Legal aspects of computer crime is the law inadequate?

*** J.R. SULAN**
Commissioner for Corporate Affairs
South Australia

I would like to begin my paper by reading to you a quotation from August Bequai's book "White Collar Crime – A 20th Century Crisis".

"While the average bank robber realises only about $15,000 the average computer theft netts about $400,000. Experts estimate that the likelihood of such crime being discovered by the authorities is 1 out of 100. One recent study places the annual loss at over $100,000,000 and this estimate does not include the cost of investigating and prosecuting these crimes. The problem is serious and ever increasing."

The increasing use of computers in the developed world, both in commerce and government, and the coming of ELECTRONIC FUNDS TRANSFER SYSTEMS (or EFTS), the cash less society where funds will become a series of electronic impulses transmitted over telephone lines from the place where a purchase is made to the purchasers bank and thence to the vendors bank, or indeed from one financial institution to another, involving anything from a few dollars to hundreds of thousands or even millions, has created a never before seen opportunity for the criminal, where the rewards are great and the risk small.

Almost all, indeed if not all, of the experience of computer crime comes from overseas – the U.S.A. and Europe. However that should not be a reason for any of us to suppose that frauds, or related crimes involving computers have not already, or will not in the future occur in this country. Our trends in computerization mirror those of overseas, and it follows that we will inherit the same problems.

The operation of a computer system can be divided into 5 main components. The first stage is the **INPUT.** Here data is translated into a language the computer understands. A number of devises can be used to effect the translation, such as opticals scanners and card readers. At this stage of the operation false or misleading information can be introduced into the computer. In this way payment for non-existent services may be made. Unintentional errors can also occur which can result in erroneous payments.

The second stage is the **PROGRAMME.** At this point the computer is given the instructions which will tell the computer the manner in which it is to operate, that is, process the data given to it. A programme may be altered, manipulated or falsified and therefore the instructions given to the computer will be erroneous. The more complex the programme the greater the scope and ease for manipulation and the more difficult the detection of the interference. Programmes can be very valuable in terms of what they cost to prepare (or duplicate), and the disruption to a firm's operation if they are destroyed or stolen. For these reasons programmes are threatened by theft. They can be sold to a firm's competitors or a foreign government or even held to ransom as has happened in the United States and Europe.

The third stage is the **CENTRAL PROCESSING UNIT** or CPU. The CPU contains the control units of the system. It guides the system, retrieves the necessary data and directs the computer to perform. The CPU also contains the memory devices of the system. It is a vital part of the entire system and its destruction would be a likely target for the saboteur.

**Mr. J.R. Sulan, LLB (Adelaide) was formerly Senior Assistant Crown Prosecutor in South Australia and is now Commissioner, Corporate Affairs Commission in that State. The following paper was presented by Mr. Sulan at the most recent ANZAAS Conference, Adelaide, 14 May, 1980 and is now republished by kind authority of Mr. Sulan.*

The fourth stage is the **OUTPUT.** Here data is received from the CPU and translated into intelligible language. Output can of course be stolen or sold. For example the computerised mailing list of a large publishing house would be very valuable to a competitor. This has already happened in the United States.

The fifth stage is the **COMMUNICATION PROCESS.** This is the transmission of data back and forth from a computer to another computer or to a terminal. It is at this stage the interception of data can occur.

At all stages of its operation a computer system is open to human interference. It is after all operated by humans and supposedly for humans. Experience has shown that the interference may come from someone working within the computer facility as well as from an outsider. The interference may be direct and human, such as the alteration or theft of a programme, or by means of electronic penetration such as tapping the telephone line being used by a computer in order to intercept and record messages. The point is that the means of interference are many and varied and may come into play at any of the different points along the compyter operation.

August Benquai has classified five categories of computer crime:

1. Sabotage of the system as a whole or any stage of the process. For example, the destruction of the entire system or of a programme or of the theft of a programme.
2. The theft of services. This involves the use of the firms computer at someone elses expense, for example, employees using the company's computer for their own benefit but at the company's expense.
3. Property crimes usually involving the theft of goods or other property through the use of a computer, for example using the computer to order cheque payments for non-existent services.
4. Data crimes involving the theft of information which may be valuable and confidential and therefore of great value, for example to a business competitor or a foreign government.
5. Financial crimes. These usually involve large sums of money. The Equity Funding case in the United States which involved over 2 billion dollars is the most notable example. The computer is used by the criminal to engineer complex and sophisticated swindles.

Some examples of the categories of computer crime referred to are as follows:—

Italian terrorist groups have carried out bombing attacks on at least ten computer centres in that country and the average costs of each attack has been assessed at approximately one million dollars. The computers were singled out because they were instruments of the capitalistic system. The attackers were armed and used fire bombs, explosives, petrol and firearms to damage and destroy the computer facilities. In each case the attacks were carried out very quickly, caused extensive losses and it appeared that the terrorists knew precisely what they were doing. This type of crime presents no unique difficulty in the area of law enforcement, however it represents an enormous cost to the community when a system is destroyed. Sabotage has not been confined to political extremists. Individuals have been responsible for such acts, often motivated by a resentment to the impersonal and inhuman aspect of computers. The lack of security surrounding computers has made it relatively easy for saboteurs to carry out their destruction.

Examples of the theft of services are numerous and I will only give two cases. In the first, employees of a computer service developed a programme for writing orchestral arrangements. They set up an arranging service and used the firm's computer to prepare the arrangements. In another case a political candidate used a city's computer to prepare and post mail in connection with his election campaign.

Jerry Schneider was the president of his own electronics firm on the West Coast of the United States and he had some understanding of the workings of computers. At that time the Pacific Telephone and Telegraph Company depended on a computerised ordering system. Schneider obtained information about their internal system and the codes required to access their computer so as to order materials and equipment. Using a touchphone he was able to access the company's computer and order large quantities of equipment which were put out onto loading bays. He had keys and documents issued by the computer and all he had to do was go along and collect the material, which he did early in the mornings to avoid the usual checks which would have been made had the company's staff been there. He used a truck to resemble P.T.T.'s vehicles when he collected the materials. In this way Schneider obtained an enormous quantity of equipment from the company. He was caught.

He was sentenced to imprisonment which was suspended and he served only 40 days in actual detention. He is now a consultant on computer security.

An example of data theft is the case in California where a computer service company wanted to bid for the contract of a jet engine manufacturer. An employee of the company obtained the codes giving him access to the computer of a rival firm. Using his terminal he dialed the rivals computer and obtained a copy of the programme used by that company to prepare jet engine designs. In this way the company was able to bid against the rival for providing services to the jet engine manufacturer. The employee was caught and prosecuted and a fine imposed. His employer was not prosecuted.

Six men were able to syphon a million dollars in winnings from a dog track. Three of the men worked for the track and three for the firm that supplied the computers which were used to compute the bets. They used a computer to take part of the winnings from the trifecta pool. In the trifecta, punters had to predict first and second in three specified races. All the money waged on the trifecta was pooled and the State and the track each took a share, with the remainder being divided with the winners. Two computers were used to maintain and produce the lists of all winners including the trifecta pool. The conspirators would shut one computer and they would enter and issue additional winning tickets as part of the trifecta pool. These tickets would then be presented and in this way they obtained a part of the pool. It appears that they had been working this system for about five years. They were caught when one day a real winner collected $156,000 with several tickets. That was an unusually high payoff and the auditor for the State Gambling Commission investigated the computation of the payoff. In this way he discovered that all winning tickets had been printed on one machine and the winning tickets sold from that machine exceeded the value of all trifecta bets placed by the machine. In the ensuing investigation one of the conspirators turned Crown evidence and in exchange for immunity agreed to testify against the other members involved. If it had not been for the fortuitous circumstances they may never have been caught. Fortuitous discovery, or an informant giving the game away is the means by which the crime is discovered in a majority of cases prosecuted. In many instances the victim is unaware that anything is amiss.

This case demonstrates one of the devices often used by law enforcement agencies in the United States when investigating serious crimes. That of immunity. Federal and State Statutes confer upon witnesses immunity from prosecution in exchange for testimony, both voluntary and compelled. Immunity can therefore be used as an inducement to obtain testimony, typically of a witness of a multi-party crime and where that witnesses testimony is necessary if charges are to be laid at all or where it is believed necessary for the successful prosecution

of his fellow wrong doers. Immunity mav also be used to compel testimony, where there is power to do so, e.g. witnesses before a grand jury. The immunity conferred may be use or derivativeuse immunity, where no testimony or other information compelled upon any order (or any information directly or indirectly derived from such testimony or other information) may be used against the witness in any criminal case (e.g. the Federal Criminal Code 18USC6001-6002). However, the witness may still be prosecuted on the basis of completely independent evidence. The immunity may also be transactional, that is complete immunity from prosecution for offences to which testimony relate. The immunity may also be informal, that is in the form of an undertaking by the prosecutor not to bring any criminal charges.

The grant of immunity from prosecution has proved to be a powerful weapon in the hands of the authorities. With it, many cases have successfully prosecuted where otherwise they would not have been. There is legislation in Australia protecting a person from being compelled to incriminate himself. A system, such as in the United States where a witness can be granted immunity in exchange for his testimony or in order that he may be compelled to answer questions has certain merits, particularly in the difficult area of corporate and computer Crime and in my view should be looked at to see whether or not it can be adopted in this country as part of the law enforcement process.

The proposed Companies Bill and the Commonwealth Securities Industry Act, 1980 goes some way in providing that a person in certain circumstances can be compelled to answer questions and his answers may not be used against him in criminal proceedings if he is compelled to answer above an objection. However, in my opinion the Companies Bill and Securities Industry Act does not go far enough because if the investigation is unrelated to the affairs of the company or dealing in securities, the provisions have no application.

On a more light hearted note, I came across the case of a man in the United States who went to his bank and obtained a loan. He was given a booklet of numbered vouchers with which to make his repayments. The vouchers were magnetically incoded so that they could be read by the computers. When the time came to make his first payment, he forwarded the payment with the last voucher given to him. He subsequently received a letter from the Bank thanking him for his prompt repayment of the loan. He was never prosecuted. I am assured by bank officers that this could never occur in Australia.

Computers, for the first time, pose unique problems for us. A large corporation purchasing a computer may do so because it may improve its efficiency, reduce costs or simply for the prestige of computerization. A substantial part of that company's affairs is then entrusted to the computer, and of course, to those individuals who run the computer. Unlike the paper system which the computer replaces, the new system is not one which is properly understood by management. The computer removes management from the day to day supervision of the company's affairs. It does not understand the process whereby the computer maintains the company's books and affairs not does it understand the potential threat which the computer brings. The normal controls and auditing procedures which were adequate for the previous system are no longer possible with computerisation. Either through lack of understanding, or deterred by cost, or fear in the loss in the efficiency in the computer system, inadequate security measures are taken by management to protect the integrity of the system or to detect any interference or manipulation of it. The first step towards prevention of computer crime is to make the system less vulnerable to interference, either from outside, or by the company's own employees. This involves a number of security measures such as adequatelv housing the computer and limiting access to it to prevent or deter sabotage to the computer itself. A proper screening of employees who will work within the computer facility may help to identify persons who should not be placed in such sensitive positions. Another area to consider is the implementing of working systems designed to minimize the opportunity given to an individual to manipulate the system to his own benefit. Access to the computer facility should be restricted to only those persons working within the facility. A daily log should be kept of all those individuals who have had access, with their time of entry and departure being recorded. The duties of personnel operating the facility should be fragmented and segregated as much as possible to ensure that only a small number of people have access to all operations of the system. In addition, personnel should be rotated. This means additional cost, but in the final analysis if one is to reduce this type of crime it comes back to people. Just as if one is to prosecute persons who commit this type of crime, then there must be others who are observant and prepared to speak up when they see and hear something suspicious. Management must be made aware of the potential threats posed by computers to their company's operations and should be prepared to assume responsibility for safeguarding the company's interests.

The second step towards prevention is to make detection of any interference certain and swift. At present the computer criminal can carry on his work for a long period of time, taking large sums of money or goods without anyone suspecting or being aware of what he is doing. Proper auditing and routine checks can be of great benefit in detecting computerized theft or fraud. The mere continued presence of an outside observer must have some deterrent effect upon potential wrongdoers. It is human nature that if one makes something easy then the temptation may prove to be too strong.

Computer crime has presented the law enforcement agencies with a problem they are inadequately trained to handle. Experience elsewhere has shown that even where it is known that one has been using the computer to steal from a company, it is not always easy to piece together how the crime was committed and to find sufficient evidence to ensure a conviction. From its very nature the crime is both complex and sophisticated, and committed by an expert in the field who will undoubtedly endeavour to cover his tracks. It is not unreasonable to expect then, that it will require an expert to unravel how the crime was committed and by whom. The law enforcement agencies must have personnel trained and competent to investigae computer crime. In addition the legal profession and the judiciary have little knowledge or understanding of anything connected with computers. The lawyers who prosecute and defend and the judiciary who preside over the trials of computer criminals, and sentence them for their crimes, need to be educated.

The law, at present does not specifically provide for computer related crimes and therefore if we are to prosecute the criminal we must catagorize his misbehaviour into the existing framework of the criminal law. This task, in some instances, will be difficult, if not impossible. We can, I think, distinguish between conventional crimes committed with the aid of a computer and for which the criminal law already provides sanctions, and those forms of misbehaviour which do not, or may not, constitute offences but which warrant the sactions of the law. If we are to prosecute computer crime we must categorize the crime into one of the following:—

1. Theft;
2. Embesslement;
3. Obtaining Property by False Pretences;
4. Wilful and Malicious Damage to Property;
5. The Falsification or Alteration or Destruction of Records or Documents.

Theft, or larcency as it is more properly called, is the taking or carrying away of property belonging to another (including a company) with the intention of permanently depriving the owner of it. In the computer crime situation if the theft involves the stealing of goods, such as in the Jerry Schnieder case, then the law makes it an offence. It is a conventional crime effected through the use of a computer, but no different really to stealing of any other sort. What of the criminal who steals tapes containing the programme? The tapes may only be valued at a few dollars, however the cost of the tapes to the owner in terms of preparing the programme and the disruption to his or its business activities occasioned by the theft may amount to thousands or even tens of thousands of dollars. How are courts going to assess the value of the property stolen? Is it to be the actual value of the tapes, or the cost of preparing the programme, or the cost of preparing a new programme, or the cost of the disruption to business activities. The value of goods stolen is important because that determines which court, superior or inferior, has jurisdiction to hear the matter, and if and when a conviction is recorded, in assessing penalty. What is unique in the cahse of computers, is the disproportionate difference between value of the property stolen and the cost occasion by its theft.

If on the other hand the computer containing the programme is accessed, either by an employee or by an outsider using a remote terminal, and the programme copied, so that nothing material is taken, then no offence has been committed.

However, an agreement between two or more persons to effect such an operation may amount to criminal conspiracy even though the completed act itself does not constitute a crime.

Another example of theft which falls outside the law is the theft of services, the use of computer at someone elses expense. Nothing tangible has been taken and therefore no offence committed. Even where an employee of a computer service company uses computer time for his private purposes and charges the time to one of the company's clients, it is doubtful whether he has committed any offence.

Embezzlement is the misappropriation by an employee of his employers money or goods. This is, in essence a conventional crime even though effected through the use of a computer and is adequately covered by the law. The use of a computer to perpetrate a crime may however present unique difficulties in detecting, investigating and proving the offence.

To commit the offence of obtaining property by false pretences there must be an obtaining of property by some misrepresentation of fact to a person, knowing it to be false and with the intent to defraud. If property is obtained exclusively through the agency of the computer, with no false pretence of fact being made to any person, then that could not consitute the offence of false pretences. If however, computer generated material was used to make a false pretence to some person, then that would be an offence, though again this would be an example of a conventional crime using the computer to affect the offence.

Acts of sabotage against computer hardware or the building housing the facility, are adequately covered by the criminal law. It is when damage is inflicted to computer soft ware that difficulties arise. Take for example the operator (and this occurred in France) who instructs the computer to wipe clean its memory tapes, or the person who passes a powerful magnet neat the computer tapes, thus rendering unreadable the information stored on them. Programmes and valuable data may have been irretreivably lost. The present law does not seem to adequately deal with a crime of this nature. It is uncertain whether such actions constitute a criminal offence. And, if they do, how is one to assess damage?

The falsification, alteration and destruction of records and documents are in many instances criminal offences. Directors

of companies can be prosecuted for publishing flase information. The destruction of company records is an offence. However, the falsification, alteration or destruction of data held in a computer may in many cases not amount to an offence, although clearly it should be.

Some jurisdictions in the United States have enacted legislation dealing specifically with computer crime. The Federal Legislature in the United States introduced a Bill in 1977, entitled the Federal Computer Systems Protection Act of 1977. In the preamble Congress found that computer related crime was a growing problem in the government and in the private sector, that such crime occurred at great cost to the public, that opportunities for computer related crime were great and the prosecution of persons engaged in computer related crime was difficult under current Federal Criminal Statues. The Bill then provided for computer fraud. It reads as follows:—

a) Whoever directly or indirectly accesses or causes to be accessed any computer, computer system, computer network or any part thereof which in whole or in part operates in interstate commerce, or which is owned by or under contract to or operated for on behalf of or in conjunction with any financial institution of the United States Government or branch, department or agency thereof or any entity thereof or any entity operating in or effecting interstate commerce for the purpose of —
   (i) Devising or executing any scheme to defraud or;
   (ii) Obtaining money property or services by means of false or fraudulent pretences representations or promises shall be fined not more than $50,000 or imprisoned not more than 15 years or both.

b) Whoever intentionally and without authorisation directly or indirectly accesses, alters, damages or destroys any computer, computer system or computer network described in subsection a) or any computer soft ware programme or data contained in such computer, computer system or computer network shall be fined not more than $50,000 or imprisoned not more than 15 years or both.

The Bill then went on to define access as meaning to approach, instruct, communicate with, store data and retrieve data from or otherwise make use of any resource of a computer, computer system or computer network. Property was defined to include financial instruments, information including electronically produced data and computer soft ware and programmes in either machine or human readable form or any other tangible or intangible item of vale. Services were defined to include computer time, data processing and storage functions. In addition computer, computer system, computer network, computer programme and computer soft ware and other related matters were defined in the Bill. Legislation such as this provides a far more rational approach to computer related crime than trying to fit crimes within the traditional framework of the law.

If we are dealing with computer crime we will, not unnaturally, need to rely on computer data, i.e. computer output to prove the crime. Documentary evidence is admissable in criminal proceedings (as well as civil), providing certain prerequisites are satisfied (those inclusionary rules of evidence which must be satisfied before a piece of evidence is fit to be admitted) and providing the documents themselves, or any part of their contents do not infringe one or more of the exclusionary rules of evidence (which render an otherwise admissable piece of evidence, inadmissable). The scope of this paper will only allow me to discuss the most important and potentially restrictive exclusionary rule — the rule against hearsay evidence. This rule, simply put, states that as ertions of persons other than the witness who is testifying are inadmissable as evidence of the truth of that which is asserted. The rule applies to oral as well as written statements and the rationale of the rule is that in such cases there is no opportunity to cross-examine the maker of the statement and thus test the truth or accuracy of that statement. A number of exceptions exist, developed by the common law or created by statute.

Computer data would invariably be hearsay unless the person who initially fed into the computer the information on which the data is based or a person who was present when the information was fed into the computer could testify as to his, or their knowledge of the truth and accuracy of the information or unless the data fell into one of the exceptions to the rule. Because of the intrinsic nature of computers they are usually employed in areas where a great amount of information is being processed, for example, banks. The computers are being operated by specially trained operators who have no personal knowledge of the information being processed. Therefore there is no-one who can testify as to the truth or accuracy of the data and it is therefore admissable unless it can be brought within one of the exceptions to the rule. Here in S.A. we have legislation specifically providing for the admissability of computer evidence in criminal proceedings (i.e. a statutory exception to the rule).

In 1972, Part VIA of the Evidence Act was enacted to provide for the admissibility of computer evidence in civil proceedings. In 1979 this was extended to include criminal proceedings. The Act defines computer to mean —

" . . . a device that is by electronic, electromechanical, mechanical or other means capable of recording and processing data according to mathematical and logical rules and of reproducing that data or methematical or logical consequences thereof."

"Computer output" or "output" is defined as meaning —

" . . . a statement or representation (whether in written, pictorial, graphical or other form) purporting to be a statement or representation of fact —

(a) produced by a computer; or

(b) accurately translated from a statement; or representation so produced."

"Data" is defined to mean —

. . . a statement or representation of fact that has been transcribed by methods, the accuracy of which is verifiable, into the form appropriate to the computer into which it is, or is to be introduced."

The Act goes on to say —

"Subject to this section, computer output shall be admissable as evidence in any civil or criminal proceedings."

In other words the Act provides for the admissibility of evidence which may otherwise be inadmissible because it offends the rule against heresay. The Court however must first be satisfied of seven conditions:—

1. "that the computer is correctly programmed and regularly used to produce output of the same kind as that tendered in evidence pursuant to this section."
2. "that the data from which the output is produced by the computer is systematically prepared upon the basis of information that would normally be acceptable in a Court of law as evidence of the statements or representations contained in or constituted by the output."
3. "that, in the case of output tendered in evidence, there is, upon the evidence before the Court, no reasonable cause to suspect any departure from the system, or any error in the preparation of the data."
4. "that the computer, has not, during a period extending from the time of the introduction of the data to that of the production of the output, been subject to a malfunction that might reasonably be expected to affect the accuracy of the output."
5. "that during the period there have been no alterations to

the mechanism or process of the computer that might reasonably be expected adversely to affect the accuracy of the output."

6. "that records have been kept by a responsible person in charge of the computer of alterations to the mechanism and processes of the computer during that period."

All of the requirements already referred to are dependant, to a greater or lesser degree, on proper records being kept by an appropriate and responsible person of the operation of, and any alterations to the computer system. Given the assumption that very few persons responsible for the computer operations of their organisation would be aware of the requirements of the Act it is not improbable the some difficulty would be encountered in satisfying a Court of these first six requirements. The answer is in better awareness of these requirements.

7. "that there is no reasonable cause to believe that the accuracy or validity of the output has been adversely affected by the use of any improper process or procedures or by inadequate safeguards in the use of the computer."

I have already commented on the lack of safeguards practised by the industry. These requirements touch upon the most fundamental weakness in the use of computers – a lack of adequate safeguards and controls over the computer operation. I believe that as we gain more experience in investigating and attempting to prosecute computer crime, the greatest difficulty that we will encounter will be the inability to use in evidence computer output because of inadequate safeguards and controls and records of the operation of the computer systems.

The Act also provides that where two or more computers have been used in the recording of data and the production of output, that the seven requirements referred to be satisfied in respect of each computer.

In the area of corporate crime, which I think is analogous to many computer related crimes, the investigation and unravelling of complex frauds which are committed behind a screen of inter-related corporate entities and the manipulation of accounts and records, presents the authorities with a daunting and difficult task requiring the co-operation between the fraud swad police, accountants and lawyers. It is only through the joint efforts of these professional people that corporate crimes come before the courts. The prosecution of these frauds are usually a lengthy, costly and difficult undertaking require the presentation of evidence, both oral and documentary and of a technical and complex nature. The trial of serious criminal cases in this country is conducted before a judge and a jury of twelve lay persons. The trial judge has charge of the proceedings, he determines questions relating to the admissibility of evidence and he directs counsel and the jury on all questions of law. The facts, notwithstanding anything counsel may say or indeed the trial judge, in the course of his summing up to the jury, are for the jury and the jury alone. In enpaneling a jury, an accused has a statutory number of peremptory challenges, in this State three, and in joint trials, a feature not uncommon in corporate frauds, the number of peremptory challenges available to the defence is multiplied by the number of accused persons. Invariably any person experienced in business or holding professional qualifications is challenged. The result is a jury made up of persons whose business and accounting experience is limited to organising and balancing their own personal budget.

Upon these people is thrust the responsibility of comprehending and determining the complex issues presented in corporate frauds. To add to their difficulties such trials are usually lengthy (trials of four to six weeks duration are not uncommon), the documentary evidence may number in the hundreds and include detailed accounts and other company records. They, on the other hands, are required to return a verdict within a few hours and although they have the documents with them whilst they are deliberating, they do not have the benefit of the transcript of the proceedings. They must rely on memory or on returning into court to have exerts of the evidence read to them. It is not surprising that doubts have been raised over a lay juries ability to do justice in such cases, not only to the prosecution case, but to any defence put forward by an accused.

The same considerations would apply to trials of computer related crimes and indeed may be exacerbated by the fact that a computer was used to perpetrate the fraud. If the computer remains an unknown, "orwellian" device to all but a few trained experts, how can we expect a lay jury to properly comprehend the way in which a computer was used to effect a fraud possibly running into millions of dollars.

One of the factors which tends to make the prosecution of corporate crime a lengthy exercise (in terms of the number of days or weeks to hear all the evidence) is the amount of time spent in what lawyers call "formal proof". That is, proving the existence of certain facts which are ancillary to proving the fraud, but which must nevertheless be proved in evidence. I refer to such matters as the existence of companies, details of directorships and other office holding, proving records and books of account of the company or of a group of companies and proving bank records and the existence of certain transactions, payments, cheques and withdrawals. Such formal matters may not be in dispute, as indeed a lot of the evidence presented by the prosecution may not be disputed. Nevertheless courts, juries and witnesses spend a vast amount of time engaged in hearing of these matters.

Courts in other parts of the world have adopted a system of pretrial conferences where prosecuting and defence counsel come before a judge, preferably the judge who will preside over the trial. In the course of the pretrial conferences matters not in dispute are determined (and the jury can be directed as to undisputed facts). In addition any disputes including the admissibility of evidence can be determined and a ruling given, instead of determining them in the course of the trial and in the absence of the jury. Other matters which could also be determined are severance of trial involving joint accused, objections to the form of the indictment, the venue of the trial and any procedures to be adopted during the course of the trial. The results of such pretrial procedure would be a shortening of the trial and a saving in the time of the courts, thus freeing them to hear other cases. The trial would be simplified, the jury would not suffer the interruptions they do now, whilst matters we determined in their absence. Furthermore, both prosecution and defence could better present their cases, the issues having been clearly defined beforehand. I can see no real difficulties in adopting such a court in this country and if the mounting pressure on the time of our criminal courts is to be relieved, some form of pretrial conference is both desirable and inevitable.

The trend in this country in recent years has been to make more and more offences, particularly statutory offences triable summarily. In many instances the option is given to an inferior court to hear and determine a matter or to set it down for trial before a superior court with jury. One example of this is a variety of offences created under the Commonwealth Bankruptcy Act. If the inferior court opts to hear the matter summarily then the maximum penalty it can impose is less than would be available to a superior court following conviction by a jury. This option however is not available in Australia for the more serious fraud cases involving large sums of money. Some jurisdictions overseas, where trial by jury is the rule of law, an accused is given the option of a trial before a single judge. The experience in Canada, where an accused can elect in a trial involving a serious fraud, has been that most choose to stand trial before a single judge, particularly where their defence is of a technical nature. In the United States

many serious crimes are determined by a trial judge alone – the accused being allowed to waive his right to trial by jury. It has been estimated that in some states, waiver of jury trial occurs in 75% of trials for serious offences.

Trial by a single judge would result in a speedier trial and it would avoid the problems encountered when presenting difficult and complex cases before juries. The trial judge has the training and experience to evaluate and understand evidence, he would have the transcript of the proceedings available and he could take longer to consider his decision than is presently available to a jury. Trial by jury is, however, firmly entrenched in our system of criminal justice and is accepted by the community at large as a fair and impartial means of ensuring justice. Indeed I believe that in most types of criminal conduct the right of trial by jury should be retained. To abolish it for certain classes of crimes would be bound to meet very strong opposition. Giving an accused person the right to waive trial by jury in serious fraud cases, including computer related frauds would perhaps engender less opposition. However, whether the option would in this country be exercised at all is a matter of conjecture and would not in my opinion be of any benefit in the short term. In a joint trial of two or more accused, unless all of the accused were in consensus as to the mode of trial, the only possible procedure would be trial by jury.

The second alternative is trial by a panel of judges. It has all the advantages of trial before a single judge as well as one essential feature of trial by jury, and that is a forum where views and opinions can be discussed, and where ones reasons and conclusions can be critically examined by others and any flaws brought to light. It avoids the one criticism I would make of trial by a single judge in cases where the liberty of the individual is concerned, and that is the danger of a biased or arbitrary decision being made.

The third alternative is trial by a judge and special jury. The power to order the empanelling of a special jury could be given to the court at its discretion on application of either party, where, because of the intricacy of the case, or other relevant consideration the proper administration of justice in the case could best be served by trial before a special jury. The jury panel from which the jurors are selected, could then be drawn from specially qualified lay persons having expertise of those issues likely to arise in the course of a trial. Because the jury would be made up of experts perhaps six jurors instead of the traditional twelve could be justified.

The fourth alternative is trial by a judge sitting with assessors. Mr. Justice Wilson in his paper "The Jury System in Relation to White Collar Crimes 1976" had this to day of this alternative:

"The logic of such a proposal is inescapable, given the proposition that these long and difficult cases require professional adjudication without at the same time losing that confidence of the community which lay participation has tended to preserve . . ."

There has been quite a strong tendency in Europe in recent decades to replace the jury with lay justices or assessors, sitting with the judges and sharing with them the responsibility of deciding both fact and law and determining sentence. Germany appears to have lead the way with the Schoffen in 1924, followed by the Scandinavian countries and France. The size of the tribunal seems to vary a good deal, as does the degree of permanency attaching to the appointment of the lay assessors. In my submission, there is no warrant for considering a tribunal consisting of more than one judge and two assessors. The assessors should not sit regularly, otherwise they would tend to lose their lay character; they could be drawn as required by ballot from a panel compiled by the sheriff on the nomination of reputable commercial, scientific or professional bodies. The concept is that the assessors would bring relevant expertise to the particular case, while at the same time contributing to the general outlook of a layman which has been described as one free from any responsibilities to the State, unfettered by any narrow legalistic approach, unaffected by lengthy experience of the police and criminals and drawn from wider social backgrounds than professional lawyers."

I believe that some changes to the present system are necessary if we are to adequately cope with corporate and computer crime. We have available a number of options. Whatever changes are made, and I believe that they are inevitable, we must ensure that they are such as will not destroy the confidence which the community has in the fair and proper administration of justice.

This brings me to the last point I wish to make, and that is the question of penalties. In a recent study in the United States of 207 corporate criminals convicted of very serious frauds, many of them involving computers the following facts emerged:

a) Only one third were gaoled, for up to three years, for thefts of almost 16 million dollars.
b) Nearly half of them received less than 12 months for offences which netted 23.6 million dollars.
c) 26% received only fines, suspended sentences or parole. They netted 21.6 million dollars.

Penalties for the computer criminal in the United States have been uniformly light. The reasons for this trend are not clear. I can only suggest a few –

1. Because of the inadequate security companies exercise over their computer systems, it may be seen that they are almost inviting someone to come and steal from them.
2. The novelty of the crimes. Because computer related crime is a relatively new phenomena and so different in nature from the conventional crimes courts are used to dealing with, judges may be inclined to treat an offender leniently.
3. The background of the computer criminal. Courts take into account the background and previous character of a convicted person when assessing penalty. Such factors as family background, education, work history, social standing and previous convictions all play a part. The computer criminal is more likely to come from a good background, he does not have previous convictions, he has a good education, he usually has an excellent work history in well paid employment, he is married, prosperous and in all other respects a solid citizen. This differs markedly from the background histories of a large proportion of the persons who come before the courts and of course is something which operates in favour of the computer criminal.

It is difficult to rationalize the seriousness of the offences to the penalties imposed upon computer criminals. What the courts in the country will do when they come to sentence the computer criminal is uncertain, for no-one has yet been convicted of a serious computer related crime in Australia. However, if we look to see how our courts treat white collar criminals – directors who misappropriate their company's funds, doctors who defraud medibank and the like – their sentences are invariably lighter than criminals who steal by other less sophisticated means.

I believe penalties that reflect the seriousness of computer related crime would provide a deterrent. As I have already pointed out the profile of the computer criminal is that of a well educated well paid and motivated individual. The crime is usually well thought out and planned in advance and with knowledge that –

1. Detection is unlikely.
2. Even if detected prosecution is unlikely to follow.
3. Even if prosecuted, because of the complexity of the crime a conviction is not certain.
4. Even if convicted the chances of serving a lengthy prison sentence are small and indeed a suspended sentence is more

than likely.

Computer crimes are not crimes of passion or crimes that have their origin in the depressed and underprivileged background of the offender, who is more controlled by events than able to control them. In those instances the deterrent effect of imprisonment has, at most, a dubious effect. Not so the computer criminal He knows full well the course he is about to embark upon. The knowledge of certain imprisonment if he is caught is more likely in my view to have a deterrent effect. He has, after all, more to lose. Couple that with certain detection and a criminal system designed to deal with him, he may be dissuaded from embarking on his criminal activity.

In conclusion ladies and gentlemen, I feel that we as a society are ill-prepared to meet the threat posed by the computer criminal. If we are to adequately cope with this threat we must make some radical changes to the manner in which we control the computer and in the arena of law enforcement and criminal justice. Only then can we go from being one step behind the computer criminal to being one step in front of him.