COMPUTER CRIME AND SECURITY:

THE

POST-COMPUTERISATION INFOTHREAT

BY

OHWOBETE, JAKPOLOHO A.O
PGD/MCS/090

DEPARTMENT OF MATHS/COMPUTER SCIENCE
FEDERAL UNIVERSITY OF TECHNOLOGY
MINNA

MARCH, 1994

COMPUTER CRIME AND SECURITY:

THE

POST-COMPUTERISATION INFOTHREAT

BY

OHWOBETE, JAKPOLOHO A.O

(B.Sc (HONS) ACCOUNTING)

BEING A PROJECT SUBMITTED TO THE DEPARTMENT OF MATHEMATICS/STATISTICS/
COMPUTER SCINCE IN PARTIAL FULFILMENT OF THE REQUIREMENTS
FOR THE AWARD OF THE POST-GRADUATE DIPLOMA IN COMPUTER SCIENCE
OF THE FEDERAL UNIVERSITY OF TECHNOLOGY, MINNA, NIGER STATE,
NIGERIA.

MARCH, 1994

CERTIFICATION

We, the undersigned, certify that we approve the following research essay as adequate in scope and quality for the partial fulfilment of the Post-Graduate Diploma in Computers Science and Mathematics.

---------------------------- ------------------

R. O. BADAMOSI DATE

SUPERVISOR

---------------------------- ------------------

DR. K. R. ADEBOYE DATE

HEAD OF DEPARTMENT

21/4/94

EXTERNAL EXAMINER

DEDICATIONS: (1)

OVERTHERE

TO MY MAKER, the Almighty God, who has, is, and will always be the Captain of my FATE throughout my earthly sojourn, I say here is another one for you. It is dedicated to you 'Cause you CAUSED it to happen - as before. And once again, as before, I say:

> For like a child sent with a fluttering light
> To feel his way along a gusty night
> Man walks the world; again and yet again
> The lamp shall by fit of Passion be slain
> But shall not HE Who sent him from the Door
> Relight the lamp once more and yet once more?
>
> Farid-Uddin Attair
> (Bird parliament)

DEDICATIONS: II

OVERHERE

Mrs R.B.O. Ndanusa nee Makanjuola, here is to you since you made it to be when they thought it won't be, that you will not allow it. Well, as they have found out, you allowed it for the whole duration, and what is more, wholeheartedly too. So what words of dedication would convey the deepest appreciation felt by Me, Myself and I to you, this God-sent Employer of the Century? NONE. Again and yet Again We say NONE.

So here is to you my dearest Madam (how is Abi?):

Iron breaks stone
Fire melts Iron
Water extinguishes fire
The cloud consumes water
The storm dispels clouds
The man withstands storm
Fear conquers man
Wine banishes fear
Sleep overcomes wine
And Death is the Master of sleep
But **CHARITY** saves even from death
WHAT YOU GIVE YOU GET

I thank the two of you. Indiscriminate generosity I would say. All the lecturers I went through. You all contributed immensely to make the programme and the project a resounding success. Thanks to you all. To all my Classmates. You were all too good to Mr. Brown. I I doubt if I will ever have it this good any where else. Especially, I thank my very good friend and protector, Miss U.K. She patiently put up with all my pranks and mercurial dispositions while ensuring that I never for a minute forget why I was here. Any wonder I call her my mother? Lest I forget, Roseline Unueroh should also be thanked. She resolutely bore all the insinuations and other bitter jokes from all and sundry - all because of Mr. Brown. I thank you, Roseline, for being a Sister.

On the home front, special regards to the following people who have made it quite pleasant and easy going to me:

Violet Dioru
Mrs P. A. Isenmila
Kolawole Ojo
Musa Mayaki
J.A. Omodojo
Alhaji Anache.

For going through this horrible handwriting of mine and ensuring that I do not ask her before doing it, my second vote of thanks goes to Miss Ruth Ehigboria, my colleague in the office. If you can decode this, then this is to you: Vale et me ama.

To myself, after my family, I congratulate myself once more with these few line from BYRON:

Here is a sigh for those who love me
And a smile for those who hate
And whatever sky is above me
every fate.

TABLE OF CONTENTS

ABSTRACT

The past few years have witnessed great advances in information technology. These world-wide technological advances in the areas of business and personal computers, the fast and sometimes, incredibly increasing extent of storage and processing capabilities, the miniaturisation of computer chips installed in industrial products, the blending of information-processing and new information communication technologies, as well as the on going researches in the field of artificial intelligence (AI), have led to what is now collectively referred to as the information age. The end product of this is the total and in some cases, partial computerisation of operations in most companies, Government departments and the Military. Truly, we are now in the turn of the information age where computers are now used extensively to administer monetary transactions, prepare balance sheets and other accounts control production, hold confidential information and direct air control and defence systems.

Analogous to these technological advancements and consequent dependence on computers is the emergence of a new problem - the problem of computer-related crime and data insecurity. At the base level, it is not computers that commit crimes or make data insecure; it is the people using them. Surveys have shown that people in the information processing field give little priority to security and more to getting systems up-and-running, meeting programming deadlines and keeping up-to-date with the rapidity changing

technology. The end result of this is vulnerability to criminal-minded elements who can communicate with the computer.

Computer related crime is a threat, the dimensions and full implications of which are not fully recognised and properly addressed at the moment. it is a threat not only to individual companies and other business entities but to the economy as a whole. It is also a threat to the security of a nation. This threat should be of major concern to all those in the information processing field. Unfortunately, this is not the case now. This is the reason for this project. Why are we all in a haste to get "computerised" without making adequate provisions for the security of the systems?

This project is directed at achieving the following purposes amongst others:

1) Identification of Computer Crime
2) The emergence of this new threat
3) The level, impact and prospects of Computer Crime
4) The legal dimensions of Computer Crime
5) The prospects of prosecution of Computer Crime
6) Security measures of Computer users.

However, the project has pointed out clearly that no system is really secured; security of a system is only as reliable as the current level of technology and staff integrity can permit. This is not to suggest that the computer criminal and hackers can not be given a really tough time in their bid to break into a system.

CHAPTER 1

INTRODUCTION

1.1 PREAMBLE

The world is currently witnessing a new and highly sophisticated revolution. This revolution has nothing to do with wars and the conquering of recalcitrant and belligerent nations - even though it helps to decide that effectively - but everything to do with how the information for our daily transactions is captured, processed, stored and retrieved for use. It is the computer revolution. This has led to what is now known as the information age, an age in which "computerisation" has become the watchword the world over. From the Military to the highly complex multinational-Corporation and the smallest office, the computer is now regarded as an indispensable office equipment, so much so that it now ranks at par with the telephone as a yardstick for measuring the seriousness and sophistication of a business entity in some less developed countries. Computers are now used extensively to administer monetary transactions, prepare balance sheets and other accounts, control production, hold confidential information and direct air control and defence systems for precision bombing (remember the smart bombs and patriot missiles?).

Analogous to these technological advancements and consequent dependence on computers is the emergence of a new problem - that of computer-related crime and data insecurity. Very few people talk about computer and data processing security, but lamentably fewer still, do anything about it. The result of this is the rising wave of computer crime in the advanced world. This phenomenon is now assuming a threatening dimension in the developing countries to which Nigeria belongs. A crime has been defined as an offence for which there is severe punishment by law. According to a definition worked out by a group of experts invited by the OECD to Paris in May 1983, the term Computer Crime (or 'Computer-related Crime') is defined as any illegal, unethical or unauthorised behaviour involving automatic data processing and/or transmission of data. This project has used this classic and broad definition of the OECD as a working hypothesis to provide an analysis of the main problems surrounding the new phenomenon. It examines the impact and future development of computer offences. It has also followed this up by showing how the legislature, the business community, and the law enforcement agencies have so far dealt with these problems as well as proffering control measures which ought to be taken to safeguard computer security. The belief is that the more people are aware of how vulnerable and susceptible to computer crime they are, the more security conscious they will become and hence, the more security precautionary measures they will adopt in the new information age. It is one thing to become "fully computerised" and quite another to maintain the integrity of the data so that a business can withstand the assault of the computer criminal.

1.2 STATEMENT OF THE PROBLEM

Everybody is talking about acquiring a computer and becoming fully computerate. Hardly a day passes without some management board deciding on how soon the operations of the company or production department will be computerised. More, and increasingly more, of the activities of Social Clubs, Government Departments, School records, Military Operations, Company affairs and, here we come, household budgetary allocations, are being computerised. The big question however is whether those yearning for, and already using the computer, ever care to find out how easily and vulnerably so, the computer criminal can break into their supposedly invincible computer to commit whatever crime catches his fancy.

This project therefore seeks to analyse the phenomenon of computer crime and the effective counter measures available to check it. It also tries to examine how far the government has devised measures to check the activities of the computer criminal and how an entity or individual can determine its or his degree of exposure to computer crime.

1.3 OBJECTIVE OF THE STUDY

Any research study undertaken is specifically geared towards achieving certain objectives. The following are the modest objectives of this research effort:

1) To examine the phenomenon of computer crime, the various dimensions to it and how this has emerged through the evolutionary process of the new information age.

2) To objectively analyse how far this phenomenon of computer crime has spread its tentacles, its effect to the information processing sub-sector of the world economy and likely trend of computer crime in the future.

3) To undertake an international comparative analysis of legal provisions of various countries to combat computer-related crimes and the problems and possibilities of prosecuting computer criminals.

4) To analyse computer security and detective measures which can be applied to tackle computer-related assaults and also show other preventive, anti-preventive and anti-anti-preventive techniques to beat the computer criminal and hacker in their own game.

1.4 RELEVANCE OF THE STUDY

1) It is hoped that the study when completed will assist the information processing community in their operations and enable them to take adequate security measures to guide against losses and intruders.

2) The study when completed will identify the various security factors involved in computerisation and as a result, enable software engineers and data processing managers to incorporate security-threat counter-measures into their systems.

3) It is also the ambition of this project to enlighten all computer users more on security related issues which have more often than not, been taken for granted or outrightly overlooked in their bid to get their systems up and running.

4) It is hoped that this study will provide a base for other researchers who might want to conduct further researches into the area of computer crime and security.

5) Lastly, but not the least, it is also hoped that this study would be of empirical relevance to other sectors of the business community that may wish to adopt the security measures to suit their specific objectives.

1.5 METHOD OF STUDY

The work presented in this study is based on the following:

- A review of research efforts already carried out in the past by different Authors in the area of computer crime and security.

- A critical examination of the provisions of the law in relation to computer crime in the statute books of six advanced countries and Nigeria.

- Interview of some data processing managers and information processing technologists in various sectors of the Nigerian economy.

1.6 SCOPE AND LIMITATION

Scanty availability of the relevant books for information in the area of security and computer crime and inaccessibility of governmental statutes narrowed the scope of this work. Also, most DP Managers (of the few available) interviewed were not forthcoming in discussing cases of fraudulent tamperings with their DP equipment for fear of adverse publicity. This greatly hindered the result of the study.

Financial and time constraints experiencd as a result of the need to incorporate current information applicable to Nigeria also helped in no small measure to scale down the scope of this study.

Nevertheless, the study will be of relevance to all of us in the secret world of bytes and bits who can find the time (and copy of this work I hope) to read.

CHAPTER 2

LITERATURE REVIEW: COMPUTERS - A HISTORICAL EVOLUTION

2.1 IN THE BEGINNING

From time immemorial, the human being has deviced means to assist him in calculating and processing data. Such devices were usually peculiar to the level of technology that have been attained and can be classified into the following three groups (lipschutz, 1987):

Manual-mechanical device
Electromechanical device
Electronic device.

The manual/mechanical device is a simple mechanism powered by hand. The Abacus and Slide Rule are examples of this type. The electromechanical device is usually powered by an electric motor and uses switches and relays of the type found in most household appliances. The Desk calculator and Punched Card data processing equipment are examples of this type. The electronic device, represented by the modern computer has as its principal components transistors, printed circuits and the like.

The earliest data processing equipment were all manual-mechanical devices. The era when these mechanisms were used can be exclusively referred to as the Dark Ages of data processing (lipschutz, 1987) and dated from 5000BC - 1890 AD. The following mechines were used in the dark ages:-

Abacus (C.5000 B.C)

Napier's Bones (1617)

Oughtred's Slide Rule (C.1632)

Pascal's Calculator (1642)

Jacquard's 100m (1801)

Babbage's Difference Engine (1832)

Babbage's Analytical Engine (1833).

The Abacus which is a frame with beads strung of wires or rods is said to have been developed in the far east of China where it is still widely used. Arithmetic calculations are done by deft manipulation of the beads. The Abacus was followed by Napier's Bones. This was a device invented by a Scottish Mathematician called John Napier. Napier's "bones" are a set of eleven rods with numbers marked on them in such a way that by simply placing the rods side by side, products and quotients of large numbers can be obtained.

It should perhaps be pointed out that Napier is best known for the invention of logarithms, that eventually led to the slide rule. The slide rule though appearing in various forms in Europe during the seventeenth century, was invented by the English Mathematician, William Oughtred. It consists of two movable rulers placed side by side, each of which is marked off in such a way that the actual distances from the beginning of the ruler are proportional to the logarithms of the numbers printed on the ruler. By simply sliding the rulers, multiplications and divisions were easily achieved. What may be rightly considered the first adding machine was invented by the French Mathematician, Blaise Pascal, at age 19; called Pascal's Calculator, the device registered numbers by rotating a cogwheel gear by one to ten steps, with a carry-over rachet to operate the next-higher-digit wheel when the given cogwheel exceeded ten units. The automobile odometre is an example of a device that still uses a series of cogwheels to calculate data. It would be uncharitable to call Pascal a lazy man, but he invented his calculator primarily to dodge the tedious manual calculations that were his father's job when he operated a tax-collection office.

If it was thought that only Mathematicians contributed to the development of information processing equipment during the dark age, the invention of the punched-card machine in 1801 by Joseph Marie Jacquard a French weaver, has disproved this. Simply called Jacquard's loom, the pattern woven by the loom was determined by the placement of holes in a control card as only those threads whose guiding hook encountered a hole in the card could enter the pattern. His loom somehow aided Charles Babbage in conceptualising Babbage's Difference Engine.

Charles Babbage is credited as the first pioneer in the development of modern computer machinery, even though his machine never worked during his lifetime. His Mechanical Difference Engine and his Analytical Engine took advantage of techniques used by Joseph

Jacquard to control patterns produced by looms. Only a part of the Difference Engine was ever constructed. It was based on the principle that, for certain formulas, the difference between certain values is constant. The Analytical Engine followed the difference engine with a much deeper and more general conception. Even though the machine was not realized, owing to the limited technology of the time, it is said that it would have contained many features of present-day computers, including punched-card input, storage unit, arithmetic unit, printing unit, and control by a sequential program (Brightman, 1986).

We now come to what is commonly referred to as the middle ages of data processing. This period dates from 1890 - 1944 and was said to have begun when Dr Herman Hollerith, a statistician with the U.S. Bureau of the Census, completed a set of machines to help process the results of the 1890 Census. Using 3 by 5 inch punched cards to record the data, he constructed a box to sort the data and a manually fed electromagnetic counting machine to tabulate the data. The 1890 Census was processed in one-fourth the time needed for the 1880 Census. It should be mentioned in passing that Dr. Hollerith left the Census Bureau to build and sell his own tabulating machines. His company metamorphosed into the gigantic IBM.

In 1908, Powers patented a 20-column punching machine. In the same year, Hollerith developed a vertical sorting machine which processed almost 200 cards per minute. By this time, the speed and capabilities of punched card machines continued to improve. Verifiers were invented to check that the right data were entered into the cards. Collators were also invented to merge several sorted decks of cards into a single sorted deck. Electromechanical accounting machines were developed which could read cards containing both alphabetical and numerical data, perform simple arithmetic operations and print the results. This led to the modern age of data processing and information technology which can be said to have started in 1944 by the production of Mark I.

The Mark I was the brainchild of Howard G. Aiken, a Professor of Applied Mathematics at Harvard University. Built by IBM, it was an electromechanical (relay) device, like the calculators which preceded it and was capable of automatically performing a long sequence of arithmetical and logical operations. Mark I was followed by other four Marks; Mark II through V. The series of Marks ushered in what is commonly referred to as the computer generations.

2.2 THE COMPUTER GENERATIONS

The term computer generation is employed to indicate to which technological generation a computer belongs. By this, computers are usually classified into the followings:-

Ist Generation
2nd Generation
3rd Generation
4th Generation

2.2.1

FIRST GENERATION COMPUTERS (1946 - 1959)

The first generation computers utilized vacuum tube components. The first large-scale vacuum-tube computer was the ENIAC (Electronic Numerical Integrator and Calculator) and was completed in 1946 by John Mauchly and Presper Eckert at the Moore School of Electrical Engineering at the Unverisity of Pennsylvania. It would accomplish in one day what previous computers took 30 days to perform. Like babbage's Difference Engine, part of the motivation for the ENIAC was the need to construct tables automatically - in this case, ballistic tables for U.S. Army Ordinance Department which funded the project. Work on the ENIAC began in 1943 and it was completed in 1946. It was an enormous machine weighing 30 tons and containing over 18,000 VACUUM TUBES. While the Mark I required about 3 seconds to perform a 10-digit multiplication, the ENIAC required only 3 microseconds.

The first generation also witnessed the first computer to use the stored-program concept which had been developed in the mid-1940s by the famous Mathematician, John Von Newmann in collaboration with H H Goldstine and A.W. Burks. It was called the EDSAC (Electronic Delayed Storage Automatic Computers) and was completed in 1949 at Cambridge university in England. The first American Computer to have the stored-program (also in the first generation) was the EDVAC which stands for Electric Discrete Variable Automatic Computer - also built at the

Moore School and completed in 1952. Another famous first generation computer is the UNIVAC I which became operational in 1951 and was run 24 hours a day until 1963. It is fondly remembered for having predicted the victory of Dwight D Elsenhower in 1952, during the Presidential election husslings in the United States.

2.2.2

SECOND GENERATION COMPUTERS (1959 - 1965)

The so-called second generation computers can be taken to be those produced during the second decade of the electonic computer era; there is no general agreement about the exact period involved. Denning in Computer Survey (Dec. 1971) defines 1950 to 1960 as the second-generation period, while Bell and Newell in Computer Structures: Readings and Examples (1971) suggest 1958 through 1966. We however note that it is mainly characterised by the change from vacuum tube to transistor technology. Other important developments also occurred which are summarised below:

1) The transistor, which had been invented in 1948 at Bell Telephone Laboratories, gradually replaced vacuum tubes in the design of switching circuits.

2) Cathode-ray-tube memories and delay-line memories were replaced by ferrite cores and magnetic drums as the technologies used in main memories.

3) The use of index registers and floating-point arithmetic hardware became widespread.

4) Machine independent "high-level" Programming Languages such as ALGOL, COBOL, and FORTRAIN were introduced to simplify programming.

5) Special Processors (IO Processors) were introduced to supervise input-output operations, thus freeing the CPU from many time-consuming house-keeping functions.

6) Computer manufacturers began to provide systems software such as compilers, subroutine libraries, and batch monitors.

The most popular second-generation computer was the IBM 1401, of which some 15,000 were manufactured.

2.2.3

THIRD GENERATION COMPUTERS (1965 - 1970)

The year 1965 may be considered as marking the beginning of the third generation computers, but the distinction between the second and third generations is not very clear-cut. The following developments are frequently singled out as salient features of the third generation.

1) Integrated circuits began to replace the discrete transistor circuits used in second generation machines, resulting in a substantial reduction in physical size.

2) Semiconductor (IC) memories began to augment, and ultimately replaced, ferrite cores in main-memory designs.

3) A technique called microprogramming came into widespread use to simplify the design of processors and increase their flexibility.

4) A variety of techniques for concurrent or parallel processing were introduced such as pipelining, multiprogramming, and multiprocessing. The objective of all this was to increase the effective speed at which a set of programs could be executed.

5) Methods for automatic sharing of the facilities or resources of a computer system, e.g., its processors and memory space, were developed. These were intended to improve resource utilisation, particularly the use of memory space.

Popular third-generation computers include the IBM system/360 series and GE 600 series.

2.2.4

FOURTH GENERATION COMPUTERS (SINCE 1970)

The fourth generation could be considered to have come into existence since the early 1970s with the introduction of systems-network architecture, whereby a standard network was derived which allowed networks of computers to be upgraded without alterations of programs. This generation also includes microcomputers, retail terminals, databases and extremely large internal and external storage capacities. This generation marked the introduction of very large scale integration (VLSI). Major innovations of the fourth generation computers are listed below:

1) Large computers that are much faster, much less expensive, and of much greater data processing capacity than equivalent-sized third-generation computers.

2) A multitude of relatively inexpensive mini-computers (actually first introduced in the third generation).

3) Even further miniaturised computers popularly called microcomputers.

Among the advanced input/output devices employed in fourth-generation computers are optical readers, by which whole documents can be fed into the computer; audio response terminals, by which an operator can vocally introduce data or instructions; and graphic display terminals, by which an operator can feed pictures into the computer.

It is expected that a new generation, the fifth, with computers having advanced features such as expert systems and artificial intelligence will be categorised into the computer evolution lexicon in the not too distant future.

2.3 COMPUTERS AND THE INFORMATION SOCIETY

The information revolution which is a combination of massive increases in the world's inventory of information and the technical development of the means to cope with it - including the computers - will one way or the other affect every segment of our lives. For most of us, participation in the technical aspects of the information society means using a telephone, radio set and a microcomputers. To be sure too, others will be employed in the information processing and communications field as programmers, technicians and analysts. Computers have now become an everyday phenomenon in our lives. All of us, the users of information services and computers, will somehow use personal computer resources on our jobs and in our homes. Computers now dictate how information is acquired, stored, processed and presented for consumption. To the business world, the advent of the desk-top computer and its ability to retrieve needed information from many diverse sources promises a huge increase in productivity of decision makers. The advantages offered by computer resources have been described in Business Week (Nov. 1983) as follows:

1) Individual Managers can now make decisions by combining information developed within their companies with outside databases, including economic and industry statistics. This allows them to assemble studies of markets, competition, pricing, and forecasts in hours rather than months.

2) Electronic mail allows reports, memos and other correspondence to be transmitted simultaneously to many people within the company as well as outside of it.

3) New systems can turn reams of numbers into charts and colourful graphs thereby enabling information to be more quickly digested for faster action.

4) Voice store-and-forward telephone systems let users send phone messages digitally by computer to any number of recipients within the company.

5) Computerised scheduling systems make it possible to set dates for large meetings without consulting executives individually.

In these and other capacities, computers are appearing everywhere in the office. Computers are increasingly being used outside of the work-place too. Within the next decade, it is projected (Brightman, 1986) that most homes of even modest means will have a computer that can easily be connected to the same information sources used by professional researchers, scholars, and commentators. Then the true information society will have arrived.

2.4 USES AND ABUSES OF COMPUTERS

The computer has now become a very useful tool for the handling of hitherto tedious and sometimes repetitive tasks. Uses of the computer can be conveniently categorised into the following headings:

1) **In the Computing Industry**

Computers are now being used in producing computers. Advances in artificial intelligence has greatly helped in ensuring that computers aided manufacture (CAM) also applies to the computer industry itself.

2) **In the Automotive Industry**

Assembly line activities that were manually handled are now being conveniently done with the aid of computers. It is now possible for the whole car manufacturing process right from the design stage to the assembly line to be handled by computerised robots without a single human intervention.

3) **In Weather Forecasting**

The weather is said to change every 12 minutes and this must be calculated simultaneously for the whole world if any measure of accuracy is to be achieved. The super-computers like IBM G9 are designed for just this purpose to enable accurate forecasts to be made.

4) **In the Aviation Industry**

Computers are now used in designing and testing all aircrafts. In the training of future pilots, the computers' flight simulators have greatly assisted in this direction. Air control procedures have also greatly benefited from the computer revolution.

5) **In the field of communications**

Facsimile communication is an advance in communication technology that has been made possible with the help of computers. Digital advances have also ensured Sattelite Link-ups and automatic transaction of dialogue.

Other areas of human endeavours in which the usage of the computer has become inevitable are:

In the Banking Sector

Space Research

Games, Televisions

Medicine

Police and Criminal investigations.

"The desktop revolution has brought tools that only professionals have had into the hands of the public. Only God knows what will happen now" were the words of Marvin Minsky of MIT in A new world Dawns (Times, 3rd Jan. 1983). Because information can be available to anyone with access to a computer and the necessary data transfer equipment, possibilities for misuse arise. Two dangers, real and threatening, that have been brought about by the rise of the computer have been identified (Brightman, 1983):

Computer Crime

Abuse of privacy.

These days, news reports frequently describe illegal electronic break-ins of computers and data banks. Indeed, computer crime has become the most feared variety of white collar crime. In 1983, an employee of the Wells Fargo Bank used its computer to embezzle 21 U.S million dollars. Most alarming, detected computer crimes are just the tip of the iceberg as most business organisations detest the negative publicity that follows any successful computer break-in. It has been estimated by the U.S. Chamber of Commerce that detected computer crime alone costs the American business community more than U.S. $100 million a year (Brightman, 1983). Not all computer crimes involves stealing. Some computer enthusiasts, called hackers need no more motive than the love of challenge to break into computer systems and data banks, either to damage them or simply to explore them. Increasingly, statutes that outlaw the "intentional accessing to defraud, extort or obtain money, property, or services with fraudulent intent or malicious accessing, alterations or deletion, or a malicious accessing for a credit rating" are been enacted in most countries where the information revolution has caught on.

In addition to computer crime, many people fear that the legal use of data banks threatens to violate individual privacy. Potential targets for abuse include data banks containing information about consumer credit, legal political activity, financial holdings. Abuse of the computer is inevitable. Given a little ingenuity, almost anyone can find out what everyone else is doing or has done, if not in one place then in another. Computer security ensures that exposure to computer crime and abuse is greatly curtailed.

2.5 **LOOKING AHEAD: COMPUTERS IN THE FUTURE**

Predicting the future these days is a risky business. The information revolution is moving so quickly that gazing into the crystal ball can actually endanger one's credibility. When the first large scale computer was built in 1944, the chief designer of the machine, Mr Howard Aiken, thought and then predicted that only 5 computer machines would satisfy the computer requirements of the world. As we have now known, Aiken's prediction was somehow foolish. For another example, early in 1984, David Winer, President of the Software firm, Living Videotext, described his ideal portable computer. It would take three years to develop, weigh as much as twenty-five pounds, and cost upwards of $5,000 BYTE (PYTE, Jan. 1984). Eleven months later, Data General Corporation introduced a portable computer, the Data General/one, that surpassed all of Winer's specifications. It weighed in at ten pounds, fit easily in a briefcase and sold for U.S. $2,895 (BYTE, Nov. 1984).

Seeing where we are going, historians tell us, requires that we know where we have been - forecasts of the future must be based on the past. In the future, we will see the dreams of the computer pioneers fulfilled as computers evolve the ability to "learn" from their own experiences. Further advances in the field of artificial intelligence will make this a distinct possibility.

The cost of computing and computers will be much lower five years from now. This is reminiscent of the small calculators which now cost less than a tenth of their market entry cost in the early 1970s.

Computers will become increasingly available so that, by the turn of the century, they will be as common-place as the telephone.

By the turn of the century too, computers will program themselves. The user will enter the specifications for a job to be done, and the computer will write its own program to do it. We expect program generators - programs that write other programs - to have been perfected to a level that will enable the lay-person to develop specialised programs to satisfy his unique needs.

It is also expected that the large number of proprietary data banks that serve the public today will consolidate into an information utility, much like the telephone system.

CHAPTER 3

COMPUTER CRIME: A NEW INFOTHREAT

3.0 INTRODUCTION

One of the by-products of the phenomenal increase in electronic data processing system via the computer is the increasing wave and growing sophistication of computer crime. Modern administration relies on computer technology and databanks for efficient and smooth operations. The triumphant march of computer applications not only has an advantageous side but also leads to the crucial importance of the operation and security of computer systems for business and the society. In the business community, for example, the majority of monetary transactions is administered by computers in the form of deposit money. Balance sheets are prepared with computer support. A company's entire production is frequently dependent on the functional ability of its data-processing (DP) system. Furthermore, many businesses store their most important company secret~~e~~s in a computer. Modern administration relies on computer technology in a similar way. Sea, air and space-control systems, medical supervision as well as defence also depend in a large extent on modern computer technology (Sieber, 1985). *

As a result of this seemingly wholesale dependence on computer technology, the increasing level of criminal offences involving DP systems registered over the last decade in western advanced societies and now, in developing economies, represent a threat to individual companies as well as to a country's economy and society as a whole. This danger has been increasingly recognised in recent years and has led to national and international concern about the new threat which is called 'Computer Crime'.

3.1 WHAT IS COMPUTER CRIME?

A problem which often arises when the need to have a working definition of a subject becomes imperative is that of identifying what is encompassed within the subject-matter and then attempting a definition based on this delineation. The subject of computer crime is all encompassing. It involves the following (Carrol, 1987):

Loss of EDP Equipment and facilities
Denial of service
Improper Disclosure of Information
Improper Disclosure of Information
Improper Modification of Information
Loss of Data, Software, and Supplies
Improper Disclosure of Software
Improper Modification of Software
Improper Creation of Negotiables.

According to a definition worked out by a group of experts invited by the OECD to Paris in May 1983, the term Computer-Crime, or its modified version, Computer-related crime, is defined as "any illegal, or un-authorised behaviour involving automatic data-processing and/or transmission of data". This definition is all encompassing as it permits the use of the same working hypothesis for all kinds of criminological, criminalistic, economic, preventive, or legal studies. However, John M Carrol in his book, "Computer Security" defines computer crime as "all threats directed against electronic data processing (EDP) equipment and its supporting facilities (Hardware), programs and operating systems (software), supplies, information handled by the EDP system, negotiable instruments stored or created at the facility, and critical resources required by the EDP system to render services". An obvious shortcoming of this definition is its non-recognition of threats directed against data processing personnel, users of the processed data and others who may be subject to blackmail by the computer criminal (the humanware). As a result, the OECD definition is accepted as a standard definition for Computer-crime (Sieber, 1986) and forms the basis of most work on the subject of computer-crime.

3.2 COMPUTER-CRIME: ARE YOU VULNERABLE?

An EEC-sponsored investigation by the consultancy firm of Arthur Young in 1981 revealed two important facts about vulnerability to computer criminal attacks. The first was that most management do not know what level of losses their businesses could sustain and still survive. Secondly, computer security is usually felt to be the sole responsibility of the Data Processing Manager. A cause for concern arising from the second point is that Data Processing Managers, where there is any, give very little priority to security.

On the contrary, their prime concern centres on getting the system up-and-running, meeting programming deadlines, staff turnover problems and keeping up-to-date with the rapidly changing technology. Vulnerability is usually classified into the following and is related to the possibility of attack:

Resources Sharing Systems
Microcomputers
Human beings

The probability of attack on the other hand may be classified according to the quality assaulted, such as confidentiality, integrity, or availability; and by the material under siege, which may be data or property. actions of this nature may be launched by non-employees or employees, or may be accidental, which may be acts of God. The attack by a person or group in turn may be unintended or malicious and in the latter case may be either surreptitious or overt. The probability of computer criminal assault determines how vulnerable a system or person is and in effect what security measure will be taken as counterattack.

The Principal points of vulnerability in resource-sharing data systems are processors, storage devices, communications facilities, remote terminals, users, and systems personnel. The hardware of the central processor is vulnerable to failure of protection circuits, confounding of bounds and relocation registers, and misuse of privileged instructions. The software of the central processor is vulnerable to by passing of file protection and access control programs or falsification of user identification.

Storage devices are vulnerable to unauthorised copying of stored information and theft of removable EDP media and to hardware or software failure that could result in compromise. Communication facilities can be compromised by undesired signal data emanations, cross-talk between secure and unsecure circuits, and the insinuation of technical surveillance devices. Resource-sharing devices are also susceptible to users who may mispresent or forge their identification or authorisation, may seek un-authorised access to sensitive material by browsing and can use debugging procedures to circumvent security mechanisms. Remote terminals are vulnerable to technical surveillance devices and can produce potentially compromising text in the form of hard copies. System personnel who have normal access to supervisor programs, core dumps and files stored on removable EDP media could constitute security risk if they are not loyal and reliable.

The Microcomputer has now become a common phenomenon in homes and offices. Microcomputers can, with the appropriate devices, communicate with large main frame computers. They can neither identify themselves nor the people who use them. They store data on diskettes, and sometimes, hard disks. Anybody who can physically approach a microcomputer can steal any of the data in it or even the machine itself. The determined person can also copy files residing in any mainframe computer with which the mico can communicate onto floppy diskettes and steal that information as well.

The vulnerability of human beings to computer-crime is well illustrated by the following story 2:-

April 5, 1976

Twelve persons at Brooklyn College were implicated in a grade-switching conspiracy. All were present or past employees of the College. A total of sixty-four charges were made in thirteen students' records. The scheme was revealed when a Professor denied ever giving a certain student the grade shown on his transcript. The altered transcripts belonged either to the conspirators, their friends, or relatives.

It should be noted that this attack can be very easily carried out as all that is required to make the alterations is access to the terminal, knowledge of the procedure and the students' numbers.

In summary, the following groups are vulnerable to computer-criminal attack:

The Computer Hardware component
The Computer Software component
The Humanware interface

3.3 DIMENSIONS IN COMPUTER CRIME

The subject of computer crime has gone hand in hand with the technological development of computer systems. Security measures have not kept pace with the potential for fraud and penetration. Even the law has not been effective in this areas as most of the laws dealing with fraud require specific evidence in the form of false documents or changes in records that can be introduced as evidence in a Court of Law.

Computer crimes are often simple schemes that do not require technical knowledge of complex systems to achieve their fraudulent objectives. Computer frauds tend to be large in amount and are often methods discovered by accident when using the computer system in a legitimate manner for other purposes.

Computer crimes fall generally into two types, either abstraction of assets or penetration of the computer for illegal purposes. These two types of crimes can be further categorised into three main groups which have fallen within the OECD definition of computer-crime. These are as follows:

a) Computer-related economic crimes such as computer fraud, computer espionage, and computer sabotage.

b) Computer-related offences against personal rights especially against the citizens' right to privacy

c) Computer-related offences against super-individual interests under which can be classified offences against national security, control of transborder data flow, integrity of computer-based procedures and data communication networks.

3.3.1

THE ECONOMIC DIMENSION

A principal motivating reason for committing crime is the desire for money. Some people find that they like the high life style and need money for it to continue. A sudden need for extra funds in the case of personal problems at home or marital difficulties, alcoholism, or drug use may cause an otherwise model employee to steal from the company. Again, most employees who are terminated for good and sufficient reason are hostile to the company for some time after. In all the instances mentioned above, the computer offers an easy way out for them.

Computer-related economic crimes constitute the main field of computer crime up to the present day. Excluding accidental and negligent damage to computer systems, six main categories of computer-related economic crimes have been developed. These are 3:

1) Fraud by computer manipulations against EDP systems

2) Computer espionage and software theft

3) Computer sabotage

4) Theft of services

5) Unauthorised access to EDP systems

6) Traditional business offences assisted by EDP

1) **Fraud by Computer manipulations against EDP systems**

Fraud by EDP systems by computer manipulation involves the changing of data or information for purposes of financial gain. This is usually targeted at data representing assets in the system such as deposit money, claims, working time, credit ratings, and results of calculations of balances. Up to the present, the cases known are primarily manipulations concerning salaries, invoices, pensions, and, in the advanced countries, social security payments as well as manipulations of the account balances of bank balance. Projections are that the increasing replacement of cash money by deposit money means that this field of computer crime will also be the main area of computer fraud in the future. This is illustrated by the case of Mark Rifkin. In 1978, he fraudulently managed to get $10.2 million dollars transferred from the Security Pacific National bank in Los Angeles to a New York bank by means of a telephone call. In some cases, the data being the object of computer fraud represent tangible and corporeal objects which are taken away by the perpetrator after the manipulation of the computer system. This concerns cash money, materials, merchandise or goods. These classic objects of crime generally result in smaller losses than manipulations of intangibles, since the losses here are limited by the actual amount of goods available.

In 1984, two Germans, a programmer and a stock clerk, altered the program and the databases of a spare-parts store's computer so that spare-parts taken away by them were invoiced at very low prices. The losses here amounted to DM31,000.

A specific group of computer crime cases primarily concerning tangible cash money, goods, and services registered by computer systems has now been made possible by the increasing number of cash dispensers installed by banks and by electronic high-efficiency vending machines equipped with electronic sensors. Cases of crimes directed against these objects are especially rampant in Japan where uptill December 1982, 328 cases in 37 prefectures were reported, of which 181 concerned vending machines; 98, money-changing machines, 43, amusement machines; 4, Pinball machines; and 2, automatic ticket machines. At the end of 1982, 39 of these cases were cleared and 58 people were arrested, of whom 23 were members of organised crime groups. An analysis of the differences between traditional fraud and computer fraud in the field of the objects of crime shows that the assets now represented and manipulated in the EDP systems where the target of traditional fraud long before the computer existed. What is however new about the object of computer manipulations is the fact that the information representing these assets is no longer stored on paper, which is visible and in an easily readable form but in an invisible and machine-readable concentrated form in Electronic storage devices. It is this change from paper-represented assets to paperless-represented assets that is the reason for problems both in the scope and the detection of crime and in the application of existing legislations.

We have observed that information stored in EDP systems is no longer handled by human beings but by computers. Analogous from this, it is seen that the mode of perpetration forms the main difference between traditional fraud and computer fraud. Here, the offender can either feed the computer incorrect data from the beginning, which is known as <u>input manipulations</u>, interfere with the correct processing of the computer through the <u>console, program and hardware manipulation</u> or subsequently falsify the initially correct result given by the computer - a method knows as output manipulation. Input manipulation can be carried out by the adding, omitting, changing, exchanging, or incorrect posting of input. These data-dilly-dallying are usually carried out by clerks, data typists, transaction participants, and operators responsible for the collection, checking, transmission, and input of data to be processed. This is examplified by the case of a DP employee in Zurich who succeeded in manipulating the automatic foreign payments transactions of one of the biggest Swiss banks. He cleverly avoided security measures set up by the bank in order to prevent such manipulations. He had accomplices working in concern. Thus when DM98 were, for example deposited in Frankfort, his accomplices, drawing the money in Lugano and Davos, did not receive 100 Swiss France but N100,000 Swiss France. Similarly, for their 897 deposited in New York, they did not receive 251 but 251,000 Swiss France. The perpetrators made a profit of about 700,000 Swiss France through these manipulations before they were caught, sentenced to prison and later put on probation in 1976 5.

Compared with input manipulations, which in many cases can be carried out without any knowledge of DP, the method of program manipulation is more computer-specific and, above all, much more difficult to discover. These manipulations are committed either by changing the company's existing programs, usually by adding Trojan-horse routines, using special versions of the virus programs or outrightly applying additional programs written by the perpetrators.

Standard Utility Programs which are able to by-pass most security measures (e.g. Superzap Utility) can also be employed to achieve criminal ends. Correct processing of the computer can be subject to crime not only through program manipulations but also by the abuse of mechanical control elements or integrated circuits of the DP system.

The most spectacular case of console or hardware manipulations occurred in West Germany in the mid 1970s and involved concealment of speculative foreign exchange dealings at the Herstatt Bank. It was estimated that amounts totalling several billion US dollars had not been recorded in the accounts or had been falsified. An aspect of this case was the way in which the offenders by-passed a security measure written into the program. In order to avoid improper use, the small computer's program had been designed to print out the word 'interrupt' on the accounting form produced by the computer as soon as the 'interrupt' key was pressed. The perpetrators prevented this error message, which would have necessary led to discovery of the manipulation, by removing the accounting form from the system after it was completed but before the 'interrupt' key was pressed. The word 'interrupt' was therefore not printed on the form but on the empty drum.

The increasing use of remote DP systems in recent years now provide a particularly interesting variation of the manipulation techniques described so far and will be of great significance in the future. Where the computer is connected to remote DP via the public telephone network or other methods of data-communication, the offender can carry out manipulation from his own home, using his own DP terminal and without personally entering the offices of the company affected by the crime. Perpetrators have further improved on complex manipulation techniques into a new method called the 'Salami technique' whereby they take many 'thin slices' of financial transactions which they reckon no one will miss and transferring these amounts to a favoured account 6.

Empirical studies, especially those done in what was still then West Germany indicate that more than 90% of the manipulations detected were committed by employees of the victimized companies. Also, about 60% of the perpetrators detected, especially in the field of input manipulation, did not have the skills in the field of DP and the number of cases involving specialists taking advantage of their superior skills in systems analysis and programming was relatively small 7. The question of whether this is due to the fact that systems analysts and programmers commit fewer crimes than generally assumed or due to the fact that manipulations of these people are especially difficult to detect cannot be answered with certainty.

2) **Computer Espionage and Software theft**

This represents one of the most frequent forms of computer crime. It is quite profitable for the perpetrator just as it is dangerous for the company affected because of the valuable information stored in the computer centres of most companies. The primary targets here are the computer programs, the value of which was estimated in 1985 to be approximately $55 billion US dollars. In the Commercial sector, computer espionage concerns computer-stored cost accounts, balance sheets, and customer addresses. The centre of attraction in the technical sector is development, research, and production data and of course, computer-clip designs, the sales value of which is demonstrated to have netted $17 billion dollars in 1983 and increased by 100% in 1984.

The high concentration of data in electronic memories, especially tapes, disks, and chips and the possibility of using a computer to copy data quickly and unobtrusively are leading to new dimensions of industrial and commercial espionage in this sector.

been exposed. By this method, the radiation and electronic fields generated by computer terminals and electronic typewriters are intercepted, analysed, and recorded from distances up to 3000 feet using standard television and recording equipment which can be obtained reasonably cheaply and easily stored in any car packed near the computer centre. In the field of telecommunication systems, the technique of wiretapping in order to obtain passwords and other secret information from telecommunications and teleprocessing may range from a coil on a drop-wire to the picking up of stray microwaves from satellites or terrestrial stations or penetrations of data-switching computers. Because of the computer's great working speed and its abilities to sort, match, disseminate, and copy information, wiretapping of a computer communication can be much more efficiently organised and is much more dangerous than the traditional wiretapping of an oral communication.

Apart from these acts committed by hackers and from the well-known copying of mass-marketed programs practised by computer-users and software dealers, the theft of software and data is committed primarily by disloyal employees of the victimized company, usually shortly before leaving a job and by licencees in breach of contract. In the defunct Soviet Union, theft of high technology was organised by the State (KGB) and by the Chief Intelligence

Directorate of the Soviet General Staff (GRU). In 1983 for example, 11 containers with computer system (including a Digital VAX 11/782) were consficated in Hamburg and Hallsingborg, Sweden, on a ship bound for the then Soviet Union.

3) **Computer Sabotage**

The high concentration of data stored in the electronic devices coupled with the dependence of many companies on DP ideally make computer sabotage another prime danger for business and administration. Here, the objects of sabotage are the intangible computer facilities as well as the intangible data containing computer programs and other valuable information.

The method of achieving computer sabotage can be differentiated between those that cause physical damage and those that cause logical damage. In the case of causing physical damage, the most frequently practised methods are igniting or bombing a building. These are mostly phenomena experienced in the highly developed world. The most popular method of causing logical damage is through the use of crash programs which can erase large volumes of data within a short period. These programs can be utilily, self-written, or 'Trojan-horse' routines built into application programs or into the operating system. Crash programs can be executed at a later state, after the perpetrator has left the firm. A special variation of this sabotage technique using 'timebombs' is the implementation of cancer-routine. This is made up of a few time-consuming program instructions and a set of commands which cause the self reproduction of the 'cancer-program' in another, arbitrarily chosen, part of the application program during each run. An extremely dangerous form of the cancer-routine are virus-programs.

Virus programs are self-reproducing programs which copy and implement themselves in other programs and data files to which they have access and which are not yet infiltrated, thus spreading through all shared resources. If such programs are implemented in the computer or in other parts of the operating system, or even in free programs offered to system operators on a system's bulletin-board, the virus-program can infiltrate the whole DP system and even complete networks. In teleprocessing systems it is possible to carry out sabotage programs via telecommunication lines from some distance away. Cases involving computer sabotage by remote DP are reported from the United States where a group of 8th-grade-students of the New York Dalton School were able to use their school's training computer to penetrate the databanks of various Canadian companies and the Federal Government and, in some cases, to destroy their data 8. Further techniques to cause logical damage which have been revealed are: erasing data by magnets or degaussers; operating a power-off switch during a production run; putting a plug, chip, or printed circuit motherboard into an incorrect socket; or changing labels, tape numbers, and other data.

Available information reveals that the majority of acts of sabotage recorded up to the present have been committed by angry employees seeking revenge, protesting against rationalisation of their company, or just wishing to retire early. A second group of perpetrators could be said to have emerged from the business community. The aim of computer sabotage committed by companies can be to gain competitive edge over their rivals or to facilitate the take-over of a company. A particularly threatening financial motive in computer sabotage underlies the cases of 'bitnapping', in which computer programs or other data are stolen in order to be used as a means of extortion.

4) **Theft of Services**

The unauthorised use of DP systems, often referred to as theft of services or 'time-theft', is very widespread in the DP Sector. The objects here are the processing, storage, and transmission services of computer hardware and very often also programs and other data, which are used by DP employees for their own purposes. In some cases, time theft, especially if committed by employees, does not cause considerable damage to the company concerned, and represents less of a danger than the offences enumerated so far. A company's interest can however, be severely affected by abuse of remote DP systems (by using the company's account numbers or rented computers for which the actual time of utilisation has to be paid) or when the company loses its services or customers by blockage system or by 'blacking' of the labour or its employees. We end this section by recalling the following:

July 4, 1977. Two Programming Managers for Unival in Philadephia were charged with theft of $144,000 worth of computer time used to revise music into digitised form. They were running their own company using their boss's equipment.

5) **Unauthorised Access to DP Systems and 'Hacking'**

Also known as illegal entry, the usual motivation is the challenge to crack a code (hackito ergo sum); this can be categorised as a special form of 'theft of services'. The hacker has been described as a person usually bright, eager, highly motivated, courageous, adventuresome and qualified, willing to accept a challenge. He has exactly the characteristics that make him highly desirable employee in data processing 9. Hacking activities have especially continued abated, sometimes with vicious intent and damaging results. For example, a 19 year old computer operator working for a chemical research company abused his position of trust by exploiting privilege knowledge obtained in his employ, to hack into a number of ICL installations and to destroy the system's accounting records to cover his tracks. In one spectacular instance, he was alleged to have damaged both live files and all their backup copies on an ICL 2988 computer running under the VME Operating System, and in consequence sabotaged and invalidated the findings of a breast cancer experimental research project. He was also charged with breaking into JANET, the joint academic network which links computers at British Universities, and erased records of his hacking activities from the system log 10.

When some cases of hacking become public, hacking can be useful for the detection of loopholes in computer systems. However, in general, they are dangerous, because data may be destroyed by negligence, system blockades may be caused, and security deficiencies found by acts committed as a challenge may be subsequently used for financial fraud.

6) <u>The Computer as a Tool for Traditional Business offences</u>

In recent years, the possibilities of computer misuse have been increasingly utilised by the management of fraudulently operating companies to commit general business offences at the expense of business partners, consumers, investors, or governmental agencies. The majority of cases discovered up to now involve the manipulation of computer-administered revenues, accounts, balance sheets, stock-taking lists, and tax deductions. The erasing of stock-keeping lists and balance sheets to disguise business offences and to render penal procedures more difficult is also a frequently practised method. This is clearly illustrated in the case of a Teller at New York's Union Duke Savings Bank who was arrested and charged with stealing $1.5 million U.S. dollars from the bank's deposits over a three-year period. He is alleged to have used the bank's computer to shuffle accounts and then to have fed in false information so that the accounts always appeared to be up to date. He was reported to have used his illicit earnings to bet up to $30,000 a day on professional sporting events. The affair came to light in connection with a police gambling raid on a bookmaking establishment. Another well known example of a computer-assisted general business offence is the American Equity Funding case which led to some of the most extensive losses caused by computer manipulations in the United States.

3.3.2

THE INVASION OF PRIVACY DIMENSION

The issue of computer-related abuse of privacy has been the subject of popular discussions and even predates computer-related economic crime. However, because of the small number of severe criminal cases and the dependency of the evaluation of most privacy infringements on a difficult balancing of interests, these cases have been discussed more in terms of public, civil, and sometimes, labour law problems than as a matter of criminal law. Today, in many cases, an evaluation of privacy infringements as 'abusive', illegal; or 'criminal' is still difficult because often a balancing between the rights of an individual to his privacy and the rights of society to information is necessary. This balancing of interests not only causes different evaluations of the legality of the respective acts in various countries but also different concepts of the role which criminal law should play in this matter.

Computer-related infringement of privacy has the following sub-groups which has been identified for ease of analysis:-

1) The production and use of incorrect data

2) The illegal collecting and storing of data

3) The illegal disclosure or misuse of data

4) Infringements of formalities and information rights of privacy laws.

Privacy infringements committed by the use of incorrect data can be further subdivided into 2 distinct types of abuses: the manipulation and erasure of data by unauthorised persons and the collection, storage, processing, or disclosure of incorrect data by their bona-fide holder. As far as incorrect personal data originate from computer manipulations committed by unauthorised persons, both the illegal and the criminal nature of the act are easy to determine. This is also true where the contents of databanks are changed, possibly by the erasure of data. In the second, it is obvious that the collection, processing, or dissemination of incorrect data by its holder is also illegal. Where these acts are deliberately committed, the evaluation of the criminal nature of the act does not raise major problems either.

Privacy and personal rights cannot only be affected by the use of false data but also by the collection and storage of correct data. The abusive character of such acts can either consist of the methods by which the data were gathered or the content of the data. On the techniques to obtain data a variety of acts can be listed which are clearly detrimental infringements of privacy. Included here are such acts as wiretapping, bugging, illegal access to another person's data files by infringement of security measures, etc. An example of these intrusive technique can be gleaned from the case of the 16 year old West German hacker, who, among other acts, programmed 'data tape' which collected the personal identification data of other videotex systems-users. He further manipulated and destroyed the data files of some users, changed the valid passwords of others (who could therefore not longer work with their system), and sent libellous letters by using false sender-identifications.

The other aspect which can render the storage of information illegal is that by which the content of the information is not supposed to be stored. Where there are no legal restraints, the expanded possibilities to collect, process, and transmit large amounts of information could be used to create excessive profiles of individuals, households, or groups of people. We note however, that the obvious question of who is supposed to store what kinds of information is one of the most difficult in privacy protection. This is especially important for credit-reporting systems, police, intelligence and other administrative agencies, personal information systems in the field of labour registration, and registration of private consumption of news media services.

The third group of privacy infringement concerns the illegal disclosure and misuse of data. Here, a distinction can be made between acts that concern personal data and those concerning non-secret personal data. Where there are statutes protecting special secrets, the illegal character of the disclosure of personal data in general is clear. This is especially so in the fields of medicine, banking, etc. To a high degree, this is also true for acts in which data are misused, i.e. where information is legally collected and stored but used for a purpose other than that for which the data were obtained. The threat to privacy in the field of information is clearly illustrated by an Austrian case in which a Police officer of the Federal Police of Vienna had, from 1961 to 1978, given to a private detective data from the register of criminal records, the register of persons, the file of police searches, and Interpol files. The police officer was sentenced on account of breach of secrecy by a public servant. In the area of non-secret personal data, it is difficult to decide whether the disclosure and use of personal data is detrimental to society and should be called abusive, illegal, or criminal. This is especially true in the case of information-exchanges between various government agencies or between credit-reporting agencies and their clients. The issue of whether computer matching by government agencies violates the constitutional right of privacy was thoroughly addressed in the case of Jaffese V Secretary of Health, Education and. Here, a list of persons receiving veteran's disability benefits was matched against a list of social security recipients. This was necessary because the amount of a veteran's payment is dependent upon annual income from other sources, including social security benefits. The Court rejected the plaintiff's claim of a constitutional guarantee of privacy, finding that the right of privacy does not prevent intra-agency functions 11.

The difficult balancing of interests necessary to differentiate between legal and illegal collection, processing and disclosure of personal data in many countries has led not only to the criminalisation of substantive infringements of privacy but also to the creation of formal duties of registration or of licensing the processing or transmission of personal data.

The violation of these formal duties as well as other duties to inform or support supervisory agencies or individuals concerned are sanctioned by legal penal provisions which in turn have now created new criminal offences in the world of DP. The case of the French company SKF can be cited as an example. SKF had stored information concerning the private life, political opinions, and union membership of job applicants in a manual storage device without reporting it to the French National Commission on Information and Liberties. This is an infringement of Section 42 of the French Law on Data Processing, Data files and Individual Liberties of 6 January, 1978 for which a maximum penalty of 5 years imprisonment is stipulated. The French Commission for information and Liberties handed the case to the State Prosecutor who is now demanding a fine amounting to one year of the company's turnover 12.

3.3.3

OTHER DIMENSIONS TO COMPUTER CRIME

As a result of the increasing expansion of computer techniques in all areas of social life, computer-abuse will not be confined to economic and privacy offences but will also extend to most other classic-crimes. This extension of computer crime can be illustrated in the field of Political, State, Administrative and Judicial interests. Abuses of computer technology in the political domain concern shifts of power between governments and parliament caused by different access to databanks. Political abuse could happen, for example, through manipulation of political elections by computer-based alterations of electoral districts. We refer to this as computer-assisted gerrymandering. An illustration of the possibility of direct manipulations of election results is shown in the 1986 election in Phillipines, when computer personnel refused to continue to work because of alleged orders to manipulate the results. The possible extension of computer crime to offences against human lives has been illustrated by the Japanese White Book on Police in 1983. This describes the incident of 18 January 1979 when an aircraft, landing at JFK Airport in New York with the Russian Ambassador on board, was endangered by computer manipulation by an air-traffic controller. The vulnerability of air and traffic-control systems has also been shown by the terrorist attacks in 1985 on the computer and communications systems of Tokyo Airport and the Japanese railways. Threats to the lives of people caused by computer manipulation are also possible in the fields of computerised hospital supervision systems, control systems for nuclear power plants, and of air, sea, and road transport systems. The malfunctioning of the North America NORAD defence system in 'detecting' an attack by Soviet weapons (13) which in reality had not taken place shows that manipulation and sabotage in the field of highly computerised defence systems could have even graver consequences.

1) Management Awareness of Computer Risks - A European Survey, 1988.

2) Computer Security by John M Carrol, Butlerworth 1987, pg 26.

3) Sieber, Dr Ulrich International handbook on Computer Crime. H. Willey, 1986 p. 3.

4) Computer and Law Journal 471

5) Sieber, Computer Kaminalitatt und Strafrecht 1980 p 39

6) Parker, Fighting Computer Crime 1983 p.267

7) Sieber, Supra P.127 et seq

8) Parker, Supra P.144 et Seq

9) Don Parker: Crime by Computer

10) Ken Wong
Computer Security: What is new? In Kelth Hearden: A handbook of Computer Security; Kegan Page 190 pp 80 & 81

11) Mandell, Computer, Data Processing and the Law (1984) p.188

12) Report of Activities 5e 1985 Annex 18 P.217

12) GAO Report MASAD 81-30 (1981)

CHAPTER 4

LEVEL, IMPACT AND PROSPECT OF COMPUTER CRIME

4.0 INTRODUCTION

The last few years have witnessed a dramatic upsurge in international awareness of computer crime and abuse. Business executives and the general public have seen a spate of press reports on computer manipulation for fraudulent purposes, hacking and computer electronic funds transfer crimes. Even though the above problems are mostly applicable to the advanced countries where the use of the computer is all-pervading, the gradual computerisation of transactions and other data processing activities in the Nigerian economy has suddenly thrown the need to know what is at stake to the top spot in the last few years.

Criminals and other underhand dealers are recognising the merits of using computer facilities and Electronic bulletin boards to further their clandestine interests and to expedite communications in the underworld. At the same time also, the business community world-wide has benefited from better exploitation of computer and networking facilities to harness their business growths and operations. Many companies are totally dependent on the continual support of business systems to provide them with accurate and up to date management information to run their business. It is this dependence on computers that has made the commissioning of crimes very irresistible. What then is the level of criminal acts that have been recorded so far, and how damaging has this been? What is the likely future trend of computer crime as we approach the magical year, 2000 AD?

4.1 COMPUTER CRIME: TO WHAT LEVEL?

The question of the level and scope of computer crime is one that is certain to lead to a heated debate any day and at any time. From the early 70s when the all-pervading influence of computers was beginning to be felt at all levels of business in the developed economies of the Western World, the significance of computer crime was denied by some authors. Estimations today show that one in forty computer Centres in the advanced world is affected by computer crime, that only 1% of all computer offences are detected and that only one in 22,000 perpetrators is sentenced to prison 1. It should be added that in relation to the above figures scientifically sound methods do not allow any reliable statements to be made about the actual scope of computer offences and as such, only estimates based on substantiated experience are possible. This is more so as hard facts about computer-linked crime are notoriously difficult to come by - a result of the precautionary nature of business people: no one finds it easy to admit to mistakes, nor risk the evaporation of business confidence that might all too readily follow a public admission of corporate loss. A question that readily comes to mind when computer crime is mentioned is the one related to the analysis of recent recorded cases of EDP crimes. In the admirable BIS crime Casebook 2, Ken Wong provides the following analysis shown in figure 4.1 of all those crimes reported to him. The survey which was based on 95 cases of computer crime in the United Kingdom had theft of Equipment topping the list with 26%, followed by hacking/system penetration and Theft of Information with 17% and 16% respectively. Arson and Logic/Time bomb came a distant 6th position with 9% respectively. The survey is graphically illustrated below:

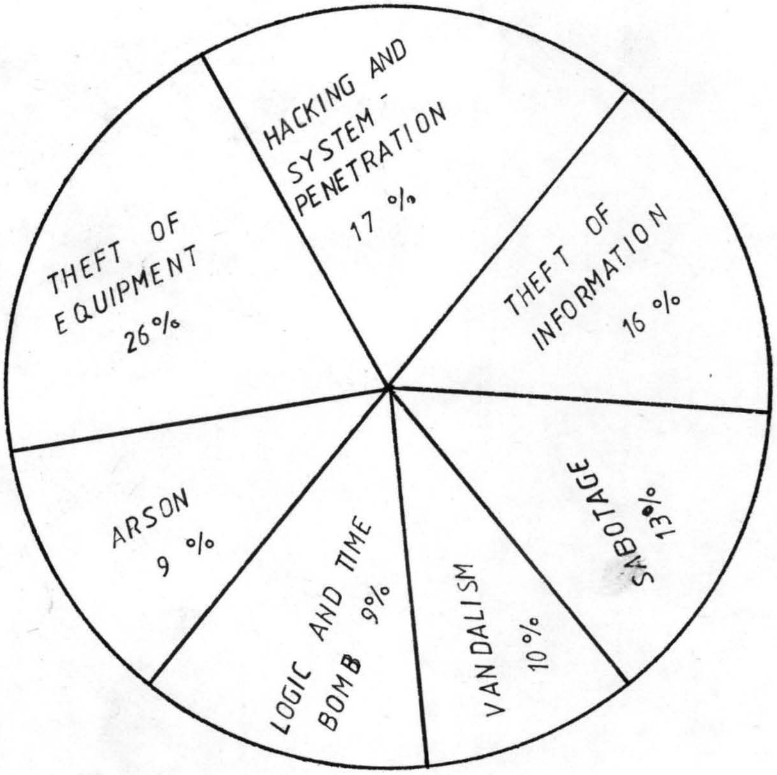

Figure 4.1 Analysis of Computer Crime.

Source: BIS Computer Related Fraud Casebook (1983, BIS Applied Systems)

There are two aspects to be considered when issues related to the level of computer crime are discussed. These are the number of known cases and the problem of undetected offences, usually referred to as the dark figure.

The last few years have witnessed the description of computer crime in many publications. As stated earlier, most of these have no scientific value as they are unverified newspaper reports, secondary literature or popular books, in which the writers often quote each other without critically examining the sources of their information. World-wide, only a few empirical research studies provide reliable information. Even at this, an exact comparison between these is not possible because of the different underlying definitions of the phenomena investigated as well as the different research methods of selection and verifications. It can be stated however that the number of perfectly verifiable computer crimes in all reliable empirical studies is not very large. The most widely pulicised of all computer crimes to date is the 1973 fraud case of the Equity Funding Corporation of America, organised and executed by the concerted efforts of at least 20 data processing and management personnel. The fraud resulted in the loss of $600 million U.S. dollars to shareholders, and a further $1000 million in policies. There were indications that the fraud was not particularly well planned, but essentially a response to expediency justified by wishful thinking on financial prospects.

Empirical studies relating to the level of computer crime in the United States have been conducted by the American Bar Association. The EDP Fraud Review Task Force of AICPA sent questionnaires to banks and insurance companies and published a report on this survey in 1984. It shows that of the 9405 banks surveyed, 5127 responded, 105 of which reported they had experienced at least one case of what was believed to be EDP-related fraud. Another questionnaire sent to 1232 Insurance companies had 854 respondents of which 40 identified cases that they believed to be EDP-related fraud 4. A task force on computer crime of the American Bar Association in February 1984 distributed a lengthy survey to approximately 1000 private organisations and public institutions. It received 275 respondents, 27% of which have sustained 'known and verifiable losses due to computer crime during the last twelve months.' Also, in the United Kingdom, the local Government Audit Inspectorate in 1981 invited the business community to report on cases of computer fraud. The agency received 319 replies which resulted in 67 cases of computer crime and a number (79%) of companies which had not been affected by computer fraud. For its 1985 computer fraud survey, the Audit Commission for local Authorities in England and Wales received 943 replies from Local and State authorities and commercial organisations. The 943 replies, which constituted a 55% response rate, resulted in 77 cases of computer fraud 6.

No known similar studies have been conducted in Nigeria to date so the level of computer-related crime in the Nigerian context is hard to determine. It is however generally believed that when studies are eventually carried out, there will not be much difference between the results here and those conducted in the advanced countries.

The relatively small number of verifiable computer crimes does not permit any conclusion concerning the number of actual cases, as the number of undiscovered offences in computer crime is suspected to be considerably higher. This assumption is justified due, firstly, to the low proportion of computer offences which become known - a factor of the inherent difficulties of detection and proof in the EDP sector. Also, many of the offences that are discovered are subjected to the internal disciplinary procedures of the companies concerned rather than being reported, - a fact attributable to the fear of damage to the company's reputation and lose of confidence by investors, shareholders, and customers or in order to facilitate the compensation for the damage done. Thirdly, cases reported to the law enforcement agencies are not always systematically prosecuted since effective treatment requires special knowledge as well as high expenditure in terms of time and money. Finally, it should be added that it is a matter of chance whether reported cases of computer crime are discovered among other cases of fraud and breach of trust, because the criminological term 'Computer Crime' does not appear in official legal administration statistics 7.

As the four factors enumerated above for determining the level of undiscovered offences must be multiplied many time, the level of computer crime should be estimated as being considerable. Precise figures cannot be given for the reasons discussed above.

4.2 COMPUTER CRIME: HOW MUCH IS LOST?

It is primarily the potential harm to society, not the actual losses revealed in cases up to the present, which make computer crime a serious threat for the developed and developing countries. Various international inquiries into computer crime show different amounts of losses in computer crime which are likely to be the result of the different disclosure techniques in the respective countries and research areas. One fact is however clear from all the studies: Losses in computer crime are much more severe than those in traditional crime. The following selected studies show the level of losses that have been recorded in the past. This is a fair yardstick with which projections into the future could be accurately made.

In the United States, a study by the Stanford Institute International in as early as 1975 indicated an average loss of $450,000 and in 1979 an average amount of $1,685,000. The later figure is based on verified and unverified cases. A study by the U.S. General Accounting Office indicated that a monetary loss could be determined in 49 of the 69 cases undertaken. The total loss was $2,161,413 and the average was $44,110. The U.S National Centre for Computer Crime Data has not been left out in the bid to curb computer crime. Its study in 1985 revealed the following figures:- 18 cases of 'theft of money' with an average loss of $524, two cases of 'theft of programs or data' with an average loss of $81,000, and five cases of 'damage to programs' with an average loss of $93,600 8.

In the United Kingdom, the study by Ken Wong, a private Security Consultant, based upon 95 cases, found average losses of around £31,000 in the field of computer fraud and £1.2 million in computer related arson and bombing 9.

In Japan, 15 of the 19 input manipulations registered by the Central Police Bureau of Tokyo in 1982 showed losses of more than 10 million yen 10.

Similar data for losses occasioned by computer crime are not readily available in Nigeria. This could be attributed to the fact that studies in this area of the EDP revolution have not been carried out.

The reason for the high losses in computer-related property crimes is primarily the high value of DP stored data. In the field of fraud, this is illustrated by the high sums administered in electronic funds transfer systems or stored in computer-based accounts. The perpetrators can even exceed the existing accounts by creating fictitious values, because fraud in deposit money stored in DP systems, in contrast to traditional embezzlement, is not limited by the actual amount of money at hand in a cash register. In the field of sabotage, it is especially the dependence of firms, administrative units, governments, and economies on DP systems which make computer crime a serious threat. The destruction of a computer centre and its computer-stored data can easily lead to the risk of bankruptcy for a firm which does not possess adequate back-up facilities. As the opening sentence of this section shows, it is primarily the potential harm to society, not the actual losses revealed in cases up to the present, which make computer crime a serious threat for developed and developing nations. Again, it is only fair to point out that computer crime is extremely difficult to prove. One case, involving a $33,999 loss, took one thousand man-days of Police investigation before charges could be laid. Total cost: $65,000 11.

4.3.0

CASEBOOK OF COMPUTER CRIME

It is not the purpose of this section to examine specific cases of computer crime in depth but rather to convey some idea of the variety and common incidence of known computer crime. As stated earlier, the real probability of unknown crimes is even more frightening and disturbing.

4.3.1

THE CASE OF THE BANK EMPLOYEE

This case is drawn from the BIS Computer Related Fraud Casebook (1983, BIS Applied Systems). The 19-year-old employee in a large clearing Bank had access to the branch's magnetic master tape for daily update of the bank's head office, for debt and credit transactions of all major accounts. He first succeeded in erasing his credit card account balance of £189 by paying in a bogus credit transaction on the daily update tape. He then credited a friend's account for £15,000 by submitting a document to Key into the master tape. The money was spent in the West end of London. The fraud would have continued to work had he confined his activities to his own branch. However, he tried to transfer £182,000 to another friend's account at a different branch of the bank. For all inter-bank transfers certain documents were required to accompany the transfer, and these were found missing.

Amount: £197,000.

How discovered: The document accompanying the inter-branch bogus transfer was found missing and the fraud was traced to the culprit. He admitted the theft and was suspended from duties.

Penalty: He and the friend who obtained the £15,000, each received a year's suspended sentence. The case of the person involved in the transfer of £182,000 could not be proved, as the account holder denied any knowledge of the transfer.

4.3.2

THE FRENCH ROUND-OFF CASE (SALAMI TECHNIQUE)

The most famous story about computer fraud perpetrated by modification of a computer program is somehow of doubtful origin. It concerns a bank teller who arranged to have the interest computations on all of the bank's depositor accounts truncated instead of rounded off (e.g if a depositor had N2.6498 in interest, he would get N2.64 rather than 2.65). The teller further arranged to have all the "breakage" credited to his personal account. When first told, it was reputed to have occurred in Lyon, France, where the teller was said to have withdrawn his ill-gotten funds after his account had grown to 5,000 france, and then to have moved on to a better paid position at another bank. When told in the United States, the story was entitled "the French round-off". This same story is also famous in France where the miss - en - scence shifted to New York and where the teller is described as having returned to an unnamed Carribbean Island after stealing $100,000. In France, the story is called "le round-off Americain". This is the origin of the technique known as the "Salami attack" in computer crime jagon 12.

4.3.3

UNION DIME SAVINGS BANK

One of the earliest reported computer fraud was an insider job perpetrated by the Chief Teller of one of the branches of the Union Dime Savings Bank in New York. The fraud continued over a period of time during which the bank had no inkling of what was happening, and the Teller was able to extract the sum of $1.5 million in cash, most of which was lost wagering on houses and football games. The Teller had little in the way of computer education, only the minimum necessary to operate the terminal connected to the computer and was able to manipulate the accounts so as to cover up t he fraud completely. The process was basically one of lapping, but the availability of the electronic data that represented money was helpful in this process. The fraud was not discovered by the bank or by its auditors, but came to light because the auditors of the Off-Track Betting System were inquisitive as to the type of person who could wager in such large amounts and stand such great losses 13.

4.3.4

THE CASE OF THE INFATUATED BANK CLERK

In 1981, a 23-year-old, rather naive bank clerk, earning only £200 a month, became infatuated with a 32-year-old, worldly-wise woman. In order to meet what he perceived to be her expectations of him, he lavished money on expensive gifts, travels and general 'good living'. He stole £23,000 from four bank accounts, covering the theft by transferring cash through a computer from 17 other accounts. He then lost £10,000 in Casinos, trying to repay the money. When he was finally caught, the woman deserted him 14.

4.3.5

THE TROJAN HOUSE CASE

A trojan horse is a program that looks as if it is legitimate and indeed it will behave as if it is and will do what the system operator expects it to do: edit other programs, compile them (change them from source code into runnable code), link them with supporting programs, sort lists of data, even check the passwords of persons seeking to receive service from the system.

In the period 1986-7, a group of German hackers calling themselves Data Travellers found a flaw in version 4.4 of the Dec VAC Computer's VMS operating system which enabled them to amend the system's password tables and user privileges. In collusion with an authorised user, the hackers were able to penetrate some 135 computer installations in NASA's world-wide SPAN Computer Network (space physics analysis network). The network connects the North American Space American Space Agency's Scientific Research Centres with its counterparts in Britain, France, Germany, Switzerland and Japan. Although the password lists were held in encrypted form, the hackers were able to introduce a trojan horse to the operating system to trap and copy the passwords entered by users on log-in before they were encrypted and compared with the list of one-way encrypted passwords stored in the system file to authenticate the users. Once the system manager's password was found from the log-in passwords collected, they were able to create new bogus user accounts on the system and protect them with illegal passwords. Eventually, the hackers introduced a skeleton master password which completely by-passed the system's password checking procedure so as to simplify future hacking and to elude detection.

4.4 COMPUTER CRIME: PROSPECTS AND LIKELY TREND

Electronics are not only invisible but are, to most people, also incomprehensible. The exposure to potential losses through computer systems continues to expand as the use of computers increases. Even the most sophisticated computer systems are vulnerable if the proper controls are not in place to prevent unauthorised access to the system and adequate internal controls are not present. The problems caused by computer crime are bound to intensify in the future. Increasing computerisation, particularly in the administration of deposit money, in the balancing of accounts and stock-keeping, in the field of electronic funds transfer systems, and in the private sector, as well as new computer applications such as electronic home banking, electronic mail systems, and other interactive videotex systems will lead to increases in the number of offences and losses. This will also lead to new phenomena and abuses not yet known. Future changes in the field of modus operandi of computer systems will be caused by new safety measures which will eliminate most of the simple manipulation techniques which currently prevail. This will in turn provoke new techniques of circumvention, as can be seen by the increasing number of cases of collusion among several perpetrators a reaction to improved control techniques.

International Computer Networks will lead to trans-national computer crimes committed in one country via remote DP with results in others. Where the prevention of computer crime is not harmonised, this will develop into the emergence of 'computer crime haven'.

We project too that, changes will also result in the field of the victims. Whereas today in most cases the victims are the companies who own the computer, in the future the number of consumers being hit by computer crime will increase. This will be most especially felt in the field of cash dispensers, interactive videotex-systems, and other consumer networks, as well as in the area of fraud against personal computer-users.

In conclusion, there is no doubt that the question of preventing computer crime and of concentrating efforts to overcome the specific difficulties of detection in the DP sector will be of great significance in the future.

1) Becker, The Investigation of Computer Crime (Ed by the US Dept. of Justice, 1988) pp6, 43

2) BIS Computer Related Fraud Casebook, BIS Applied Systems Ltd) (1983).

3) Sieber Utrich, Hand book of computer crime, 1986 pg 29

4) American Institute of Centified Public Accounts, report on the study of EDP-related Fraud in the Banking and Insurance Industries (1984) p.5

5) American Bar Association, Report on Computer Crime (1984); American Bar Association, Statement of Joseph B. Tompkina (1984).

6) Local Government Audit Inspectorate, Computer Fraud Survey (Photocopied 1981); Audit Commission for Local Authorities in England and Wales, Computer Fraud Survey (1985); Scottish Law Commission, Computer crime Consultative Memorandum No.68 (1986). 0.35.

7) Sieber, Computer/Krnunalitat, supra p.168 et seq.

8) Bloombecker, Secure Computing (1985)

9) Wong, Computer Crime in the UK - One yon Vulnerable (1984).

10) Japanese National Police Agency, Report for investigators of Computer Crime (photocopy, 1982).

11) John Carrol, Computer Security, Butterworth (1987) p.15.

12) John Carrol, Supra, pp.32, 33

13) Bower, et al, Computer Oriented Accounting Information systems S-W Publishing Co pp. 404, 405.

14) Hearden, A handbook of Cpt Semty p.43

15) Stearden Supra p.82

CHAPTER 5

THE LEGAL DIMENSION TO COMPUTER CRIME

5.0 INTRODUCTION

The legal understanding of computer-abuse by the law as it is at present is creating problems in two areas: Computer-related economic crimes and computer-related infringements of privacy. In contrast to this, other computer abuses such as homicide committed by computer manipulation and outright theft of equipment have not caused any major legal problems since the laws protecting respective traditional interests are formulated primarily in terms of results and not in terms of modi operandi.

However this may be, especially in English law, the use of computers is causing procedural problems in all areas of crime, particularly as far as the admissibility of computer-generated evidence and the jurisdiction (in cases of transnational computer crime) are concerned. In this chapter, I have examined some of the more important types of criminal behaviour affecting computers and considered how the law, as it current is, attempts to deal with them. I have examined legislations from different countries so that indepth insight into the legal dimension of computer crime can be gained.

5.1 LEGAL ANALYSIS OF COMPUTER CRIME

This section of the chapter will examine three main legal issues which I have grouped into the following:

1) The legal comprehension of computer-related economic crime

2) The legal comprehension of computer-related infringements of privacy

3) The procedural problems of computer crime.

1) **Computer-Related Economic Crimes**

In the field of computer-related economic crime, the main question in most Western countries is to what extent the existing provisions of the penal law as it is at present cover the new forms of offences. In Nigeria, as in most countries, the problems are caused by the fact that the respective penal/criminal provisions, some of which date back to our colonial days, primarily protect physical, tangible, and visible objects against traditional acts. On the contrary, computer crime affects not only these objects represented by new media (such as deposits stored in computer records) but also involves new objects in some areas (such as computer programs or the use of DP facilities) and, in most cases, new methods of commission (such as manipulating a computer instead of cheating a person 1. In certain areas, especially in so far as protecting computer programs is concerned, the new values and objects in the DP area are creating similar problems for the civil law. These problems are somehow closely related to those of penal law: penal law often supports and refers to civil law by protecting civil rights (e.g in the field of copyright) and the violation of penal provisions also generally entails liability for losses. The analysis of the issues involved will be further segmented into the following:

Fraud by computer manipulation

Computer espionage, software piracy, and hightech theft

Computer sabotage

Unauthorised usage.

In the field of fraud by computer manipulations, many criminal law systems face considerable difficulties in applying traditional legal remedies. Take for example, criminal acts such as theft, larceny and embezzlement. The statutory definitions of these terms in the Nigerian Criminal Code, as in most other legal systems, require that the offender take an item of another's property!

The applicability of the provisions, therefore, depends on the circumstances of the particular case, especially on the object and modus operandi of the crime. The provisons can be applied directly if the perpetrator, using the computer misappropriates tangible property, such as cash, cheques, or inventory. Where a case of fraud by computer is the problem is no less easy as the statutory definitions of fraud in most legal systems require that a person be deceived. As the deception of a computer is inappropriate in this case, the applicability of the fraud provisions therefore depends on whether or not the offender has deceived a person checking the data. In English law, the question of whether a machine can be 'deceived' has not yet been clearly answered as the case of R.V. Moritz (1981) illustrates. Here, the Judge held in a fiscal decision involving VAT returns that 'deception' required a human mind which could be deceived. In most countries, computer manipulations that have been prosecuted up to the present could be punished according to existing provisions, but there is no guarantee of a general punishability as the above case has shown.

Penal and Civil coverage of computer espionage and program piracy are among the most topical and economically significant legal questions in the field of computer crime in the present day. An analysis of this has to distinguish (1) the general protection of all computer-stored data (including database and computer programs), (2) the additional special protection of computer programs, and, (3) the special protection of computer dupe. When information is acquired by taking away another person's tangible information - carriers e.g. tapes or disks, the classical penal provisions of theft, larceny, or embezzlement in all Western legal systems do not create any special problems. Still, the ability of DP and communication systems to copy data quickly, inconspicuously, and often via telecommunications facilities has replaced most of these traditional information-carrier theft with acts of copying information onto data devices. The question arising from this is to what extent pure acquisition of intangible information can or should be covered by these provisions. In most continental law countries, Such as Belgium, Italy or Luzembourg, it is generally difficult to apply traditional provisions on theft and embezzlement to the unauthorised abstraction of information, since these laws generally require the taking of tangible property with the intention of permanently depriving the victim (e.g. section 461, Belgian Penal Code). However, the Arnhem Court of Appeals in the Netherlands, in decision of 27 October 1983, assumed that data represented 'a tangible good' in the sense of Section 321 of the Dutch Penal Code. Here, the Court convicted an employee of embezzlement for having copied computer data and programs for the purpose of setting up his own business. The Netherlands is a continental law courting. In Common most common law countries like Nigeria, The United Kingdom and The United States, the penal provisions on theft and embezzlement can be applied to the unauthorised abstraction of information as can be demonstrated by the English Theft Act 1968. This Act defines 'property' to include 'money and all other property, real or personal, including things in action and other intangible property. In the United States, a tendency towards a 'property theory' of intellectual values can be found in the legislation of some

States which have been imposing criminal penalties for theft of trade secrets since 1964. In some States, Courts regard computer data as property in the sense of traditional larceny provisions.

It should be mentioned however that extending the penal provisions on theft to cover information is raising problems. Whereas, theft of programs was affirmed in Hancock V. State of California, it was held in Ward V. The superior Court of California that theft of a program contained in a computer's memory could not be regarded as 'theft' of an 'article' within the scope of the definition of crime contained in the relevant statute. To avoid problems of interpretation in many States, the legislature has now defined computer data or trade secrets as 'property' or a thing of value, thus making the application of the larceny provisions or new general provisions on computer crime possible. I will now consider software piracy.

Can patent law provisions be applied to computer crime where copying of programs is concerned? In most countries there is general agreement that, except for the small number of programs which include a technical invention, the protection of computer programs by patent law is not possible. This is based on the general principle that patentable inventions must not only be new and original but also suitable for industrial application, and therefore give a solution to a technical problem. A a result of this, schemes, rules and methods performing mental acts are not regarded as patentable inventions. Because patent law cannot offer much protection to Computer programs, in recent years the centre of attention has shifted to copyright protection. Since a growing number of countries are seeking to protect computer program by copyright law, the problems caused by its application both for civil and criminal law are now becoming the focus of attention. With the exception of a few developing countries, the applicability of copyright law to computer program has been discussed in all Western Countries during the last twenty years. To avoid legal uncertainty, a number of them have explicitly provided copyright protection for computer programs. The main initiator of this is the United States. Based on the report of the computer software sub-committee of the Commission on New Technological Uses of Copyright Works (CONTU) the American Congress passed the Computer Software copyright Act 1980. Section 101 of this Act declares computer programs to be literary works protected by copyright. It defines a computer as a set of statements or instructions to be used directly or indirectly in a computer in order to bring about a certain result. In the United Kingdom, Section 1 (i) of the Copyright (Computer Software) Amendment Act 1985, which received the Royal Assent on 16 July 1985, also expressly grants copyright protection of literary works to computer programs. The Nigerian copyright decree of 1988 did not specifically make provisions for computer and other software products. This is in direct contrast with the Phillipines - another developing country.

The Phillipines were quick to recognise computer programs as subject matter of copyrighting in Presidential Decree No.49 of 14 November, 1972, effective 6 December 1972. Also, India has amended its Copyright Act 1957 by the Copyright Amendment bill No. xix of 1984, which enlarges the definition of a literary work to include computer programs.

In the area of computer sabotage, the intangible nature of assets stored in DP systems presents legal problems. The provisions of mischief in most countries require that tangible property be damaged. This occurs when computer hardware is physically damaged. The problem here lies in cases of non-physical (logical) damage, especially when data are erased or when access to a computer system is damaged by purely electronic means.

According to prevailing opinion in mist countries, Nigeria inclusive, the deliberate damage or destruction of information on tapes or discs is considered to be damage to property, vandalism or malicious mischief. This results from the argument that the perpetrator either damages or interferes with the function of the physical tape or disc upon which the information is stored. The damaging of hardware and software should only be punished if the perpetrator acts knowingly. This element of wilful intention in the field of computer sabotage is particularly essential since most damage in the DP area is the result of non-punishable acts of recklessness, poor working software, and other technical errors.

The unauthorised use of computer services or time is not really a legal problem and is not covered by penal law. In specific cases however, additional criminal provisions have to be considered, for example, when employees in certain positions cause damage to their employer's equipment.

2. Computer-Related Infringement of Privacy

Even long before the invention of the computer, the extent to which the collection, storage, use, and transmission of personal data is permissible was problematic. However, due to limited methods of using data, it was formerly possible for then existing penal provisions to grant sufficient protection for a few offences of defamation and infringements of special secrets - especially in the medical area and other professional fields. Expanded possibilities of collecting, storing, accessing, comparing, selecting, linking, and transmitting data provided by new technologies since the 1960s have caused new threats which prompted many countries to enact new bodies of administrative, civil, and penal regulations.

The main work in developing an approach to privacy protection in relation to DP so far has been the one done by the OECD (the Organisation for Economic Co-operation and Development). In

1977, the OECD started to elaborate guidelines governing the protection of privacy and transborder flows of personal data. These were adopted by the council of the OECD on 23 September 1980 as a recommendation to the member States for adoption. The guidelines do not legally bind the members and only contain a recommendation to implement the general principles laid down in the text. They relate to physical persons only, applies to both the private and the public sectors, and include automated and non-automated data processing. The guidelines contain the following eight principles for national application:-

1) Collection - limitation, meaning that there should be limits to the collection of personal data and that only such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2) Data quality, stipulating that data should be relevant to the purpose for which they are to be used, to the extent necessary for those purposes, should be accurate, complete and, kept up to date.

3) Purpose-specification, requiring that the purposes for which personal data are collected should be specified not later than at the time of data collection and that the subsequent use should be limited.

4) Use-limitation, affirming that personal data should not be disclosed, made available, or otherwise used for purposes other than those previously specified except with the consent of the data subject or by the authority of the law.

5) security safeguards requiring reasonable safety measures.

6) Openness, claiming a general policy of openness about developments, practices, and policies with respect to personal data and means to establish the existence and nature of personal data.

7) Individual participation, requiring that the data subject has a right to access and to control the data.

8) accountability, calling for accountability of a data controller for complying with measures giving effect to all these principles 2.

In most countries, computer-related infringements of privacy are covered by two types of criminal provisions: the first consists of traditional provisions protecting privacy rights in general (such as the offences of defamation, disclosure of special secrets, or intercepting, recording, and divul*ging* private communications) and the second type involves the new criminal provisions of privacy acts enacted in response to the increasing usage of the computer - a provision that has not yet been incorporated into the Nigerian Criminal Code.

3) **<u>Procedural problems of computer crime</u>**

The issue of computer crime has generated a lot of concern not only to current penal law of different countries but to the procedures to be adopted in prosecuting computer crime. In relation to the prosecution of computer crime, the admissibility of evidence from computer records in courts depends to a great extent on the underlying fundamental principles of evidence in the respective country. In most of the Nordic Countriesand , France and Portugal, the principle of free introduction and free evaluation of evidence applies. The Courts in these countries can generally use all kinds of evidence and must weigh the extent to which it can be relied on. The implication here is that the legal systems in principle do not hesitate to introduce computer records as evidence. In contrary to the legal situation above, the courts in countries that operate <u>common law system</u> (e.g. Nigeria, the united States, the United Kingdom, Canada, e.t.c.) are characterised by the oral procedure. In these countries, a witness can only testify concerning his personal knowledge, permitting his statements to be verified by cross-examination. Here, knowledge from <u>secondary sources</u> such as other persons, books, or records (e.g. computer printout?), is regarded as 'hearsay evidence', and is, in principle, inadmissible. An exception to this is the 'business records exception'. This permits a business record created in the course of everyday commercial activity to be introduced as evidence even if there is no individual who can testify from personal knowledge. The question as to whether computer files and printouts are inadmissible hearsay evidence or falls under the exception has been subject to extensive debate 3.

5.3 PROVISIONS OF THE LAW: AN INTERNATIONAL SURVEY

Faced with relatively recent, but rapid developments in computer crime, many countries have amended their criminal codes or outrightly enacted computer-specific legislations to deal with this new phenomenon. The following representative survey from criminal codes of the underlisted countries highlights computer-specific legislations that are aimed at prosecuting computer-crime. The countries are as follows:

Austria
Canada
Germany
Switzerland
The United Kingdom
The United States.

AUSTRIA

THE PROVISIONS OF THE CRIMINAL CODE AS AMENDED BY THE PROPOSALS OF THE MINISTRY OF JUSTICE FOR A PENAL CODE AMENDMENT ACT OF 1985

Section 126a Damage to Stored Data

1) Any person who suppresses, alters, erases or otherwise renders useless electronic, magnetic or otherwise invisible or not directly readable stored data, without being authorised to dispose of the data or to dispose of them alone, is liable to imprisonment for a term not exceeding six months or to a fine not exceeding 360 daily rates.

section 1479 Computer Fraud

1) Any person who, with the intention of procuring an unlawful gain for himself or for a third person, causes prejudice to another's property by influencing the result of data processing records through incorrect arrangement of the program, through interference with the flow of the records or through the feeding of wrong or incomplete data, is liable to imprisonment for a term not exceeding 3 years.

PENAL PROVISIONS OF THE FEDERAL DATA PROTECTION ACT OF 18 OCTOBER 1978

Section 49. Unauthorised Interference with DP

Any person who unlawfully interferes with the rights of another with intent to cause damage, in that he erases, falsifies or otherwise alters computerised or computer-aided data or in that he procures computerised or computer-aided data shall, where not liable to a greater penalty under another provision, be liable to imprisonment for a period not exceeding one year.

CANADA

CRIMINAL LAW AMENDMENT ACT, 1985 (AMENDMENTS TO THE CRIMINAL CODE).

Section 301.2 (1)

1) Everyone who, fraudulently and without colour of right,

   a) Obtains, directly or indirectly, any computer service,

   b) by means of an electromagnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system, or

   c) Uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or an offence under Section 387 in relation to data or a computer system is guilty of an indictable offence and is liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction.

2) **In this Section,**

'Computer Program' means data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function;

'Computer service' includes data processing and the storage or retrieval of data;

'Computer System' means a device that, or a group of inter connected or related devices one or more of which,

a) contains computer programs or other data, and

b) pursuant to computer programs

i) performs Logic and Control, and

ii) may perform any other function

'data' means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer system.

GERMANY (THEN FEDERAL REPUBLIC)

PROVISIONS OF THE PENAL CODE AS AMENDED BY THE 'SECOND LAW FOR THE PREVENTION OF ECONOMIC CRIMES' OF 1986

Section 202a Data Espionage

1) Any person who obtains without authorisation, for himself or for another, data which are not meant for himself and which are specially protected against unauthorised access, shall be liable to imprisonment for a term not exceeding three years or to a fine.

2) Data within the meaning of sub-section 1 are only such as are stored or transmitted electronically or mechanically or in any other form not directly visible.

Section 263a Computer Fraud

1) Any person who with the intention of procuring an unlawful gain for himself or for a third party, causes loss to another by influencing the result of data processing by improper programming, by the use of incorrect or incomplete data, by the unauthorised use of data, or by otherwise interfering without authorisation with the processing, shall be liable to imprisonment for a term not exceeding five years or to a fine.

Section 269 Falsification of Data of Evidentiary Significance

1) Any person who, for purposes of deception in a legal transaction, stores or alters data of evidentiary significance such that, when perceived, they would yield an ungenuine or falsified document, or when uses data thus stored or altered, shall be liable to imprisonment for a term not exceeding five years or to a fine.

SWITZERLAND

AMENDMENTS TO THE PENAL CODE AS PROPOSED BY THE COMMITTEE OF EXPERTS FOR THE REVISION OF THE PENAL CODE (PUBLISHED IN 1985).

Section 143

Unauthorised Procuring of Data

1) Any person who, with the intent of unlawfully enriching himself or another person, procures without authorisation electronically stored data or programs, is liable to punishment of penal servitude for a term not exceeding five years or of imprisonment.

2) If the offender acts without the intent of enriching himself or another, he is, upon application, liable to punishment of imprisonment or of a fine.

Section 144

Damage to Property

1) Any person who, without authorisation, alters or erases electronically stored data or programs shall also, upon application, be liable to punishment.

Section 147

Fraudulent Misuse of a Data Processing System

Any person who, with the intent of unlawfully enriching himself or another person, induces a data processing or data transmission record, the result of which is incorrect, or prevents such a record, the result of which would have been correct, and thus procures a transfer of value to the disadvantage of another, shall be liable to punishment of penal servitude for a term not exceeding ten years of imprisonment.

THE UNITED KINGDOM

THE FORGERY AND COUNTERFEITING ACT 1981

PART 1

FORGERY AND KINDRED OFFENCES

1) **The Offence of Forgery**

A person is guilty of forgery if he makes a false instrument with the intention that he or another shall use it to induce sombody to accept it as genuine, and by reason of so accepting it to do so or not to do some act to his own or any other person's prejudice.

2) **The Offence of Copying a false instrument**

It is an offence for a person to make a copy of an instrument which is, and which he knows or believe to be a false instrument, with the intention that he or another shall use it to induce somebody to accept it as a copy of a genuine instrument, and by reason of so accepting it to do or not to do some act to his own or any other person's prejudice.

6) **Penalties for offences under Part 1**

1) A person guilty of an offence under this Part of the Act shall be liable on Summary Conviction -

a) to a fine not exceeding the statutory maximum; or

b) to imprisonment for a term not exceeding six months; or

c) to both.

Interpretation of Part 1

8) **Meaning of "Instrument"**

1) Subject to sub-section (2), in this Part of this Act "Instrument" means -

a) Any document, whether of a formal or informal character;

b) Any disc, tape sound track or other device on or in which information is recorded or stored by mechanical, electronic or other means.

PENAL PROVISION OF THE COPYRIGHT (COMPUTER SOFTWARE AMENDMENT ACT 1985

Section 3 Offences and Search Warrants

Where an infringing copy of a computer program consists of a disc, tape or chip or of any other device which embodies signals serving for the impartation of the program or part of it, sections 21 to 21b of the Copyright Act 1956 (Offences and Search Warrants) shall apply in relation to that copy as they apply in relation to an infringing copy of a sound recording or cinematograph film.

UNITED STATES

THE FEDERAL COUNTERFEIT ACCESS DEVICE AND COMPUTER FRAUD AND ABUSE ACT 1984

Chapter xxi - Access Devices and Computers

Sec.2101. This chapter may be cited as the "counterfeit Access Device and Computer Fraud and Abuse Act of 1984".

1030. fraud and related activity in connection with computers

a) Whoever -

2) Knowingly accesses a computer without authorisation, or having accessed a computer with authorisation, uses the opportunity such access provides for purposes to which such authorisation does not extend, and thereby obtains information contained in a financial record of a financial installation, as such terms are defined in the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.), or contained in a file of a consumer reporting Act (15 U.S.C. 1681 et seq.); or

3) Knowingly accesses a computer without authorisation, or having accessed a computer with authorisation, uses the opportunity such access provides for purposes to which such authorisation does not extend, and by means of such conduct knowingly uses, modifies, destroys or discloses information

in, or prevents authorised use of, such computer, if such computer is operated for or on behalf of the Government of the United States and such conduct affects such operations;

Shall be punished as provided in sub-section (c) of this section.

c) The punishment for an offence under sub-section (a) or (b)(1) of this section is:

a fine of not more than the greater of $5,000 or twice the value obtained or lose created by the offence or, imprisonment for not more than one year, or both, in the case of an offence under sub-section (a)(2) or (a)(3) of this section which does not occur after a conviction for another offence under such sub-section, or an attempt to commit an offence punishable under this sub-paragraph.

5.3 <u>PROVISIONS OF THE LAW: IN NIGERIA</u>

Even though the Northern and Southern States of Nigeria operate the penal and criminal code system of justice respectively, the provisions regarding forgery are basically similar. I cite below sections of the Northern Nigeria Penal Code dealing with forgery and falsification. It is noted that no specific mention was made of altering computer software programs to achieve results that but for such alteration and falsification would have been impossible.

NORTHERN NIGERIA PENAL CODE

CHAPTER XX: FORGERY

Section 371 Falsification of Accounts

Whoever being a clerk, officer or servant or employed or acting in the capacity of a clerk, officer or servant, wilfully and with intent to defraud, destroys, alters, mutilates or falsifies, any book, paper, writing, document of title or accounts, which belongs to or is in the possession of his employer or wilfully and with intent to defraud makes or abets the making of any false entry in or omits or alters any such book, paper, writing, document of title or account, shall be punished with imprisonment for a term which may extend to seven years or with fine or with both.

Section 377

Making or possession of any instrument for counterfeiting a property mark:

Whoever makes or has in his possession any die, plate or other instrument for the purpose of counterfeiting a property mark or has in his possession a property mark for the purpose of denoting that any goods belong to a person to whom they do not belong, shall be punished with imprisonment for a term which may extend to three years or with fine or with both.

THE NIGERIAN COPYRIGHT DECREE (NO 47) 1988

PART 1 COPYRIGHT

Section 1 Works eligible for copyright

1) Subject to this section, the following shall be eligible for copyright:

   a) Literary works
   b) Musical works
   c) Artistic works
   d) Broadcasts.

2) A literary, musical or artistic work shall not be eligible for copyright unless:

   a) sufficient effort has been expended on making the work to give it an original character; and

   b) the work has been fixed in any definite medium of expression now known or later to be developed, from which it can be perceived, reproduced or otherwise communicated either directly or with the aid of any machine or device.

Section 2 Copyright by virtue of nationality or domicile

1) Copyright shall be conferred by this section on every work eligible for copyright of which the author or, in the case of a work of joint authorship, any of the authors is at the time when the work is made, a qualified person, that is to say -

   a) an individual who is a citizen of, or domiciled in Nigeria; or

   b) a body corporate incorporated by or under the laws of Nigeria.

Section 5 General nature of copyright

1) Subject to the exceptions specified in schedule 2 to this Decree, copyright in a work shall be the exclusive right to control the doing in Nigeria of any of the following acts, that is

   a) in the case of a literary work, to do and authorise the doing of any of the following acts -

      i) reproduce the work in any material form

      vi) distribute to the public, for commercial purposes, copies of the work, by way of rental, lease, hire, loan or similar arrangement.

Section 14 Infringement of Copyright

1) Copyright is infringed by any person who without the licence or authorisation of the owner of the copyright -

   a) does, or causes any other person to do an act, the doing of which is controlled by copyright;

   e) makes or has in his possession, plates, master tapes, machines, equipment or contrivances used for the purpose of making infringed copies of the work.

section 18: Criminal Liability

1) Any person who -

   a) makes or causes to be made for sale, hire, or for the purposes of trade or business any infringing copy of a work in which copyright subsists; or

   c) Makes, causes to be made, or has in his possession, any plate, master tape, machine, equipment or contrivance for the purposes of making any infringing copy of any such work;

shall, unless he proves to the satisfaction of the Court that he did not know and had no reason to believe that any such copy was not an infringing copy of any such work, or that such plate, master tape, machine, equipment or contrivance was not for the purpose of making infringing copies of any such work be guilty of an offence under this Decree and shall be liable on conviction to a fine of an amount not exceeding N1,000.00 for every copy dealth with in contravention of this section or to a term of imprisonment not exceeding 5 years, or to both such fine and imprisonment.

Section 39: Interpretation

1) In this Decree, unless the context otherwise requires - "Literary work" includes, irrespective of literary quality, any of the following works or works similar thereto -

a) Novels, stories and poetical works;

b) Plays, stage directions, film scenarios and broadcasting scrips;

d) Computer Programmes

e) Text books, treatises, histories, biographies, essays, articles.

"Computer Programs" means a set of statements or instructions to be used directly or indirectly in a computer in order to bring about a certain result.

5.4 PROSPECTS OF DETECTION AND PROSECUTION

Detection of, and possible prosecution of computer crime is an issue that has attracted much learned discussions in the recent past. This is largely attributable to the fact that computer crime is a somewhat invisible and often sophisticated phenomenon. So sophisticated in fact, that it will take experts in computer programming and experienced data processing personnel to discover that a crime against the computer and its software contents has been committed. It is said that all known computer crimes discovered up to the present date amounts to less than 10% of all assaults on computers and software contents.

The detection and consequently, correct and concise application of the law and the prosecution of computer crimes, especially by investigating authorities and courts is complicated by particular difficulties of discovery and detection in the data processing area 4. I have listed these difficulties below.

1) **Criminal acts are usually disguised by perpetrators.**

   The detection and consequent prosecution of computer crime in many cases is hindered by the fact that the criminal acts are disguised by the perpetrators. An example can be cited from computer fraud which is often concealed by the manipulation of data processing printouts. Also, computer espionage committed by copying data files as well as 'time theft' per-se do not appear as crimes in victimized companies which do not have an opportunity to discover an prove unauthorised usage.

2) **Computer Crimes do not leave traces**

In many cases, the investigation and prosecution of computer crime is aggravated by the fact that program and data alterations do not leave traces comparable to classic document forgeries. As it were, handwriting analysis is no longer possible in electronic data banks. As an illustration of this, the following German case will suffice:

> The problem of following electronic traces was colourfully illustrated in a then West German case. The perpetrators had replaced the name and address of one of their employer's suppliers with that of a fictitious firm on the master data file which was connecting account numbers with suppliers' addresses to check the payment of invoices. As a result of this alteration, the subsequent invoice of a supplier resulted in a cheque made out, not to the supplier, but to the perpetrator's fictitious firm. This payment of about DM135181 to an unknown supplier caused suspicion and the cheque was stopped and investigations carried out.

3) **Evidence are not usually visible**

The detection and prosecution of computer crime requires a great deal of checking computer data. As most of these data are no longer stored in a visible, human-readable form but in an invisible and only machine-readable highly concentrated electronic storage devices, detection becomes almost impossible. The main problem therefore consists of a lack of visual and understandable evidence caused by the anonymity, compression, and often even encoding of electronically stored data.

4)

Evidences are usually encoded by perpetrators

A computer crime perpetrator can make these problems even worse and expected search and seizure procedures more difficult by protecting his data with passwords, hindering instruction, and cryptographic techniques. In the same vein, in the field of privacy infringements cryptographic techniques can make effective control of stored data - especially in the field of small personal computers - very difficult.

5) **Perpetrators usually erase evidence**

Another difficulty of detection and consequent prosecution results from the fact that the perpetrators can easily avoid proof by erasing data. Usually, their explanations for such acts are mistakes in computer handling.

A sophisticated 'automatic' method of this method was disclosed in a Dutch proceeding against an illegal arms dealer. A gun-runner, who has stored the addresses of his clients in a small computer, had changed the regular commands in the operating system so that the input of a copy or print-command via the computer's keyboard would execute the erasure of all data. This trap, especially programmed for expected search-and-seizure procedures, was however, detected by the DP specialists of the Dutch 'Fraudecentrale', who sensed that something had been changed in the computer's operating system and therefore produced copies of the seized discs in their own computer system 5.

6) <u>Inexperience of investigators and prosecutors</u>

In addition to the above problems, the prospects of detection and consequent prosecution of computer crime has been further aggravated by the fact that many auditors, investigation officers and judges are not familiar with information media and therefore cannot deal properly with the technical aspects of Data Processing. Sieber has this to say in this regard:

"The problems of State Agents unfamiliar with DP may be illustrated by a report of a DP specialist describing to the author (Sieber) how he crossed the West German/Swiss border with a number of magnetic tapes containing valuable data.

When he was asked by the customs officers whether the tapes were empty or not and truthfully declared their valuable contents, he received the answer: 'then you don't need to pay any duty, as used tapes are worthless" 6.

5.5 RECOMMENDATIONS

From the above analysis, it becomes obvious that mere reforms of penal and procedural laws to accommodate computer crimes is not sufficient to make the detection and successful prosecution of computer crime possible. An appropriate measure would be the training of auditors, accountants and other investigating officials. Such training could be modelled on the Royal Canadian Mounted Police Computer Crime Investigation Course, the content of which is as detailed below:

a) Computers and electronic data-processing fundamentals;

b) Introduction to Computer Programming;

c) Computer Security;

d) The law and evidence;

e) Computer crime

CHAPTER SIX

COMPUTER SECURITY MEASURES

6.0 WHAT IS AT STAKE?

"There is no such thing as computer security. There are only various degrees of insecurity. Any person who can dial into your computer from a telephone; submit a deck of cards, a magnetic tape or cassette, a floppy disk, or disk pack at your service counter for processing; send you a message by electronic mail; or write a program that you subsequently run on one of your computers can do any or all of the followings:

i) copy all of your sensitive files

ii) juggle your accounts to cause you financial loss

iii) re-program computers embedded in other equipment to manufacture defective products, wreck production equipment, kill or maim employees, or launch weapons at friends and allies".

John M Carrol wrote the above quotation in the introductory page of his book "computer security" in 1977. Even though we are all not bound to agree with his strong assertion, the fact still remains that the issue of ensuring a high level of security for EDP equipments programs and results is a very important one.

The security problems associated with a computer system include all those commonly associated with protecting property and information generally, as well as many problems peculiar to the electronic data processing environment. What is at stake then, is the vulnerabilities of Resource-sharing Computer Systems and microcomputers. In resource-sharing data systems, the principal points of vulnerability can be identified as the following:

Processors

Storage-devices

Communications Facilities

Remote Terminals

Users and System Personnel.

While the central processor can be susceptible to failure of protection circuits, the file protection and access control program software of the central processor can be by-passed or out-rightly have user identification falsified. In each of the above scenarios, the loss of a vital element of EDP resources cannot be ruled out. Storage devices are susceptible to unauthorised copying of stored information. Users can misrepresent or forge their identification or authorisation, seek unauthorised access to sensitive information through browsing and can even use debugging procedures to circumvent security mechanisms. Systems personnel usually have normal unrestricted access to supervisor programs, accounting files, systems files, protective features and files stored on EDP media. Where they are not loyal and reliable, serious security risks, the types that can result to losses usually arise. Even in the microcomputer environment, anybody who can physically approach the machine itself can steal any of the data files with a little bit of manipulation or outrightly remove the equipment itself. He can copy files residing in any mainframe computer with which the micro can communicate into floppy diskettes.

6.1 AIMS AND SCOPE OF SECURITY

Evidence have shown that most cases of computer crimes were caused, enabled, or at least simplified by the victim's inadequate security systems. Computer security strategies have five basic objectives to fulfil:

Deterrence
Prevention
Detection
Minimising Effects
Fulfilling Legal Requirements.

Any security measure must be capable of deterring people from attempting to commit any unauthorised act. Where the commission of a crime is being hatched, the mere evaluation of the odds represented by the security measures in place should be able to discourage the potential criminal. It is however to be noted that deterrence in many cases is hardly achievable where there is a crack band of criminals. Where this is the case, security measures should at least be able to prevent the successful completion of the criminal act. Unfortunately, prevention of crime, much like deterrence is hardly attainable when the cost elements are considered. In this case, safety strategies should be focussed at detecting computer crime so that the execution of completed acts could be terminated to permit correction and recovery. This in turn will generally deter other potential perpetrators.

The fourth aim of security is to minimise the effects and damages of computer crimes which could not be prevented. This will also ease recovery and correction. The above four aims of computer security are primarily for the benefit of the computer user. The fifth aim of security measures is to fulfil legal requirements of privacy, tax and commercial law. Somehow, the fifth aim helps greatly in serving Social and public interest too.

Computer security measures should not be restricted to the issue of computer crime alone as there are other more or equally damaging phenomenon that can render data and computer usage ineffective. Besides the intentional acts of computer crime, consideration should also be given to threats caused by negligence, human errors and professional incompetence, to natural occurrences and environmental forces such as fire, storms, smoke, as well as to airconditioning breakdowns and power failure.

6.2 COMPUTER SECURITY: WHOSE RESPONSIBILITIES?

Computer security is not a matter that should be left to a single person who may be designated the EDP Director or other appropriate nomenclature. It is a collective responsibility that has as its co-ordinator the EDP Director. He has to create a mood of continuing security awareness on the part of staff, to see to it that they are both aware of security precautions and actually carry them out. Where the company is a fairly large one, the Director will appoint a Security Co-ordinator who may either be an EDP Personnel with training and interest in security or a security person with training in EDP. The Director has to continually liase with other company Managers whose data he processes and then decide upon a minimum level of essential EDP service that he will undertake to deliver despite all contigencies.

The Director has to be aware of the security implications in the roles of all EDP personnels, especially the following:

1) Tape Librarian, who has custody of EDP media
2) Data base administrator, who manages data bases
3) Systems Integration Manager, who is usually responsible for integration of hardware and software systems

4) programming Manager, responsible for customer programs

5) Systems Programming Manager, responsible for the computer operating system, that is, the collection of programs governing the operation of the computer itself.

6) Data Preparation Manager, responsible for the preparation and validation of all input data.

While the above class of personnel have their specific duties to perform, the attainment of an appreciable level of security rests on their shoulders. This however presupposes that the company is fairly large, the EDP environment being an elaborate set-up where a sizable fraction of the company's capital has been invested in EDP equipment and personnel.

6.3 DIMENSIONS TO COMPUTER SECURITY

Computer security measures share certain protective features with other kinds of security. These are in the areas of administrative and organisation measures, provisions to ensure the loyalty and reliability of personnel and normal physical and environmental safeguards. Other protective features are however peculiar to EDP security as they relate to hardware equipment, software (programs) and communications in cases where a remote environment is under consideration. From whichever perspective it is examined, any security measure adopted should have the following desirable qualities:-

Completeness

Correctness

Simplicity

Survivability

Fall-safe

Spoof-proof

Cost effective

A computer security measure must do the job it is intended to do and should never depend on the supposed ignorance on the part of a potential adversary. It should be complete, in that it should function in every possible mode of operation, and it should also be correct, in that it should provide the correct response to every possible stimulus.

In summary, security for computers can be examined from the following dimensions:

Physical Security

Terminal Security

Data Security

Program Security

Procedure Security

Communication Security

Disaster Preparation.

6.3.1 Pysical Security Dimension

While it was fashionable to show or exhibit computers off to important customers and visitors in the early days of the data processing revolution, the trend these days - borne out of security consideration - is to conceal the physical location of the computer room from as many eyes as possible. Physical security dictates that a system must possess the ability to distinguish among authorised persons, unauthorised visitors and other unauthorised persons. This discrimination should be exercised by automatic access-control systems or by guards. The following are physical security precautions which must be taken in any computer installation.

i) Security starts by limiting access to the computer room only to those who have a specific need to be there. To ensure this, admission badges should be worn conspicuosly by those who are entitled to be there for any business.

ii) Where computer room personnel for some reasons are to stop having business with the computer room, entrance cards should be collected from them and destroyed so that access is denied to them.

iii) In cases of known security violation or any other threat from any source, changes in access rules and requirements should be effected immediately.

iv) Where an employee is disengaged whether by volition, the rule of 'instant termination' should be invoked to ensure that the employee leaves the premises immediately without returning to the place of work. Cases have been reported in the past of employees who have damaged their terminals or corrupted software programs on learning of their termination.

v) There should be a careful and deliberate location of the computer room in parts of the premises which is somehow obscure to all but those with the need to know. The fewer the people that are aware of where the computer room is located the better for everyone concerned with security.

vi) Security is a matter of attitude. Employees of the computer room should be encouraged to challenge all strangers who come within the operating environment of the computer.

vii) Tours of the computer room, whether guided, should be discouraged. The fewer the people that enter the room, the lesser the risk of a security breach.

6.3.2 Terminal Security Dimension

Advances in telecommunications have now made it possible for computers to be reached from remote sites, either in the same building or many miles away. As a result of this, terminal security for access to the computer can be as important as providing physical security in the form of controlled entry. The following terminal security measures should be formulated and strictly enforced:

i) Provide passwords and assign these to particular terminals. A password is a control technique used to restrict access to a computer; it has 3 elements:

authorisation to use computer facilities
User identification when access is sought
authentication of user identity and access authorisation

Passwords should be changed as frequently as possible. Here, the Security Manager should watch out for the practice of flip-flopping. This describes the practice of only ever using two passwords, and of complying with the requirement to change regularly by merely alternating between the two.

ii) Limit access to data files or certain parts of data file to only those who have a need to know priority. This can be achieved by building multi-access level into programs. Restrictions like this one allow only certain people to read data files but not to write into them or make any changes in any way. Discretionary access control matrix like the one shown below can fully ensure that the objective is achieved.

DISCRETIONARY ACCESS CONTROL

SUBJECT	**OBJECT 1**	**OBJECT 2**	**OBJECT 3**
SUBJECT 1	EXECUTE	READ	R/W
SUBJECT 2	GRANT	EXECUTE	READ
SUBJECT 3	R/W	GRANT	EXECUTE
SUBJECT 4	READ	R/W	GRANT
SUBJECT 5	EXECUTE	READ	R/W

With the above matrix, discretionary access-control policies can be fully implemented. Here, there are five subjects (people or computer programs acting on their behalf). There are likewise three objects (program listings or data files and four access privileges:

EXECUTE which will run the program; READ which means view only; R/W which means the subject can READ as well as WRITE into the program or data file; and GRANT which will somehow bestow privileges on other subjects. Given the above, any security violation can be easily identified and rectified.

iii) Encrypt Passwords so that they are not available in plain language. To some extent, this will eradicate 'password espionage' through shoulder-surfing.

iv) Program the system software to ensure password security while at the same time setting traps for password/entry violators. With this, whenever there is an attempted log in, the following interactive dialogue with the system will be recorded:

```
Amstrad Multisys:                  )The computer will
FUT Mx                             )generate this
There are 25 users on the          )
system 28/03/94 12.36 BST MON      )

Log in MRBROWNJABO                 )User generated
Password?                          )Computer generated
(blank)                            )
```

```
OK
MR BROWNJABO                              )
Logged in 28/03/94 12.36 BST MON          )
From Terminal 115                         )
Last Login was 27/03/94 at 09.46BST       )
SUN from Terminal 152                     )  The computer
Welcome to multisys                       )  will generate
Message from Operating Control            )  this
Password for user MRBROWNJABO given       )
Incorrectly from Terminal 105 on          )
27/03/94 at 07.22 BST SUN                 )
```

From the above dialogue in the attempt to use the computer, two security objectives have been achieved simultaneously:

i) Access has been denied to a potential adversary

ii) We have been informed that someone has incorrectly used MRBROWNJABO'S password.

6.3.3 Data Security Dimension

A company has a general responsibility to keep certain information confidential. Where this is not done, it may be exposed to legal consequences where negligence is proved. Data security is ensured by strict control and enforcement of rules pertaining to the following:

i) Unauthorised use of company data should never be allowed under any circumstances.

ii) There should never be any unauthorised modification of company data stored in the system.

iii) Unauthorised disclosure of data should be controlled so as to avoid liability for negligence.

iv) Removal or transfer of data should be carefully handled. Data that is not required for a reasonable time should be removed from computer access directly and returned to the Library where it can receive proper protection.

v) There should be restrictions on login. Create provisions so that access to critical files will have a log of those that used them and compare this to the discretionary access control matrix. Note violations of access rules.

vi) Make provisions for integrity of data in cases where there is accidental erasure or disk failure. There should always be backup files at another location in a safe place so that the correct records can still be reconstructed readily if the original files are ever destroyed.

6.3.4 Program security dimension

Just as with data files, the unauthorised modification of computer programs can cause innumerable problems. The development of programs and their usage must be closely monitored. Programs should be tested strenuosly to ensure that they do all that is required of them and nothing more. Analogous to this, all tests should be reviewed. The following precautionary steps should be taken:

i) No program should be developed and implemented by a single individual.

ii) Changes should not be made in any program without proper approval from all the parties concerned in the development of the program. This is usually achieved by holding the source programs and documentation in the Library or in locked cabinets or safe.

iii) There should be formal controls over changes; likewise, access to programs for the purpose of making changes should also be formal. This ensures that computer personnel do not take program changes lightly.

iv) No person should be allowed to copy company program without specific approval. This will ensure that opportunities for copies to be made available to others for monetary gain or other espionage purposes are greatly reduced.

v) Where possible, fire and theft insurance should be expanded to cover the lose of programs and data files.

6.3.5 Procedure Security Dimension

Computer Operation Procedures are a combination of personnel, equipment and controls which all have security implications that have to be properly addressed.

Personnel

Security effectiveness should start with hiring responsible personnel who are capable of doing the work properly and are well trained in what they need to do.

i) Formulate procedures for hiring computer room employees. Here, not only technical skills but security implications should be considered.

ii) Adopt pre-employment screening. The revision of reference should be completed by confidential enquiries to former employers, some of whom, more often than not, would fail to include misdemeanours, misconducts and other negative items in their references in order to avoid liability.

iii) During the course of employment, enforce vacation and job-rotation in order to avoid dependency on the exclusive knowledge of one person and to prevent one employee being permanently able to conceal evidence of manipulation.

iv) Note special peculiarities such as non-taking of holidays or excessive spending by employees in highly sensitive jobs. Investigate these traits discretely.

v) Watch employment termination procedures. The majority of all cases of computer sabotage and theft of software committed by employees are committed shortly before the employee leaves the company. Remove employees from the computer areas before or immediately after notice has been given. Release of staff with possible access to password files should be followed by check and change of all possible 'private passwords' and colleague's passwords installed or obtained by the employee before leaving the company.

processing

i) Plan and schedule the volume of work to process; this will control as well as make it difficult for unscheduled work to be done.

ii) Institute and periodically review computer usage logs to ensure that the system is as secure as it is supposed to be.

Equipment

An operating interruption due to power failure or equipment malfunction can cause considerable havoc whenever there is a necessity to do a day's work in a day like in the banking sector.

i) Formulate emergency drills and rehearse these so that all personnel know exactly what to do when there is an equipment failure - both for the short-term and the long-term if it should prove necessary.

ii) There should be regular backup procedure whereby data files and programs are copied onto tapes or other disk files and taken to a secure place such as a bank vault or a fireproof safe in another geographical location.

6.3.6 <u>Communication Security Dimension</u>

There are several sub-fields in communication security. They are as follows:

Line security
Cryptographic security
Transmission security
Emssion security
Technical security

Line security is concerned with safeguarding from unauthorised access the communication line interconnecting parts of an EDP system which is usually a central computer and one more remote terminals.

Cryptographic security is concerned with invoking some kind of privacy transformation of the data so that information exposed on communications lines is rendered unintelligible to an unauthorised person intercepting it.

Transmission security is concerned with conducting communications procedures in such a way that minimal advantage is conceded to an adversary who is in a position to intercept data communications.

Emssion security is concerned with preventing undesired signal data emanations transmitted without wires, usually either electromagnetic or acoustic, that could be intelligible to unauthorised persons intercepting such emanations at a location outside the secure area.

Technical security is concerned with defence against unauthorised interception of data communications facilities by the use of intrusion devices such as microphones, transmitters, or wiretape.

Communications security will take the following forms:

i) Make sure that communication with other internal or external locations is sufficiently secure so that data are transmitted accurately.

ii) Identify the originating source and check to ensure that the sending device is authorised to send that type of message.

iii) Where a considerable number of messages are to be transmitted to remote locations, use block transmission so that a standard-sized block would be used for each message.

iv) Data-carriers containing sensitive data should always be protected by electronic sealing methods or by encoding. This will guard against alteration of data during transmission.

v) Institute adequate log-on procedures, user-identifications and passwords with adequate length and proper key management.

vi) Top-secret computer applications should, if possible, be executed on separate computer hardware with no connection to telecommunications systems and remote diagnostic procedures.

6.3.7 Disaster Preparation Dimension

There is little a company can do to counter a disaster ahead of time. As a result of this, it is only natural that the kind of problems that can accompany disasters like flood, earthquakes and fine as well as the possibility of extensive damage through explosion, theft, riot and vandalism should be adequately projected and provision made in readiness.

i) Damages through flood can be prevented if the computer facilities are located sufficiently above the high-water level where water is not likely to seep in and short out the electrical equipment.

ii) In considering the possibility of damages from fire, fire proof safes or vaults should be provided to prevent the programs and data files from being destroyed.

iii) Fire extinguishers and foam with sprinklers should be installed as required. In all cases, emergency power cut-off equipment should be available in a prominent place in the computer room. This will take care of situations where smoke detections and fire alarms have been activated.

iv) As it is not always possible to prevent vandalism or other forms of civil commotion, the damages and losses can be further minimised if the computer rooms are located in a part of the building with no windows and few doors. Video surveillances for security guards should also be installed - where this is possible..

v) All important materials such as files and programs should be put away securely at the end of the working day. The computer supervisor or other designated person should always check to see that this has been done.

Recovery procedures

Disasters could occur when people least expects any, and what is more, at inconvenient times such as in the middle of the night or over the weekend. The list of people to contact in cases of emergency should be kept. Lists and telephone numbers of all personnel should be made available to those persons with a need to know. Checks should be made periodically to ensure that the lists are up-to-date and ready for use in the case of emergency.

6.4 RECOMMENDATIONS

It is strongly recommended that the Senior Management in every company should develop a computer policy statement. This should cover all aspects of computer operations. All users of computer within the company should read, understand and sign the statement. This statement should also cover all precautionary measures to guide against crime and sabotage. Security is a way of life and so, computer security should never be taken for granted.

CHAPTER 7

SUMMARY, RECOMMENDATIONS AND CONCLUSIONS

7.1 SUMMARY

This study was aimed at examining the phenomenon of computer usage and the accompanying problems of crime and security involved. The rate at which companies and individuals are acquiring computers to ease up their information processing operations is increasing at a very alarming proportion. Consequent to this computerisation is the problem of crime specifically directed at the computer and its various outputs. Control measures to prevent or at least minimise attacks against the computer are represented by security.

It was noted that most people in their quest to get every thing computerised have not realised that the ability to secure information from those who do not have the need to know and other criminal-minded individuals only start after the acquisition of computers. It was noted that the computer is only as secure as we make it. In as much as there are always criminals and adversaries who are hell-bent on having their ways, the computer is very vulnerable and on its own, helpless. Vulnerability was defined as the cost that an organisation would incur if the event took place; for this reason, the issue of computer crime and security is one that should be properly addressed by those who use the computer, those who writes the program and the government that is in power.

Computer crime was defined as all threats directed against electronic data processing (EDP) equipment and its supporting facilities (hardware), programs and operating systems (software), supplies, information handled by EDP system, negotiable instruments stored or created at the facility, and critical resources required by the EDP system to render services. The various facets of computer crime were identified and discussed. It was stated that just as the information processing world is witnessing rapid advances, the computer criminal is also perfecting more sophisticated and trouble-free techniques to circumvent all computer security measures. From this, it became obvious that we are not yet at the stage of regarding the computer as properly secured against attacks. Eternal vigilance represented by software and personnel control measures are necessary to counter this growing threat.

The legal dimension to computer crime and the prospects of prosecuting known crime was next examined. Here, it was pointed out that the very nature of the working of the computer makes it difficult to detect and consequently, prosecute computer crime, particularly as most prosecutors are not very well grounded with the intricate working system of the computer. From comparative analysis, it was discovered that most countries (especially the advanced ones) have enacted specific laws to deal with the rising wave of computer crime. It was also discovered that apart from the brief mention of computer software in a very tiny foot-note in the Copyright Decree of 1988, Nigeria has no law to deal specifically with the problems and issues represented by computer crime in both the Penal and Criminal Codes respectively.

The security measures available to computer users were next examined and it was pointed out that the most effective security measure is that represented by people. Absolute security, it was pointed out, is unattainable, hence John M Carrol stated that there are only various degrees of insecurity. No matter how good the protective measures adopted, there will always be some means of damaging the computer or data. As a result of this, the objective of any security measure is to minimise the exposure that a company faces and at best, to prepare adequately for any eventuality. A number of security measures were suggested for adoption by all computer installations, even though not all will be useful or applicable in any particular organisation. In conclusion, security measures have been compressed into four methods to reduce risks.

1) minimise the probability of a breach happening. An important part of any security program is prevention and this can apply both to physical security and discouraging manipulation and embezzlement.

2) identify that a problem has occurred. The security of the installation and the controls surrounding the systems should provide details which will reveal that an unauthorised event has happened,

3) minimise the damage of an event. Once a fire has started or a file has become corrupted, the controls and procedures already in place should be sufficient to isolate the event and restrict the effect to a small area

4) design a method of recovering from the damage. It is important for the continuity of the business that recovery is both quick and effective, whether it requires the replacement of equipment or reconstruction of a file.

Security, just like crime, is a way of life. We all should be prepared and eternally vigilant to counter the threats represented by the computer criminal.

7.2 RECOMMENDATIONS

7.2.1 To the computer users

a) **Managers should:**

Define responsibilities of those involved in systems design, in systems use, and in auditing. Develop for all users a 'computer code of conduct' and watch out for violators.

Ensure adequate training is given at all levels.

Become personally computerate (computer literate).

Allow realistic time and budget schedules for developing security in computer systems.

b) **<u>Auditors to companies should</u>**:-

Liase with computer staff in the development of systems.

Ensure provision of adequate audit trails

Become personally computer literate.

c) **<u>Computer room employees should:</u>**

Be aware of the need for security.

Ensure programmers and analysts possess general business skills, as well as technical expertise.

Allow sufficient time to develop secure systems during program development.

d) **Those concerned with security:**

Become computerate.

Analyse risks associated with using the computer.

Always ask 'awkward questions of computer staff, of auditors and all other users of the system.

Liase with other Managers, Auditors and Computer staff.

7,2,2 The Government shoud

Enact computer specific laws to deal with computer related crimes. Such laws could be fashioned on the United States, Canada and United Kingdom models.

Regulate the practice of computers by an enabling decree in line with other professions like accountancy, medicine and law.

Set up a computer crime unit in the Nigerian Police Force to monitor and prosecute computer crime. This unit should be fashioned on the Royal Canadian Mounted Police Model.

7.2.3 Computers association of Nigeria should:

Fight for a speedy recognition by the government so that the practice of computers can be fully regulated.

Monitor sharp practices by some unscrupulous computers and software dealers.

7.2.4 **The General Public should:**

Consider the full implications of 'going computers'. Plan well in advance and make adequate preparations for all eventuality before computerisation. Beware and be suspicious of computer and software vendors who make elaborate and sometimes grossly exaggerated claims about the capabilities of their computers and softwares.

Remember that getting 'computerised' is one thing whereas to keep the system running smoothly and successfully is quite another.

7.2.5 To all of us:

Caveat emptor

7.3 **conclusions**

This project will be concluded with quotations taken from legislations in two advanced countries where the use of the computer is prevalent.

1) The State of Florida in the United States enacted a computer-specific legislation, the preamble to which sets out the terms of reference as follows:

a) Computer related crime is a growing problem in government as well as in the private sector.

b) Computer related crime occurs at great cost to the public, since losses for each incident of computer crime tend to be far greater than the losses associated with each incident of other white collar crime.

c) Opportunities ... are great

d) While various forms of computer crime might possibly be the subject of criminal charges based on other provisions of law, it is appropriate and desirable that a supplemental and additional statute be provided which proscribes various forms of computer abuse.

2) The United Kingdom Data Protection Act has as one of its eight data protection principles as follows:

> Appropriate security measures should be taken to forestall destruction of personal data and against accidental lose or destruction of data.
>
> Regard should be had to the nature of the personal data and the harm that would result from such access, alteration,

disclosure, loss or destruction as once mentioned in this principle and to the place where the personal data are stored, to security measures programmed into the relevant equipment and to measures taken for ensuring the reliability of staff having access to the data.

Lastly, security is a way of life.

REFERENCES

1 Allen, Brandt. *The Biggest Computer Frauds*
May 1977, The Journal of Accountancy 52

2 Anderson, R.J. *A Guide to Computer Control and Audit Guidelines* CA Magazine, December 1974

3 Beguai, August. *How to Prevent Computer Crime: A Guide for Managers* New York: John Wilcey & Sons Inc. 1983

4 Bloombecker, Jay J *Computer Crime, Computer Security, Computer Ethics* Edited by National Centre for Computer Crime Data, Los Angeles, 1986

5 Blue, R.E and G.E. Short *Computer System Security and Operational Experience* Redondo Beach, Calif. TRW Inc. March 1974

6 Bower, B.J; Schlosser, R.E., Nweman, M.S.
Computer Oriented Accounting Information Systems
South-Western Publishing Co. 1985

7 Carrol, J.M. *Computer Security*, Butterworths Publishers, 1987

8 *The Control of Computer-Based Fraud* Computers and Security 1 No. 2 1982

9 Carrol J.M. and P.G. Laurin *Software Protection for Microcomputers* Cryptologia 8 No.2 1984

10 Coopers and Lybrand *Taking Action to Help Deter Fraud*
Executive Alert October, 1983

11 Fitzgerald, Kevin J *The Computer Abuse Profile in Australia*
Edited by the Computer Abuse Research Bureau at C.I.T., Caulfield, Victoria, 1982

12 Harry, M *The Computer Underground* Townsend, Wash: Loompanics Unlimited, 1985

13 Hoffman, L.J. *Security and Privacy in Computer Systems*
Los Angeles; Melville, 1972

14 Keith Hearden (edited) *A Handbook of Computer Security*
Kogan Page, 1990

15 Krauss, L. *SAFE: Security Audit and Field Evaluation*
Amacom, 1973

16 Krauss, Leonard & Macgahan, Aileen *Computer Fraud and Countermeasures* Englewoods Cliffs/New York, 1979

17 Martin, J. *Security, Accuracy and Privacy in Computer Systems* Englewoods Cliffs N.J: Prentice Hall, 1973

18 Norman, Adrain R.D. *Computer Insecurity* London, 1983

19 Parker, Donn B. *Fighting Computer crime* New York, 1983

20 *Computer Abuse, Perpetators and Vulnerabilities of Computer Systerms* Stanford Research Institute, Menlo Park, Calif, 1975

21 Porter, Grover L (edited) *Safeguarding MIS Assets - A Management Responsibility* Management Accounting November, 1983

22 Schjolberg Stein, *Computer-assisted crime in Scandinavia* (1980) 2 Computer and Law Journal 457

23 Sieber, Ulrich, *The International Handbook on Computer Crime* 1986 John Wiley & Sons

24 Solar , Arthur, *Computer Technology and Computer Crime* Report No.8 of the Research and Development DIV, NCCP, Stockholm 1981

25 Statland, Norman *What You Should Know About Data Security* Price Waterhouse National Office

26 Taber, John K. *A Survey of Computer Crime Studies* (1980) 2 computer and Law Journal 275

27 Wong, Ken, *Computer Crime Casebook* BIS Applied Systems, Manchester, 1983

28 *Computer Related Fraud Casebook* BIS Applied Systems, Manchester, 1983

29 *The Hackers and Computer Crime* SECURICOM 1986 Congress Proceedings edited 1986 by SEDEP, Paris.