THE DEVELOPMENT OF COMPUTER AND OTHER WHITE COLLAR CRIME

by
Mr PETER R. MARRIOT,
A.C.A., B.Ec. [Hons]

I MUST say that I feel like a slave being thrown into the lions' den as an accountant amongst a group of lawyers and others having to talk about computer crime. But, I think it is an issue that we have to come to grips with in our society today. What I intend to do is, not only just concentrate on computer crime, but to focus on two of what you might be able to describe as *"romantic areas"* which command a lot of media attention, a lot of management attention, these days. That is, the whole area of computer crime and also of foreign exchange fraud. I think that in terms of the most recent developments and in the most publicised areas of white collar crime, they have to be the main ones.

When I talk about computer crime, I mean crime that involves unauthorised access to data, unauthorised manipulation of data, unauthorised changes to programmes or unauthorised copying of programmes, right down to the good old-fashioned types of crime that we are used to in the areas of trespass and sabotage. In the area of foreign exchange fraud, well, there we are touching on the types of alleged frauds that we have seen in organisations such as Westpac, alleged frauds over in Broadbank in New Zealand, the problems that we have been having recently in companies like AWA, and a whole series of others that I have also been involved with that haven't made it to the press.

Anyway, let's start by looking at the whole area of computer crime. I think it's very important for us to get a little bit of perspective about the importance of the computer in today's society. It used to be that wealth would accrue to people who had physical capital. If you had physical capital, then resources would be directed towards yourself; you had command over those resources. The society that we are moving into today is very much information-based. Wealth and power is accruing to people who have information. Of course, data processing is a very key in that whole environment as a major means by which we process information. So, consequently, crime directed towards information will be the challenge of the future, rather than crime directed towards physical assets.

It is almost trite to say that virtually every single company in Australia is highly dependent upon data processing. Estimates say that a bank cannot last more than two or three days and remain a going concern without its data-processing system. Look at the disruption that happened with Westpac when all that happened was that it lost its ATN network. Can you imagine what would happen if it lost its entire data-processing environment?

I think this is another area where we will probably find that the directions will change. Concepts of terrorism and other types of crime of that nature against society will appear. If I were a terrorist I wouldn't go around bombing restaurants, I'd go around bombing payroll bureaus and bank data-processing bureaus and bring down the entire economy rather than just a few people. So it's an area where we have to direct our attention to see if we have got the correct management and legal framework to control those sorts of exposures.

Turnover. Electronic Funds Transfer networks in the world today move around $5000 billion a day. Think of the consequences of misdirecting only 10 per cent of that traffic.

PETER R. MARRIOT

MR Marriot is the partner responsible for the computer audit practice of the Melbourne office of the well-known accounting firm, Peat Marwick Hungerfords. He has extensive experience in the security of data processing, particularly in the environment of large companies in the finance industry.

He has developed and presented both in-house and external EDP security training courses in Australia and overseas. He has devised computer-assisted audit techniques and methods to evaluate the efficiency of EDP safeguards. Much of his work has involved the security of foreign exchange dealings, an area in which he has advised and assisted many companies.

The topic which he addressed at the Adelaide conference was a little off-the-beaten-track for many involved in the criminal justice system. It was all the more interesting for that. Mr Marriot spoke in vital and challenging terms and it is with great pleasure that we reproduce his address here. Readers are asked to remember that what follows is a report of an address and not a published paper. Any errors or omissions can be laid firmly at the feet of the editor.

PRIVACY. It used to be that we could have physical doors; we could lock things away and keep our information confidential. Now, the concept of the public database is such that unless we have controls over access to that very concentrated and very valuable collection of information, then the implications for social values and also for crime are horrendous.

A little bit of background on some of the statistics of crime in Australia and computer crime in particular. One of the big problems that we have is that organisations do not like to admit that they have had crime in their computer environment. Banks, in particular, feel that if they were to admit that they had had a fraud take place in their data-processing environment then that would impact upon the integrity of their whole operation. *"How will our customers trust us if we are having these sorts of things going wrong?"* So, consequently, the statistics that we have are very limited. Some of the learned authorities in this area estimate figures in the region of $80 to $200 million in computer crime has taken place in the last 10 years or so, but those incidences that have been actually documented only amount up to about $9.8 million and the black areas on the diagram shown represent those that relate to fraud — unauthorised manipulation of financial information. As you can see, that is the vast majority of the computer crime that has taken place. You will also notice that it is whilst it is not the majority in the case of number of instances, but it is certainly the majority when it comes to value of those instances.

That is the extent of crime. But who actually is doing it? We get some very interesting statistics here. With a large proportion of computer crime we haven't been able to identify exactly who the perpetrator has been. When it comes to crime being committed by *"hackers"*, we have a similar problem. Identification in the computer environment can be very difficult.

What, then, has been the fundamental change that has meant that some of the legal and control issues relating to computers have become so much more complicated? I think the big change has been the fact that, as I have said before, originally we used to erect walls and locks and doors to protect our assets. Now, the demand for information is such that we want to be able to have access to that on-line real-time, all these buzz words 24 hours a day, geographically throughout the world. All of a sudden those barriers have gone and that creates new challenges. We also have the problem that the people who are responsible for managing our companies are basically computer illiterate and yet they are trying to manage a generation of up-and-coming people who are highly computer-literate. That's a challenge that we all face because all of the younger members of our society have got far more exposure to data processing than we have and probably than we ever will have. How do we control that?

In summary, can I suggest some of the implications? Obviously, we have the risk of pilfering, of misappropriation of assets. There have been numerous examples of that.

Breach of privacy. There have been a number of examples, of course, where people have got into medical records and have been able to find out a lot of detail about very prominent public people. Health records, etc are obviously very private and a confidential source of information.

There are some well-documented cases of around the time of the wedding of Prince Charles in the United Kingdom where hackers were commissioned to try and find out how much Diane Spencer was spending prior to her wedding. This was to be published in some of the European magazines and so forth. That sort of confidential information was very valuable to people because of the publicity it would bring.

Industrial espionage. I go around to a lot of my clients and I find that perhaps they have got reasonable control over their main-frame environments, their main computer systems, but where are they evaluating their take-overs? They are evaluating them on personal computers. What is the control over the PC? None. It is sitting on an office desk there. Where are the diskettes? They are sitting in a drawer. Yet it is on those machines that they are evaluating whether to take over ACI, or to take over BHP or whatever. Yet security over that is very, very small.

Electronic terrorism. Perhaps Colonel Gadaffi could think about getting into an Electronic Funds Transfer Network. I think he could probably do more damage to society than through the actions that he is taking at the moment. A further comment that I would perhaps like to make on that area of electronic terrorism is that this is an area that we have really got to try and come to grips with because that is the direction in which society is heading. Unless we get control over those sorts of areas, the sorts of exposures that we can be confronted with are very difficult to conceive at this point in time because we are becoming so dependent upon it.

The last one I have on my list is organised crime. To date, there has been very little hard evidence that organised crime has got involved in any of these *"hacking"* activities or in computer crime. But let's face it, in a society which is moving increasingly away from cash and physical assets towards Electronic Funds Transfer and information on the computer system, then, really, the area where the greatest potential rewards exist is probably in computer crime and not in holding up banks. Also, at the moment in the way in that the law seems to be working, the penalties for computer crime are far less than for holding up a bank.

Obviously, we could spend hours going through some of the cases that have taken place. I do not want to do that because I think you are probably aware of some of the sorts of computer crimes that have been committed. I want to try and get down to think about some of the implications and some of the issues that arise out of that.

I think that you can probably break the sorts of crimes down, broadly, into two categories. The smash and the grab. First, the unauthorised transfer of funds and then the skipping of the country. Secondly the drip type, where there is a taking of a little bit at a time. All the sorts of crimes that you can look at, you can probably put into one of those categories.

The way that is being done has involved a number of different techniques. The programmer who goes in and changes the programme. One of the favourite ones that I have seen is that of the programmer who is a contractor and who is brought in to an organisation to write a payroll system. After about six months the payroll system is working. It is terrific. The best payroll system they had ever had. So, they no longer need the contractor. The contractor is fired. The next time they try to run the payroll system, it falls over. They call the contractor back in. The contractor works for three months. He gets everything working again. Then they don't want him. They fire him. Next week, the payroll system falls over again. In this scenario, the employer started getting a little bit suspicious by this time and brought in another contractor who, on further investigation, discovered that the programme said that if the name of the contractor was not on the payroll, then the programme was to stop. It is an interesting way of ensuring your own continued employment, isn't it?

MASTER file changes. So often computer-generated cheques are produced based on master file information. Standing information. You key in an account number and automatically it picks up the address of the creditor, the payee name, etc for cheques. Change that sort of information

and you are changing funds transfers. You can very easily misappropriate funds in that way. There have been a number of instances based upon that sort of scenario.

The other one which I think is one of the worrying ones. The whole area of virus code. This is one that I seem to be finding is growing a little bit in recent times. Virus code refers to programmes that a would-be saboteur might introduce. Perhaps the guy may not be deliberately trying to take the organisation down to misappropriate, but he may want to wreak some sort of revenge on the organisation. So he leaves behind a little programme that every time, every day, it does a little bit more damage, progressively. It spreads its disease of corruption throughout the whole system, so that eventually the system is rendered, perhaps not totally inoperable, but so damaged that to recover from the problem it becomes very very difficult.

Anyone with sufficient power could go and wipe off the entire database of National Australia Bank tomorrow if they had the right access within the system. But, all data-processing environments keep back-up so that they can recover from that sort of disaster fairly quickly. The sort of virus that it is slowly building up and therefore gets built into each of the back-ups that are being taken is very hard to protect against.

Enough of that background. Enough of my little harum-scarum tactics.

I think that it is probably fair to say, that given the growth of data processing, given our emphasis on an information society, given the growing level of computer literacy, it is almost inevitable that computer crime will take place. What do we do though to correct that problem? Who is responsible? Is it the law? Are the auditors responsible? Is it management, or is it society in general? I want to address each of those separately.

This is when I get worried, talking about the law in front of a group of lawyers. I think it is fair to say that the law has historically emphasised physical capital because in the past, that was the basis of wealth and power within society. We need to have now a subtle change in the emphasis of the law to recognise the movement in society towards an information-based society. That, of course, is going to provide challenges to the way in which laws are drafted to reflect that new change.

Some examples. Quickly running through some of the classic sorts of crimes under the heading of forgery, theft and fraud etc.

Forgery. The trouble is that most of the law at the moment is couched very much in terms of physical documents, not information stored on a computer file. Why? Because when the law was drafted it was difficult to conceive of that sort of technology.

THEFT. I come in and take a copy of a mailing list. I come in and take a copy of some confidential information about take-over bids. What have I stolen? Well, I have stolen, if you like, a copy of something. Have I deprived the other person of use? No, I haven't. All I have done is taken a copy of something. So the traditional concepts of theft do not quite hold up in that sort of environment — meaning, we need some change in our attitude to theft in a computerised installation.

Fraud. Most of the classic law in the area of fraud relies upon deception and deception of a person. If I managed to trick an automatic-teller machine into giving me extra cash, have I deceived a person? No, I have tricked a machine. The current area of fraud legislation needs to expand to recognise this broader definition of deception so as to catch machines rather than just simply people.

Are there any other legal avenues? Some of the areas that perhaps we can focus in on are things like the Copyright Act. The only difficulty there is, in my understanding of the copyright law, that if I just simply take a copy of something and I do not go and try and resell it or market it or try to profit from it by making it available to other people, then it is difficult to bring an action against me. When I just go and copy it for my own use then it is not as easy to bring a legal action against me. Trade Marks Act, Design Act, Companies Code. There is some hope within the Companies Code, perhaps, but even that is very indirect. We are starting to snatch at straws there, because in there, there is a section which says that if someone manipulates the accounting records of a company, then it becomes an offence. And given that the accounting records can be on computer then you can get, perhaps, some action there and say that they have committed an offence by manipulating the accounting records of the company.

Contract. Yes, the trouble is in so many cases when you are talking about a hacker, there is no contract with the hacker so you cannot take him to law for breach of contract. So often I find with a lot of my clients that you cannot take someone to court on breach of contract even if he is an employee because so often the policies and procedures within the organisation are so poorly defined that it is very difficult to say, *"Well, you have breached some term of our contract,"* because everything is so informal.

What do I, then, see as the issues from the legal perspective? A need for effective legislation. That really means not so much changing the fundamental concepts behind the law, but updating them to reflect the technology that we are now employing. I think it is interesting to note that in the USA there is, in fact, a requirement to report any fraud that takes place, any computer crime that takes place. I think that that is the sort of legislation that should perhaps be considered in the Australian environment as well.

TRAINING. This becomes a problem that not only focuses on police and lawyers, but also right the way across the board — management, auditors, too, as we come to speak about in a moment. If we don't understand this sort of crime, if we don't understand the sorts of techniques that are used, it is very difficult to protect against it and it is very difficult to legislate against it. We can all understand someone smashing into a bank with a revolver. We perhaps cannot understand someone jumping into an IBM MBS-operating system and using an apiath-authorised programme to change the IO appendages to access a sensitive data set. But that is the sort of scenario that we are talking about that these sorts of crimes must be based upon.

It is interesting to note that the Victorian Parliament is considering some legislation to try and correct some of the problems that I have referred to by broadening the definition of deception to get over this problem that it has to be a person and a machine does not count; and to extend forgery to electronic documents as well as physical documents; and also to get over the problem that in a network-type environment, I can literally dial into a computer centre in another country let alone in another State. Obviously, it can create some legal hurdles when you are trying to sue someone or take action against someone who is resident in another State, but who has committed the crime in yet another State.

So much for the legal side of things. But there are other things that I want to get across in this session. It is okay, no doubt, to go and pick on the law and say that the law has not kept up-to-date. But it is not only the law that has not kept up-to-date. I would comment that in many ways *"the best deterrent is certainty of detection"*. So how can we be sure that this sort of crime gets detected? Perhaps even better, how can we be sure it

gets prevented in the first place? In that area, I want to speak about the role of the auditor and the role of management.

Auditors are out-of-date. I am responsible for our computer-audit practice and I am still saying that, in general, auditors are out-of-date. The technology is moving so quickly. The other problem, too, is that it is not really clear as to exactly who is responsible within the audit profession for looking after these sorts of issues. To look at the external auditor for example: his responsibility is laid down within the Companies Code which simply says that he has to form an opinion as to whether the accounts are true and fair. Now as I sometimes joke with my clients when I am trying to encourage them to do something about their computer-security deficiencies, I say something along the lines of, *"Well, really, when it comes down to it, I don't care if your data-processing environment blows up as long as you write it off in the accounts"*. That is the sort of problem that perhaps the external auditor has. At the moment, he does not really have an official brief to look at these sorts of areas. All he has to do is form an opinion on the accounts.

The internal auditor. So often we find the internal auditors, unfortunately, have come from a background where they have been management people who have not made it. Increasingly, though, we find that organisations are recognising the need for competent internal auditors in establishing EDP audit functions, but there is such a shortage of EDP auditors that it is not funny. The market for EDP auditors is extremely tight.

I APOLOGISE. I know that when I give a presentation I jump around and move around. In fact, someone once described me as being rather like a cross-eyed discus thrower — by that he meant that I do not break many records, but I certainly keep the crowd alert.

Management. I think it is fair to say that management have a large responsibility in this area. Management have put a lot of pressure upon data-processing people to deliver results. Management want information. They are not necessarily providing sufficient resources to, not only provide information, but also to provide that information in a secure fashion. By the same token, management has tended to ignore the need to implement adequate control. Now I have been around a large number of very large organisations in Australia, including banks, and some of the larger corporate organisations, indeed all of them to a certain degree, are exposed to potential computer crime. The exposure is very very small when one refers to the banks. Others are basically just lying back there waiting to be taken. Why? Because there is not really an awareness of the need for security and control. So, ultimately, I guess those organisations are hoping that the law will be able to protect them for their own negligence in not putting controls in place in the first place. The other problem that we tend to get is that senior management, because they do not understand, tend to abdicate responsibility for security and control down to their data-processing people. The consequence of that is that you are asking the people that you are trying to control to a certain extent to implement controls for themselves. From the good old-fashioned internal control point of view, that is not very good.

There have been a number of recent surveys done on the adequacy of security in data-processing environments within Australia and the result of all of those findings has been that invariably the risks seem to far out-weigh the investment that has been put in to protect against those risks. We have an imbalance. There is scope for improvement in control. I am thinking of a survey done of about 370-odd organisations where they only came up with about five that they regarded as having adequate security. I know that amongst my client base, I would only regard one of my clients as having what I would consider as being acceptable security. If you think about that in terms of a large chartered accounting firm in Melbourne with 385 staff — think of the number of audits we must do in that size organisation — that is a very small proportion.

Some of the key issues where people go wrong leading to these problems with security. I do not think I have come across an organisation yet, before I went through and did a review and recommended that they establish one, that actually set down a policy as to what they wanted to secure and what their attitudes were to security. This is to cover a whole series of areas like who actually owns the data? What do we do if someone violates this data? I had one organisation where a programmer had written a very nifty little trick. He had written a programme which put a screen up on the video display terminal that was to mimic the normal log-on screen so when someone came along it looked as if it was asking for someone to log-on when, in fact, it was his own programme. The purpose of that was so that when the person did come along it would capture his password. This programmer was building up a collection of passwords. As soon as the password was entered the thing would fall over and say, *"System error — please log-on again"*. No-one was suspicious at all. Eventually they found out what this guy was doing and it took them five days to decide whether they should fire him or what to do with him. They had to take on legal opinion and the legal opinion said, *"Well, look, you've never actually at any point laid down clear policies in this area. That guy could quite easily sue you for wrongful dismissal"*. A lot of problems existed because policies were not laid down. Consequences of violations of policies weren't specified.

LOGICAL security. By that I mean password-type security. So often we find that the responsibility for managing that security is very poorly specified. The people who are managing that security are perhaps the people you really want to protect against. We also ultimately have the problem that in any environment, in any data-processing environment, there has to be someone who holds the key. Ultimately, someone can do anything in that environment. How do we protect against that sort of person?

In an environment where we have nation-wide and, in some cases, international telecommunication networks, how do we identify the person we want when a crime takes place? The password system that we use at the moment as the main vehicle for authorisation of access to a computer system is, at best, hopeless. The whole basis behind hackers getting into a system is through abuse of the password system. We need really to be moving to some sort of more sophisticated means of identifying and establishing the authenticity of someone who is trying to access our system through a terminal.

A final comment in the area of computer crime before I move on to foreign exchange fraud. I know we have moved on very quickly, but I guess my objective is very much to raise in your mind some issues, some problems, so that when we have the workshop tomorrow, we can expand on these a little bit more and discuss them. I think that society has some major responsibilities in this area. I think the way that, to some extent, the media has portrayed it, the hacker is almost seen as being a hero when in actual fact what he is doing is potentially committing a crime against society. He is breaking in and obtaining confidential information about your own personal credit details and finances. That is not being a hero — that is a crime against society. Unfortunately, films like *"War Games"* and the like have only sought to dramatise all this and to make it sound all very romantic. But really, there is a need for change in social attitudes as much as management attitudes and for the law itself to recognise that these sorts of things are crimes and not fun games.

Some of you may be wondering why someone who is talking about computer crime is also able to talk about foreign exchange

law. It seems like quite an unusual combination. The history behind that is that I was given responsibility to do the audit of a foreign exchange operation. Why? Because it was a major data-processing system and everyone thought the issues were in data processing. I soon came to realise that the issues were not in data processing, but that they were in management of that foreign exchange operation. In Australia every day, there is $30 billion turned over in the foreign exchange market. We have only got to look at the sorts of losses that have taken place in big trading companies and other organisations to understand the consequences of inadequate control. It used to be, too, that the only losses that we saw were losses that took place purely because of management mis-judgements, if you like. Inappropriate strategy when it came to foreign currency management. In recent times we are starting to see more fraud; and by fraud I mean situations where the dealers who are responsible for managing those foreign exchange risks are actually taking actions that were not authorised by management. I will expand on that a little bit now.

The concept of what is called *"Off-market Trading"*. I do not know how many of you have sat inside a foreign exchange dealing room, but it is a strange experience. Foreign exchange dealers are a unique breed of professionals that provide any organisation with a major challenge to control their activities. The market is very fast-moving and it has its own language and own ethics. This area of off-market trading may allow a dealer to enter into an arrangement with another organisation whereby they agree to always give each other concessional rates. *"I'll always shave five points off my rate, but I want you to give me 50 per cent of it back as cash in my pocket"*. In an environment where the Australian dollar has moved up to 200 points in one day, five points on every transaction is virtually impossible to detect. Yet, I am aware of one publicly-announced crime and two other clients of mine have called me in to investigate these sorts of problems. All that has taken place in Australia in the last three years. The amounts that we are talking about are not small. In one case, the amount of the loss represented 25 per cent of the shareholders' equity of the company. So it is certainly not small.

Unauthorised trading. So often we find — and some examples of that are evident in Australia and overseas — where a dealer takes a position, as he is managing his foreign currency risk, and he makes a mistake. He makes a loss. He still believes that his judgment is right. He takes a bigger position in the hope of it getting the profit back again. It still goes wrong. He takes on an even bigger position and he exceeds the discretion given to him by management. He starts to trade in an unauthorised fashion and, invariably, what then happens is that the dealer is forced to commit a number of frauds. He suppresses the fact that he is exceeding his position. He has gone over the limits that have been given to him; he holds back deals; he rigs records; he falsely reports to management a whole series of his transactions in the hope of making the loss back again and no-one finding out what he has done wrong. Another example of fraud!

MISAPPROPRIATION is not common in Australia at the moment, but certainly the exposure exists in any environment where you are moving around $30 billion a day. If one was to only mis-direct one of those transactions, one would not have to work for the rest of one's life.

Where do foreign exchange frauds take place? Everywhere, potentially. The exposures exist in all organisations. It used to be, when I started doing consulting work in this area, that it was the banks and the near banks (the merchant banks and finance companies) that were calling me in. Over recent times, 80 per cent of the work that I have been doing has been in corporated organisations. They are recognising the risks that exist. The AWA loss is just a classic example of that.

Semi-government organisations must face the same things — foreign currency borrowing, concepts of active debt management and all these sorts of things require that control in those areas is just as important.

Why do these frauds take place? What has gone wrong that lets them take place in the first instance? Absence of policies. What happens in a typical scenario is that management identifies that they need to have more expertise in managing treasury, and I don't mean Government Treasury, I mean treasury operations, management of interest rate, currency liquidities and those financial risks their organisation confronts. So, what do they do? They establish a specialised treasury function they bring in a whizz-bang dealer from a bank and say *"Go for it, manage our risks"*. What policies do they establish for him? Frequently, none. Do they establish a form of mechanism with limits in which he is allowed to trade? Do they establish formal mechanisms and systems to monitor what he is doing? In a lot of cases they do not. As a result, they have not got adequate management control over those treasury activities and it's a recipe for unauthorised trading and losses taking place.

Management abdication. An extension of what I was just saying. I find this that so many organisations, especially corporate organisations, because they have established this treasury function, they therefore think they do not have to worry about those risks anymore. They think that it is all under control and they do not monitor what is happening. They do not watch on a day-to-day basis to find out what that dealer is doing; what losses he is making; what positions he is taking; and they find out about it when, all of a sudden, there are huge losses. They start to see their cash flow getting affected and they wonder what is going on and they investigate and they find out too late about all these transactions.

Verbal contracts. In the foreign exchange market, deals are done over the telephone. There may be very little documentary evidence that the deal has even taken place. The potential to suppress a transaction is obviously very great in that environment.

SUMMARY

Under the heading of Computer Crime, I see the priorities that society must face looking at a global level. First of all, it must look to prevent the crimes taking place in the first place. That very much becomes a management responsibility; to put the systems in place to prevent crimes from happening. Failing that, it must have the systems in place to detect quickly that a fraud has happened and to stop it from happening again. Closely associated with both of those issues is the whole area of having to change the basic social attitudes of our society; also to educate people throughout society into the issues associated with computer and computer crime. Then, finally, I see then the need, of course, to have the legal fabric there, so that when all these others fail, there is the legal framework there to be able to take action against the person and to act as the ultimate deterrent.

On the foreign exchange side, the first issue is, education. So often, when I have gone to different clients, one of the major recommendations I have had to make has been to recognise the need for training of people to understand what is happening. If they cannot understand the operation, they cannot control those operators and they are blindly trusting what the dealers are telling them. Finally, there is a need for systems to monitor what activities are taking place and to ensure that they are all authorised and being properly recorded.

Throughout all of that, I guess I am trying to make sure that we do not find ourselves behind the eight-ball suffering a loss for a computer crime or, alternatively, for a foreign-exchange fraud.