure is not representative of the whole population. This belief is based on two reasons. The findings of the first and second hypotheses reflect contrary opinions to this total acceptance of hacking as a serious crime.

Secondly, the police respondents were confronted with a direct question asking whether they thought that hacking was acceptable or otherwise. This was opposed to a more indirect system of ranking various offences on a scale of one to fifteen. (see Appendix 1). The blunt approach to questioning the acceptability or otherwise of hacking was favoured to identify the response when respondents are confronted with a direct challenge to their acceptance of things illegal. The response that was given was one which the respondents believed they had to give whereas, the ranking of a number of offences masked the respondents' beliefs, but gave them a discreet avenue to vent their true

opinions. This indicates that hacking is seen in the same light as other computer related and fraud offences.

University respondents do not seem to be as restricted by the same environmental pressure as the New South Wales Police Academy respondents. The response that they believe that hacking is acceptable coincides with the testing of the two previous hypotheses. This opinion gives the impression that universities should address the problem of their campuses being the breeding ground for potential offenders.

The response from university respondents is hardly surprising considering earlier research by Coldwell (1993d) who examined another group of people namely post-graduate teachers. He went one step further and examined the responses of this group according to sex, discipline and age (see summarised tables in Appendix 12, 13 and 14).

From Coldwell's findings it can be seen that a possible profile is drawn depicting a male, science teacher in his thirties as the educator most likely to find hacking acceptable. It would be fair to assume that students' attitudes could be firmly established before they enter institutions of higher education and a point that Coldwell makes is that this attitude may have some bearing on the course or discipline that the students follow. He continues that, with the possibility of students' attitudes being firmly established prior to entry into institutions of

higher education, the development of ethics-based socially-oriented modules at university comes, perhaps, fifteen years too late. He believes that this education should take place at the earliest possible age. Coldwell believes that some students may have a propensity towards *machine* oriented disciplines owing to the attitudes of high school educators and, therefore, the high incidence of *machine* people emerging as the high risk group at university, concerning the acceptability of hacking, is understandable.

The students' poor perception of computer related offences appears to be developed in their formative years at High School and earlier and, then, nurtured and cultivated at institutions of higher education. It would, therefore, appear that, by the time students have graduated from the university their attitudes towards computer related crime are firmly entrenched. These graduates then secure employment in many of the high risk industries, such as finance and, with that background, it is little wonder that consultants, managers and technicians are the high risk groups of offenders according to ACARB's research.

#### **Findings and discussion of hypotheses four.**

The result from testing hypothesis four was that female university respondents express less acceptance of hacking as an offence than do male university respondents which is in contrast with the hypothesis that both would generally agree

about the insignificance of the offence. However, the statistical test does not support a strong disagreement. This finding agrees with those of ACARB concerning the possible sex of high risk groups (Kamay,1992).

#### **Findings and discussion of hypotheses five and six.**

The results from testing hypothesis 5 and hypothesis 6 were both male students and male academic staff are in general agreement about the insignificance of hacking as an offence and both female students and female academic staff are in general agreement about the insignificance of hacking as an offence.

Considering the findings of the previous tests together with that of this hypothesis, both academic staff and students within the Faculty of Business place little emphasis upon the offence of hacking. Seeking further evidence that university respondents do not consider hacking as an offence, we can consider the earlier research of Coldwell (1990a) who breaks down the groups of university student respondents according to faculty (see Appendix 15).

Coldwell shows that there is a tendency for the *science* students to be less concerned about hacking than both *arts* and *social science* students. Appendix 15 shows that nearly half of the Science students considered hacking not to be a criminal activity. Less than one-third of social science-orientated and business students, agreed. Considering the

results from hypotheses three, four, five and six where there was strong support for the acceptability of hacking from within a Faculty of Business, the depth of student acceptability of hacking as an offence may be more than anticipated.

This is a situation which may require further research. The Faculty of Science is then further broken down according to science-orientation and the results of this reveals that the *physical sciences* were more receptive to hacking than the *life sciences* (see appendix 16). From that table, we can see that the physical sciences are strongly in favour of hacking not to be viewed as a criminal activity. The sample size is the only restriction to the findings of this research. Coldwell illustrates the vulnerability of technicians within the physical sciences with a quote by the Nazi Albert Speer who commented about the ethical standard of technicians that "...I exploited the phenomenon of the technician's often blind devotion to his task. Because of what appeared to be the moral neutrality of technology, these people were without scruples about their activities." It is little wonder that students, who are our future technologists and decision-makers, have little regard for various computer related offences when our educators at high school and university share do not see computer related offences as significant.

**Findings and discussion of hypotheses seven and eight.**

The results of testing hypothesis seven were that female and male academic staff both agree about the acceptability of copying software. The hypothesis being tested was that female and male academic staff are in general agreement about the acceptability of copying software, was accepted. This result was not a surprising one in that it is a situation of *the end justifying the means*.

According to a report issued by the International Trade Commission in Arlington, Virginia, USA, American hardware and software companies lost more than four billion dollars in sales in 1986, most of it due to software theft (Morrison, 1990). But stealing is always stealing regardless of the excuse. It seems that the intellectual property rights of the creator of software are *fair game* according to university respondents. The results show that there is no distinction according to either sex or academic status in the acceptability of copying software. This is again highlighted in the findings of hypothesis eight where a high proportion of female respondents reject the hypothesis and that male students are far more likely to find copying software acceptable than are female students.

**Findings and discussion of hypotheses nine and ten.**

The result of testing hypothesis nine was acceptance of the fact that student computer users are more likely to find copying software acceptable than are student computer non-users. Thus, there is some distinction within the respondents probably on the basis that the computer user group has a vested interest in acceptability of copying software no doubt for financial reasons.

Hypothesis nine tests the situation that university staff computer users are more likely to find copying software acceptable than are university staff computer non-users. This hypothesis was rejected, however, even though it was statistically supportable the size of the sample of staff throws some doubt on the result in this case. Copying software is no less an offence than any other computer related crime or car theft or drug offences for that matter. Unfortunately, for the owners and marketers of software, university respondents do not see it that way and perhaps ethical standards should be established and enforced covering entire campuses.

**Reporting of offences to Police.**

The attitudes of the university respondents may shed some light on the reasons why many of the cases of computer related crime are not reported to the police. Research by ACARB (1990) has highlighted the fact that many

organisations have experienced some form of computer related crime, however many have not reported these offences.

Working on the previous assumption that university graduates will secure high ranking positions within many high risk industries, it is possible that this attitude may have some bearing on their reluctance to report offences. Part of the reason may be that they have a belief that offences of this ilk are not serious and therefore they are not worth reporting and risking adverse publicity and, possibly, shareholder backlash and dismissal.

## 5.0 CONCLUSIONS

From the data presented in the contingency tables (see the respective appendices), it is indicated that:

1. *University respondents and New South Wales Police Academy respondents judge computer fraud similarly as insignificant compared with other crimes.*
2. *University respondents and New South Wales Police Academy respondents judge credit card fraud differently but agree that it is insignificant compared with other crimes.*
3. *University respondents believe that hacking is acceptable in contrast with the beliefs of New South Wales Police Academy respondents.*
4. *Female and male university respondents generally agree about the insignificance of hacking although the statistical difference is a minor one.*
5. *Male students and male university staff are in general agreement about the insignificance of hacking.*
6. *Female students and female university staff are in general agreement about the insignificance of hacking.*
7. *Female and male academic staff are in general agreement about the acceptability of copying software.*
8. *Male students are far more likely to find copying software acceptable than are female students.*

9. *Student computer users are more likely to find copying software acceptable than are computer student computer non-users although this is not statistically supported by the test.*
10. *University staff computer users are more likely to find copying software acceptable than are university staff computer non-users. Whereas this is statistically supported, the small sample of staff throws some doubt on the conclusion.*

In general, this thesis indicates that neither of the two groups of respondents, which were approached in this study, correctly perceive the financial significance of computer crime as it is assessed in monetary terms in the publications of the *Australian Computer Abuse Research Bureau*. Meanwhile, although some agreement is reached regarding the significance of computer fraud and credit card fraud, copying computer software and computer hacking seem to be more acceptable to the academic respondents than to the police respondents. In the case of hacking, there was a total disagreement. That these attitudes seem to be passed on from academic staff to students also seems to be evident. That the students eventually graduate and enter the workforce suggests that computer crime is entering a development phase in Australia which will be difficult to police as we enter the next century.

## 6.0 FURTHER RESEARCH

Further research should seek university respondent's rationalisations for software copying and computer hacking in particular. The assertions that "...I was copying the software to enable me to teach the students better..." and "...hackers are motivated by curiosity which is healthy amongst students..." are, I feel, in need of further investigation. The information technology industry offers site licences to universities to enable them to offer software to students at a reasonable rate on the one hand. On the other hand, gaining entry to the computer files of other people through hacking conflicts with the opinions of the *Australian Computer Society* that privacy of computer held information is sacrosanct.

A further approach to investigating computer crime would be to assess whether people from different religious backgrounds respond similarly to it. Victoria, for example, has a higher Roman Catholic population than various other states in Australia. In short, does one's religious education - as one might expect - have any impact at all on one's attitudes towards crime, generally, and computer crime in particular. Further investigations could be made into the attitudes of various Faculties and possibly various Departments within universities. Attitudes of the judiciary could also be tested together with society's perception of, and the definition of, hacking and software piracy.

## 7.0 BIBLIOGRAPHY AND REFERENCES

- ACS** (1985): *The Australian Computer Society Code of Professional Conduct*. **ACS Inc, Sydney**.
- ANDERSON, M.** (1991): Retrieving Information from Seized Computers. *The Police Chief*. April, pp 150-155.
- ANON**, (1988): Basic Considerations in Investigating and Proving Computer Related Federal Crime. *United States Department of Justice Journal*, Washington, USA.
- ANON**, (1992a): Corporate Crooks and Gentlemen. *The Sydney Morning Herald*. September, 9.
- ANON**, (1992b): The White Collar Crime Mystery. *The Sydney Morning Herald*. March, 3.
- ANON**, (1992c): *Specialist Investigators Course Resource Material. Level Two*. New South Wales Police.
- ANON**, (1993a): Hackers tap into the CSIRO. *The Daily Telegraph Mirror*. March, 25.
- ANON**, (1993b): Nasa alert. Hacker gets bond. *The Daily Telegraph Mirror*. October, 7.
- ANON**, (1993c): Hackers. *The Daily Telegraph Mirror*. March 19.
- ANON**, (1993d): ATM's crash. *Sydney Morning Herald*. June, 29.
- ANON**, (1994a): ASIO alert on phones. *The Daily Telegraph Mirror*. May, 28.
- ANON**, (1994b): Hacker Hits Royals. *The Daily Telegraph Mirror*. November, 26.
- ANON**, (1994c): Father of Computers. *The Daily Telegraph Mirror*. June, 25.
- ANON**, (1994d): Student tapped Uni's computer. *The Daily Telegraph Mirror*. November, 29.
- AUSTRALIAN INSTITUTE OF CRIMINOLOGY** (1992): *Complex Commercial Fraud Conference Proceedings*. Aust.Instit.of Criminology, Canberra, ACT.
- BALL, L.** (1985): Computer Crime. *Technology Review*. April, pp 12-14.
- BENBOW, G. MASTERS, J & COOPER, B.** (1986): *Computer Security in Australia*. pp 1-62 Melbourne.
- BEQUAI, A.** (1987): *Technocrimes: the Computerization of Crime and Terrorism*. Lexington, MA.

- BITA, N.** (1992): Benefit Fraud Costing Millions. *The Australian*. June 19.
- BONNEY, R.** (1992): Preventing Credit Card Fraud. *Crime and Justice Bulletin*, No 17.
- BOWLES, A.** (1992): New Organisational approaches in the Investigation of Fraud. *Criminology Australia*. January, pp16-18.
- BRAITHWAITE, J.** (1991): Corporate Crime becomes a Sick Joke for Australian Institutions. *The Sydney Morning Herald*. June 3.
- BRAITHWAITE, J.** (1991): Passing the Buck for Corporate Crime. *Australian Computer Society Journal*. April, pp 3-4.
- BROWN, R.** (1983): Crime and Computers. *Criminal Law Journal*. Volume 3 pp 63-89.
- BROWN, R.** (1984): Computers as Tools in the Commission of Crime. *Proceedings of the Institute of Criminology*. Canberra, A.C.T.
- CAELLI, W.** (1989): Maintaining Systems Integrity. *Proceedings of the Australian Computer Abuse Inaugural Conference*. Melbourne, Victoria.
- CHAPPELL, D.** (1992): Entrepreneurial Crime: Impact, Detection and Regulation. *Trends and Issues in Crime and Criminal Justice*. Volume 34 AIS, Canberra, A.C.T.
- CHESTERMAN, J & LIPMAN, A.** (1988): *Electronic Pirates*. Routledge, London.
- CHRISTY, D.** (1994): Computer Crime: Still a Growing Menace. *NSW Police News*. February pp 19-20.
- CLARKE, R.** (1992): Privacy and the Law. *The Australian Computer Society*. November pp 4-10 Volume 81.
- COCKBURN, M.** (1990): NCA Sets Sights on White Collar Criminals. *The Sydney Morning Herald*. November, 24.
- COLDWELL, R.** (1987): Non-professional Practices in Computing: Some thoughts on the next decade or so. *Australian Computer journal*. 19(4), pp. 215-8.
- COLDWELL, R.** (1990a): Social Parameters of computer Crime. *Australian Computer Journal*. 22(2). 43-6.
- COLDWELL, R.** (1990b): Computer Crime: A Social Perspective. *Essays in Computer Law*, Longmans London.

- COLDWELL, R.** (1991): Attitudes towards Computer Crime. *Proceedings of the ACARB Conference*. ACARB. RMIT, Melbourne, Victoria.
- COLDWELL, R.** (1992): Technology Students and computer crime: the case of ethics. *Proceedings of the ACEC '92 Conference*, Melbourne.
- COLDWELL, R.** (1993a): Schoolteachers won't learn their lessons about hacking. *Informatics*. March.
- COLDWELL, R.** (1993b): University Students' attitudes towards computer crime: A research note. *Computers and Society*, Vol.23, No. 1-2, July.
- COLDWELL, R. & JAMES, H** (1993c): Corporate security: an Australian Ostrich. *Information management and computer security journal* (UK). 1(4). 10-13.
- COLDWELL, R.** (1993d): Perceptions of computer crime. *Proceedings of the Australian Institute of criminology conference*, Melbourne.
- COMMITTEE ON COMPUTERISATION OF CRIMINAL DATA.** (1973): *Australian Attorney-General of Australia*.
- COMPLEX COMMERCIAL FRAUD CONFERENCE.** (1991): *Australian Institute of Criminology, Canberra ACT*.
- CORNWALL, H.** (1987): *Datatheft: Computer Fraud, Industrial Espionage and Information Crime*. London.
- COUROTURIE, L.** (1989): The Computer Criminal. An Investigative Assessment. *FBI Law Enforcement Bulletin*. September pp 18-22.
- DANIEL, W.** (1986): *Applied nonparametric statistics*. Houghton Mifflin. Boston.
- DAWSON, M.** (1994): Maintaining Data Integrity: Audit and Control Issues. *Proceedings from the IIR conference*, Canberra, A.C.T.
- DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION.** (1993): Media Release. Major Australian Technology Breakthrough protect world's computer information. *D S T O*, Adelaide, S.A.
- DICKIE, J.** (1994): Improving your organisation's attitude and commitment to security. *Proceedings from the IIR conference*, Canberra, A.C.T.
- EYSENCK, H.** (1977): *Crime and Personality*. Granada, London.
- FARMER, M.** (1992): Space Invaders. *The Sydney Morning Herald*. September, 7.

- FITZPATRICK, E.** (1992): Credit card fakers caught. *The Sydney Morning Herald*. June 23.
- FLEMING, L.** (1993): Serious Fraud. *The Australian Police Journal*. pp 217 -22.
- FLEMING, L.** (1993): Credit card fraud. *Policing Issues and Practice Journal*. pp 40 -46.
- FORD, G.** (1990): Computer Related Crime. *RMCP Gazette*. Ottawa, volume 52.
- FORD, S.** (1992): Practical software quality assurance. *Proceedings of a EDPAA Annual Seminar, Perth*.
- FORRESTER, T & MORRISON, P.** (1990): *Computer Ethics*. Blackwell, London.
- FRIEDMAN, B.** (1990): A course in Professional responsibility for Computer Scientists. *Proceedings of the conference on Computers and the quality of life*. Association of computing machinery.
- GRABOSKY, P.** (1992): Complex Commercial Fraud. *AIC Conference Proceedings, Canberra*.
- GREENLEAF, G.** (1990): Information Technology and the Law. *The Australian Law Journal*. Vol 64.
- HAGAN, F.** (1989): Espionage as Political Crime. A Typology of Spies. *Journal of Security Administration*. Pennsylvania.
- HAMILTON, T.** (1991): Developing an Automated Evidence Tracking System. *The Police Chief*, April pp 146-149.
- HARTCHER, P.** (1991): \$10 Million Fraud by Government Contractors. *The Sydney Morning Herald*. October, 15.
- HAYWARD, I.** (1994): *Hackers, AI and computer security*.
- HEWETT, T.** (1991): Fraud Wastes \$1.7 billion a year: insurer. *The Sydney Morning Herald*. August, 23.
- HOLLAND, K.** (1994): Stalking the Credit-Card Scamsters. *Business Week*. January pp 68-69.
- HOLSMAN, A.** (1989): Effective Computer Security Plan. The Strategic Issues. *The Australian Computer Abuse Inaugural Conference*. Melbourne.
- HUGHES, G.** (1989): *Essays on Computer Law*. Longmans, London.
- IIR CONFERENCE.** (1994): Ensuring Security within a PC environment. *Australian Bureau of Statistics*. Canberra, A.C.T.

- JACKSON, M.** (1989): Effect on Organisations of Computer Security Breaches. *The Australian Computer Abuse Inaugural Conference*. Melbourne, Victoria.
- JOHNSON, C.** (1991): NSW credit card gangs stripping accounts. *The Sydney Morning Herald*. March 9.
- JOHNSTON, B.W.** (1991): Computer Crime. *New South Wales Police Specialist Investigators Course*. New South Wales Police.
- KAMAY, V.** (1992): *The 1992 Profile of Computer Abuse in Australia*. ACARB-RMIT, Melbourne.
- KUSSEROW, P.** (1985): Computer Related Fraud in Government Agencies: Perpetrator Interviews. *Department of Health and Human Services USA*.
- LAGAN, B.** (1992): Government get Tough on Corporate Cops. *The Sydney Morning Herald*. October, 7.
- LANDRETH, B.** (1985): *Out of the Inner Circle. A Hacker's Guide to Computer Security*. Microsoft Press.
- LANE, B.** (1989): Criminals greater threat than hackers. *Information Technology*. June 13.
- LANGLEY, K.** (1988): Computer Theft emerges as boom crime. *The Sydney Morning Herald*. March 11.
- LANHAM, D.** (1987): *Criminal Fraud*. The Law Book Company Ltd.
- LAWRENCE, L.** (1987): Evidence from Computers. Footholds on a slippery surface. *Law Society Journal*. Vol 11.
- LeCOUTEUR, G.** (1994): The Fraud Problem - Securing databases. *Proceedings from the IIR conference*. Canberra, A.C.T.
- LUISI, C.** (1988): Executing Search Warrant in an Office Automation Environment. *The FBI Law Enforcement Bulletin*. March pp 7-11.
- MADGE, J.** (1981): *The tools of Social Science*. Longmans, London.
- MANNING, W.** (1990): Data Diddling, Salami Slicing, Trojan Horses. *The Police Chief*. April pp 46-50.
- MARRIOT, P.** (1988): The Development of Computer and other white collar crime. *Australian Crime Prevention Council Journal*. pp 29-37.
- MARTIN, D.** (1993): Fighting Computer Crime. *Law Enforcement Technology*. October pp 82-84.

- MEHNERT, G.** (1988): Computer Searches and Seizures. *Law and Order*. November pp 68-71.
- McCLYMONT, K.** (1992): Fraud Squad goes to Law Firm after Dollars Vanish. *The Sydney Morning Herald*. December, 12.
- McNURLIN, B. & SPRAGUE, R.** (1989): *Information systems management in practice*, Prentice-Hall, New York.
- MILBURN, J.** (1994): Queensland Unis Response team Poised to Pounce again as Hacker Crashes. *Campus Review*, Newcastle. Newcastle University.
- MIRANDA, C.** (1994): Spy Team to Ferret for Saboteurs. *The Daily Telegraph Mirror*. September, 21.
- MOELLER, R.** (1989): *Computer edit, control and security*. Wiley, New York.
- MOORE, M.** (1990): Blind Eye to White Collar Crime: Carr. *The Sydney Morning Herald*. October, 18.
- MORRISON, P.** (1990): Computer Crime. The Improvement of Investigative Skills. *National Police Research Unit*. Adelaide, S.A.
- MOSER, C. & KALTON, G.** (1989): *Survey methods in social investigation*. Heinemann, London.
- MUKHERJEE, S.** (1989): *Crime trends in twentieth century Australia*. Geo.Allen and Unwin, London.
- MUNRO, M.** (1994): How to Manage Security in a distributed environment. *Proceedings from the IIR conference*. Canberra, A.C.T.
- NEW SOUTH WALES POLICE.** (1991): Computer Crime. *Crime Issues*.
- NEYENHUYS, H.** (1993): For a Fraud Enforcement Agency. *Serious Fraud Task Force*. New South Wales Police.
- O'CONNOR, K.** (1989): Prevention and Cure. *The Australian Computer Abuse Inaugural Conference*. Melbourne, Victoria.
- O'CONNOR, K.** (1991): Privacy Act in Operation: Some Issues Relevant to Fraud Control. *Criminology Australia*. April pp 14-20.
- O'DONOGHUE, J.** (1987): Strategies found to be effective in the control of computer crime in the Forbes 500 corporations. *Security Audit & control Review*.
- OPPENHEIM, A.** (1979): *Questionnaire design and attitude measurement*. Heinemann, London.

- PARKER, D., SWOPE, S., BAKER, B.** (1990): *Ethical conflicts in information science, technology and business*. QED Information Science.
- PHILLIPS, B.** (1985): *Social research: strategy and tactics*. Macmillan. New York.
- PLUNKETT, S.** (1993): Sabotage on Screen. *The Business Review Weekly*. pp 34-9.
- POWELL, G.** (1992): For Hackers, Networks are wide open. *The Sydney Morning Herald*. July, 7.
- RAETHEL, S.** (1994): Computer file risks HSC study. *The Daily Telegraph Mirror*. October, 6.
- ROBOTHAM, J.** (1994): Hackers. *The Australian*. July 26.
- RODEN, A.** (1991): Computer Crime and the Law. *Criminal Law Journal*. Volume 15 pp 397-415.
- RODEN, A.** (1992): Report into Unauthorised Release of Government Information. *State Government Report Vol 1*.
- SAMUELS, A.** (1991): Admissibility of Computer Evidence. *Justice of the Peace*. October pp 60-64.
- SESSIONS, W.** (1991): Computer Crimes. An Escalating Trend. *The FBI Law Enforcement Bulletin*. February pp 12-15.
- SKULLEY, M.** (1991): Corporate criminals of genus thief. *The Australian*. July, 23.
- SMITH, G.** (1985): Computerised Crime Control. *Victoria Police Association Journal*. June pp 11-13.
- SPAFFORD, E.** (1988): The Internet Worm Program: An Analysis. *Purdue Technical Report CSD - TR 823*.
- STEPHENS, T.** (1990): One in four workers ready to diddle the boss, says legal firm. *The Sydney Morning Herald*. May, 11.
- STEWART, J.** (1989): Dedicated Computer Crime Units. *The Sydney Morning Herald*. April, 12.
- STOLL, C.** (1989): *The Cuckoo's egg*. Doubleday Dell, New York.
- STRANDBERG, K.** (1993): Closing the Door on Cellular Phone Fraud. *Law Enforcement Technology*. July pp 26-32.
- STRAUB, D & HOFFER, J.** (1988): *Computer Abuse and computer security administration: a study of contemporary information systems methods*. IR MIS Working Paper. Indiana University, Indianapolis.

- STRAUB, D & WIDOM, C.** (1984): Deviancy by bits and bytes: computer abusers and control measures, in Finch & Dougall (Eds) *Computer Security: a global challenge*. Elsevier Science, N-Holland.
- SUTHERLAND, E.** (1983): *White collar crime: the Uncut version*. Yale University Press. New Haven.
- TAPPER, C.** (1989): *Essays on computer Law*. Longmans London.
- THOMPSON, D.** (1989): Executive Brief. *National Police Research Unit*. Adelaide, S.A.
- THOMPSON, D.** (1989): Computer Crime: Detection, Investigation and Prosecution. *Victoria Police*. pp 1-11.
- TSALIKIS, J & ORTIZ-BOUNAFINA, M.** (1990): Ethical beliefs. Differences of Males and Females. *Journal of Business Ethics*.
- WALDON, R.** (1994): The Trade of illegal information in the public sector - implications for security. *Proceedings from the IIR conference*. Canberra, A.C.T.
- WALKER, J.** (1992): Estimates of the Costs of Crime in Australia. *Trends and Issues in Crime*. Australian Institute of Criminology, Canberra.
- WARD, C.** (1973): *Vandalism*. Architectural Press, London.
- WARNICK, L.** (1991): The Investigation of Fraud. *Proceedings of the Australian Institute of Criminology Conference*. Canberra, A.C.T.
- WARNOCK, S.** (1994): Fake Credit Card Racket Exposed. *The Sun Herald*. March 13.
- WASIK, M.** (1989): Computers and the Blackmail Threat, computer Crime. *The Computer Law and Security Report 6 CLSR*.
- WATSON, R. & PURNELL,** *Criminal Law in New South Wales*. Sydney.
- WHITTEN, J., BENTLEY, L & BARLOW, V.** (1989): *Systems analysis and methods*, Irwin, New York.
- ZERVOS, K.** (1991): Responding to Fraud in the 1990's. *Proceedings of the Australian Institute of Criminology conference*. Canberra, A.C.T.

Appendix 1: A questionnaire.

## CONFIDENTIAL QUESTIONNAIRE

Please would you complete the following confidential and anonymous questionnaire. The results will be analysed and published in the Australian Police Journal.

1. What rank are you?.....
2. What sex are you? Male/Female.
3. What age are you? 20-29, 30-39, 40-49, 50-65, other?
4. What is your current marital status? Married/Unmarried?
5. In which country were you born?.....
6. Did you complete your HSC? Yes / No.
7. Do you have a Degree? Yes / No.
8. If " Yes " which Degree.....
9. If so, in which specialty was your undergraduate study?.....
10. In which Section are you now employed?.....
11. How long have you been employed there?.....
12. What was your earlier occupation?.....
13. Please number from 1-15, what you consider to be the 15 most serious offences. (Give the most serious the score of "1".)
 

Arson	.....
Breaking and Entering	.....
Computer Fraud	.....
Credit Card Fraud	.....
Domestic Violence	.....
Drug Offences	.....
Drunk Driving	.....
Embezzlement	.....
Malicious Damage	.....
Murder	.....
Rape	.....
Shoplifting	.....
Stealing	.....
Traffic Offences	.....
White Collar Crime	.....
14. Do you believe that hacking into computer systems is acceptable? Yes / No / Don't Know.

Appendix 2: A questionnaire.

## CONFIDENTIAL QUESTIONNAIRE

Please would you complete the following confidential and anonymous questionnaire. (Circle answers as required).

1. Which sex are you? Female / Male
2. What age are you? Under 20, 20-29, 30-39, 40-49, over 50
3. Describe your culture at home? Australian / Other (specify).....
4. In which country were you born?.....
5. Which Dept/faculty do you teach/work in?.....
6. Which type of staff are you? TEACHING / GENERAL
7. How many years have your taught/worked at Uni level....
8. What is your highest qualification?.....
9. Please number from 1 to 10 what you consider to be the 10 most serious offences in this list. Give the most serious office the score of 1.
 

Arson	....
Breaking and Entering	....
Computer hacking	....
Credit card fraud	....
Domestic violence	....
Drug offences	....
Drunk driving	....
Embezzlement	....
Malicious damage	....
Murder	....
Rape	....
Sexual harassment	....
Shoplifting	....
Stealing	....
Traffic offences	....
Computer fraud	....
White collar crime	....
other	....
10. Is copying software for personal use acceptable?  
Yes / No / Don't know
11. Do you have access to a computer at home? Yes / No  
Specify.....
12. If you have any comments to make pertinent to the content of this questionnaire please make them in clear handwriting on the back of this sheet.

Appendix 3. Respondents' ranking of computer fraud against other offences.

Ranking	Respondent's categories	Respondent's categories	TOTALS
	University Respondents  Observed (%) Expected (Chi-Sq.)	Police Academy Respondents  Observed (%) Expected (Chi-Sq.)	
1 - 5	10 (5.71) 9.96 (0.0002)	29 (5.69) 29.04 (0.0001)	39 (5.69)
6 - 10	59 (33.72) 59.1 (0.0002)	172 (33.73) 172 (0)	231 (33.73)
> 10	106 (66.57) 106 (0)	309 (60.59) 309 (0)	415 (60.58)
Totals	175 (100)	510 (100)	685 (100)

**NOTES**

**Hypothesis:** Null hypothesis regarding the responses of university respondents and police academy respondents to the significance of computer fraud.

**Statistical Test:** Chi squared = 0.0005 for 2-degrees of freedom at 5% = 5.991: so accept Ho.

**Conclusion:** University respondents and Police Academy respondents judge computer fraud similarly as insignificant compared with other crimes.

Appendix 4. Respondents' ranking of credit card fraud against other offences.

Ranking	Respondent's categories	Respondent's categories	Totals
	University Respondents Observed (%) Expected (Chi-sq.)	Police Academy Respondents Observed (%) Expected (Chi-sq.)	
1 - 5	13 (7.43) 5.88 (8.62)	10 (1.96) 17.12 (2.96)	23 (3.36)
6 - 10	51 (29.14) 51.35 (0.0024)	150 (29.41) 149.65 (0.0008)	201 (29.34)
> 10	111 (63.43) 117.78 (0.39) (100%)	350 (68.63) 343.23 (0.13)	461 (67.30)
Totals	175 (100)	510 (100)	685 (100)

**NOTES**

**Hypothesis:** Null hypothesis regarding the responses of university respondents and police academy respondents to the significance of credit card fraud.

**Statistical Test:** Chi squared = 12.1032 for 2-degrees of freedom at 5% = 5.991; so reject Ho.

**Conclusion:** University respondents and Police Academy respondents judge credit card fraud differently but agree that it is insignificant compared with other crimes.

## Appendix 5. Respondents' assessment of hacking.

Acceptance	Respondent's categories	Respondent's categories	Totals
	University Respondents	Police Academy Respondents	
	Observed (%) Expected (Chi-sq.)	Observed (%) Expected (Chi-sq.)	
Acceptable	112 (64.00) 34.23 (176.69)	22 (4.31) 99.77 (60.62)	134 (19.56)
Not Acceptable	12 (6.86) 88.14 (65.77)	423 (82.94) 323.87 (30.34)	435 (63.50)
Don't Know	51 (29.14) 29.64 (15.39)	65 (12.75) 86.36 (5.28)	116 (16.94)
Totals	175 (100)	510 (100)	685 (100)

## NOTES

**Hypothesis:** Null hypothesis regarding the responses of University respondents and Police Academy respondents to the acceptability of hacking.

**Statistical Test:** Chi-squared = 430.32 for 2-degrees of freedom at 0.5% = 10.579; so reject Ho.

**Conclusion:** University respondents believe that hacking is acceptable in contrast with the beliefs of the Police Academy respondents. (This hypothesis is rejected at an extremely high level of 0.5%.)

Appendix 6. University Respondents' ranking of hacking as a crime according to sex.

Ranking	Respondent's categories	Respondent's categories'S	Totals
	Female University Respondents  Observed (%) Expected (Chi-sq.)	Male University Respondents  Observed (%) Expected (Chi-sq.)	
1 - 5	7 (7.00) 6.29 (0.08)	4 (5.33) 4.71 (0.107)	11 (6.29)
6 - 10	18 (18.00) 25.72 (2.317)	27 (36.00) 19.29 (3.082)	45 (25.71)
> 10	75 (75.00) 68 (0.72)	44 (58.67) 51 (0.961)	119 (68.00)
Totals	100 (100)	75 (100)	175 (100)

#### NOTES

**Hypothesis:** Null hypothesis regarding the responses of University respondents according to sex to the ranking of hacking against other crimes.

**Statistical Test:** Chi-squared = 7.267 for 2-degrees of freedom at 5% = 5.991; so reject Ho.

**Conclusion:** Female and male University respondents generally disagree about the insignificance of hacking. However, the statistical test does not support a strong disagreement.

Appendix 7. Male university respondents' ranking of hacking as a crime according to academic status.

Ranking	Respondent's categories	Respondent's categories	Totals
	Male Students	Male University Staff	
	Observed (%) Expected (Chi-sq.)	Observed (%) Expected (Chi-sq.)	
1 - 5	3 (5.17) 3.09 (0.003)	1 (5.88) 0.91 (0.009)	4 (5.33)
6 - 10	17 (29.31) 14.69 (0.363)	2 (11.77) 4.31 (1.238)	19 (25.33)
> 10	38 (65.52) 40.20 (0.12)	14 (82.35) 11.79 (0.414)	52 (69.34)
Totals	58 (100)	17 (100)	75 (100)

NOTES

**Hypothesis:** Null hypothesis regarding the responses of male University respondents according to academic status to the ranking of hacking against other crimes.

**Statistical Test:** Chi-squared = 2.147 for 2-degrees of freedom at 5% = 5.991; so accept Ho.

**Conclusion:** Male students and male University staff are in general agreement about the insignificance of hacking.

Appendix 8. Female university respondents' ranking of hacking as a crime according to academic status.

Ranking	Respondent's categories	Respondent's categories	Totals
	Female Students  Observed (%) Expected (Chi-sq.) (45.05%)	Female University Staff  Observed (%) Expected (Chi-sq.)	
1 - 5	7 (7.95) 7.04 (0.0002)	1 (8.33) 0.96 (0.0017)	8 (8.00)
6 - 10	29 (32.96) 28.16 (0.025)	3 (25.00) 3.84 (0.1838)	32 (32.00)
> 10	52 (59.09) 52.8 (0.012)	8 (66.67) 7.2 (0.09)	60 (60.00)
<b>Totals</b>	88 (100)	12 (100)	100 (100)

**NOTES**

**Hypothesis:** Null hypothesis regarding the responses of female University respondents according to academic status to the ranking of hacking against other crimes.

**Statistical Test:** Chi-squared = 0.3127 for 2-degrees of freedom at 5% = 5.991; so accept Ho.

**Conclusion:** Female students and female University staff are in general agreement about the insignificance of hacking.

Appendix 9. University staff's responses to copying software as a crime according to sex.

Acceptance	Respondent's categories	Respondent's categories	Total
	Female University Staff  Observed (%) Expected (Chi-sq.)	Male University Staff  Observed (%) Expected (Chi-sq.)	
Acceptable	6 (50.00) 6.62 (0.058)	10 (58.82) 9.38 (0.04)	16 (55.17)
Not Acceptable	4 (33.33) 3.31 (0.144)	4 (23.53) 4.69 (0.102)	8 (27.59)
Don't Know	2 (16.67) 2.07 (0.002)	3 (17.65) 2.93 (0.002)	5 (17.24)
Totals	12 (100)	17 (100)	29 (100)

**NOTES**

**Hypothesis:** Null hypothesis regarding the responses of University staff respondents according to sex to copying software.

**Statistical Test:** Chi-squared = 0.348 for 2-degrees of freedom at 5% = 5.991; so accept Ho.

**Conclusion:** Female and male academic staff are in general agreement about the acceptability of copying software.

Appendix 10. University students' responses to copying software as a crime according to sex.

Acceptance	Respondent's categories	Respondent's categories	Totals
	Female Students' responses	Male Students' responses	
	Observed (%) Expected (Chi-sq.)	Observed (%) Expected (Chi-sq.)	
Acceptable	41 (46.59) 51.84 (2.267)	45 (77.59) 34.16 (3.44)	86 (58.91)
Not Acceptable	20 (22.73) 15.67 (1.196)	6 (10.34) 10.33 (1.815)	26 (17.80)
Don't Know	27 (30.68) 20.49 (2.07)	7 (12.07) 13.51 (3.14)	34 (23.29)
Totals	88 (100)	58 (100)	146 (100)

**NOTES**

**Hypothesis:** Null hypothesis regarding the responses of University undergraduate respondents according to sex to copying software.

**Statistical Test:** Chi squared = 13.928 for 2-degrees of freedom at 5% = 10.579; so reject Ho.

**Conclusion:** Male students are far more likely to find copying software acceptable than are female students. (This hypothesis is rejected at an extremely high level of 0.5%)

Appendix 11. University students' responses to copying software as a crime according to user status.

Acceptance	Respondent's categories	Respondent's categories	Totals
	Student Computer users Responses Observed (%) Expected (Chi-sq.)	Student Computer Non-users Responses Observed (%) Expected (Chi-sq.)	
Acceptable	72 (60.50) 67.65 (0.28)	11 (40.74) 15.35 (1.233)	83 (56.85)
Not Acceptable	23 (19.33) 25.27 (0.204)	8 (29.63) 5.73 (0.9)	31 (21.23)
Don't Know	24 (20.17) 26.08 (0.166)	8 (29.63) 5.92 (0.731)	32 (21.92)
Totals	119 (100)	27 (100)	146 (100)

#### NOTES

**Hypothesis:** Null hypothesis regarding the responses of University undergraduates respondents according to user status to copying software.

**Statistical Test:** Chi-square = 3.514 for 2-degrees of freedom at 5% = 5.991; so accept  $H_0$ .

**Conclusion:** Student computer users are more likely to find copying software acceptable than are student computer non-users although this is not statistically supported.

Appendix 12. University staff's responses to copying software as a crime according to user status.

Acceptance	Respondent's categories	Respondent's categories	Total
	University staff Computer Users Responses Observed (%) Expected (Chi-sq.)	University staff Computer Non-users Responses Observed (%) Expected (Chi-sq.)	
Acceptable	14 (66.67) 10.86 (0.91)	1 (12.50) 4.14 (2.382)	15 (51.72)
Not Acceptable	4 (19.05) 5.79 (0.55)	4 (50.00) 2.21 (1.45)	8 (27.59)
Don't Know	3 (14.28) 4.34 (0.414)	3 (37.50) 1.66 (1.082)	6 (20.69)
Totals	21 (100)	8 (100)	29 (100)

NOTES

**Hypothesis:** Null hypothesis regarding the responses of University staff respondents according to user status to copying software.

**Statistical Test:** Chi-squared = 6.788 for 2-degrees of freedom at 5% = 5.991; so reject  $H_0$ .

**Conclusion:** University Staff computer users are more likely to find copying software acceptable than are University Staff computer non-users. This is statistically supportable although the size of the sample of staff throws some doubt on the result in this case.

Appendix 13. Responses of teachers to hacking according to sex.

Responses.	Female Teachers	Male Teachers	TOTALS
	No observed %	No observed %	No observed %
Unacceptable	47 (75.8)	40 (47.7)	87 (59.6)
Acceptable	15 (24.2)	44 (52.3)	59 (40.4)
TOTALS	62 (100)	84 (100)	146 (100)

Note: Summarised from Coldwell (1990)

Appendix 14. Responses of teachers to hacking according to discipline.

Responses	Teachers	Teachers	TOTALS
	Science No observed %	Others No observed %	No observed %
Unacceptable	8 (34.8)	80 (65)	88 (60.2)
Acceptable	15 (65.2)	43 (35)	58 (39.8)
TOTALS	23 (100)	123 (100)	146 (100)

Note: Summarised from Coldwell (1990).

Appendix 15. Responses of teachers to hacking according to age.

Responses	20-29 No Obser %	30-39 No Obser %	40-49 No Obser %	50+ No Obser %	Not known No Obser %	TOTALS No Obser %
Unaccept.	7 58.3	22 48.9	25 67.6	8 72.7	26 63.4	88 60.3
Acceptable	5 41.7	23 51.5	12 32.4	3 27.3	15 36.6	58 39.7
TOTALS	12 100	45 100	37 100	11 100	41 100	146 100

Note: Summarised from Coldwell (1990).

Appendix 16. Inter-faculty responses to the ethics of hacking.

Response	Arts	Social Science	Science	TOTALS
Criminal	18 (66.7%)	16 (69.6%)	9 (23.7%)	43 (48.9%)
Not Criminal	5 (18.5%)	5 (21.7%)	18 (47.4%)	28 (31.8%)
Don't Know	4 (14.8%)	2 (8.7%)	11 (28.9%)	17 (19.3%)
TOTALS	27 (100%)	23 (100%)	38 (100%)	88 (100%)

Note: Summarised from Coldwell (1990).

Appendix 17. Science students' responses to the ethics of hacking.

Response	Biology	Zoology	Physics	Computer Science	TOTALS
Criminal	5+	3 = 8 (44.4%)	0+	1 = 1 (5%)	9 (23.7%)
Not Criminal	3+	3 = 6 (13.3%)	5+	7 = 12 (60%)	18 (47.4%)
Don't Know	2+	2 = 4 (22.2%)	3+	4 = 7 (35%)	11 (28.9%)
TOTALS	10+	8 = 18 (100%)	8+	12 = 20 (100%)	38 (100%)

**Note:** Summarised from Coldwell (1990).



