## NOTICE

The quality of this microform is heavily dependent upon the quality of the original thesis submitted for microfilming. Every effort has been made to ensure the highest quality of reproduction possible.

If pages are missing, contact the university which granted the degree.

Some pages may have indistinct print especially if the original pages were typed with a poor typewriter ribbon or if the university sent us an inferior photocopy.

Reproduction in full or in part of this microform is governed by the Canadian Copyright Act, R.S.C. 1970, c. C-30, and subsequent amendments.

## AVIS

La qualité de cette microforme dépend grandement de la qualité de la thèse soumise au microfilmage. Nous avons tout fait pour assurer une qualité supérieure de reproduction.

S'il manque des pages, veuillez communiquer avec l'université qui a conféré le grade.

La qualité d'impression de certaines pages peut laisser à désirer, surtout si les pages originales ont été dactylographiées à l'aide d'un ruban usé ou si l'université nous a fait parvenir une photocopie de qualité inférieure.

La reproduction, même partielle, de cette microforme est soumise à la Loi canadienne sur le droit d'auteur, SRC 1970, c. C-30, et ses amendements subséquents.

# THE NATURE OF COMPUTER-RELATED CRIME

by

George William Sittek

B.A. (Honours), University of Toronto, 1982

THESIS SUBMITTED IN PARTIAL FULFILLMENT OF

THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF ARTS (CRIMINOLOGY)

in the Department

of

Criminology



SIMON FRASER UNIVERSITY

ISBN 0-315-48881-6

PARTIAL COPYRIGHT LICENSE

I hereby grant to Simon Fraser University the right to lend my thesis, project or extended essay (the title of which is shown below) to users of the Simon Fraser University Library, and to make partial or single copies only for such users or in response to a request from the library of any other university, or other educational institution, on its own behalf or for one of its users. I further agree that permission for multiple copying of this work for scholarly purposes may be granted by me or the Dean of Graduate Studies. It is understood that copying or publication of this work for financial gain shall not be allowed without my written permission.

Title of Thesis/~~Project/Extended Essay~~

The Nature of Computer-Related Crime

Author:

(signature)

George William SITTEK

(name)

April 6, 1988

(date)

## ABSTRACT

The primary objectives of the thesis are threefold: 1) to present a descriptive analysis of computer-related crime which will facilitate a general appreciation of this form of criminality; 2) to propose an exploratory research design which will provide a framework for the collection and organization of data; and 3) to identify avenues for future research in the area of computer-related crime.

Proceeding from a general examination of the topic, three variables are identified for indepth analysis. A major area selected for research, concerns the level of technical skill and knowledge required for the commission of computer-related crimes. This variable is discussed as it relates to five crime classifications, each necessitating different levels of technical proficiency. The thesis then progresses to a consideration of the motivational and opportunity factors which can influence an individual's decision to engage in computer-related crime. Both variables are described in terms of the psychological and environmental conditions which may facilitate the criminality.

The combination of these variables forms the basis for the conceptualization of an exploratory research design that is intended to provide an organized methodology for data collection. Contained throughout the thesis are numerous case examples of computer-related crime which are used to document and clarify the analysis of the major descriptive variables. As a source of "raw

data", the cases serve to illustrate the utility of the research design for data organization. The resultant quantitative analysis is used to present one possible measurement strategy for future research efforts.

# DEDICATION

To my Parents,

for unwavering love and support.

## ACKNOWLEDGEMENTS

A special acknowledgement goes to the members of my thesis committee, who demonstrated great patience during the final stages of this thesis. They not only contributed valuable insights into the nature of the research, but they also provided a great deal of moral support which enabled me to see the project through to completion. Another special acknowledgement is to Mrs. Sams, who assisted me greatly throughout the graduate program, without her help I would have been struggling to stay above the red tape.

To Kathy Lumsden, I wish to express my deep feeling of love for her understanding during those long nights while I was tapping away on the computer. Not only did she contribute many hours of her time to proof-read this thesis, she did so without concern to her own obligations. To Dustin and Kyle, two guys who have given me a focus for future growth and prosperity, their company has provided me with countless hours of enjoyment.

To my Mom, Dad, and Brother, I also wish to express my deep feeling of love, without their help this thesis would never have been completed. Their moral and financial support was a vital life-line when I was in a time of need.

I also wish to acknowledge the sincere friendship of Andy Higgins, who only has my prosperity at heart. He has

accepted my idiosyncracies as a natural consequence of the difficulties involved in completing the last draft of this thesis. Andy provided the necessary diversions to make life a little more enjoyable during the final stages of the thesis, and for his companionship and technical assistance I will always be grateful.

Lastly, to Clay Mosher, who endured endless hours of rambling on computer-related crime without complaint or apparent discomfort. Our occasional forays into the Hart House Pub to consume a couple of "cold ones" was an idealic setting for academic discussion and provided many ideas which were eventually incorporated within the thesis. His contributions both directly and indirectly are greatly appreciated and acknowledged.

## TABLE OF CONTENTS

## LIST OF TABLES

# LIST OF FIGURES

# I. Introduction

The first computer-related crime to be federally prosecuted in the United States occurred in Minneapolis in 1966 (Parker, 1976: x). An employee of the National City Bank programmed the computerized checking system to ignore $1,357 in overdrafts to his account. The crime was discovered when the bank was forced to revert back to its manual processing system due to a computer failure (Taber, 1980: 298). The following day the Minneapolis Tribune printed the story on the front page with the intriguing headline: "Computer Expert Accused of Fixing His Bank Balance" (Parker, 1976: x). Subsequent media reporting of the case stimulated heightened interest in the area of computer-related crime which eventually gave rise to a host of contradictory research studies.

In 1973, the Stanford Research Institute (SRI) initiated a series of studies on "computer abuse" which resulted in three influential reports to the U.S. National Science Foundation. As noted by Taber (1980: 288), the primary objective of all the SRI studies was to illustrate the potential threat to society of "the sophisticated computer crime: one committed by an unscrupulous but highly skilled technologist". This orientation provoked an alarmist trend which characterized future studies, leading the United States Department of Justice (1980: 11) to conclude: "the problem [computer-related crime] has reached serious proportions and is growing worse". Based upon a sample of 375 cases, the SRI

published, what were to become, the three most widely cited statistics concerning computer-related crime: 1) a total annual worldwide loss of $300 million; 2) an average loss per incident of $450,000; and 3) only 15% of known cases are ever reported (Parker, 1976: 29-30). The enormous loss projections made by the SRI were uncritically accepted and reaffirmed by other authors (e.g., Bequai (1978), Dentay (1980), and Swanson and Territo (1980)), who further advanced misconceptions concerning the incidence of computer-related crime.

In an attempt to compile a more accurate statistical profile on the extent of computer-related crime in U.S. government programs, the General Accounting Office (GAO) conducted a major study in 1976. With the assistance of ten Federal investigative agencies, an extensive file search was performed, which resulted in 69 verified cases. Total losses were estimated at $2.2 million, with an average loss per incident of $44,000, one-tenth what had been reported previously (Taber, 1980: 282). According to Sokolik (1980: 314): "The GAO characterized most of the crimes studied as relatively unsophisticated requiring only limited technical knowledge", directly contradicting what the SRI portrayed.

With similar objectives to that of the GAO study, the Ontario Provincial Police (OPP) completed an extensive "Computer Crime and Security Survey" in 1981 which was directed toward Ontario's business sector. The study surveyed 648 corporations and received 321 responses, only 13 of which reported a loss through some form of computer-related crime (Webber, 1983: 222).

Further analysis of the 13 cases revealed that five had been reported to the police, and only three had been recommended for prosecution (Canada. House of Commons, 1983: 18: 13). Commenting on the results of the OPP survey, the House of Commons Sub-Committee on Computer Crime notes: "There is very little empirical data which clearly demonstrate that computer crime poses a serious problem" (Canada. House of Commons, 1983: 18:13).

The controversy concerning the nature and extent of computer-related crime is only one area of contention which has confounded research efforts. The "computer criminal" has likewise, been the subject of conflicting analysis. Parker (1976; 1976b; 1980; 1983) has had the most influence on the way other authors have come to view the computer-related crime offender. Krauss and MacGahan (1979: 39) state that: "developed findings from his work... tie in quite well with the characteristics of the modern day embezzler", and include the following attributes:

- Perpetrators are young (average age is 29, median age is 25, range is 18 - 46);
- management and professional skills are predominant (70% were managers or highly experienced technical professionals; and
- violation of occupational trust was evident in 65% of the cases (Krauss & MacGahan, 1979: 39).

These statistics were compiled from a rather limited population of 17 known computer-related crime offenders (Parker, 1976b: 13). As Sokolik (1980) notes, the application of such general characteristics to the entire population of computer-related crime offenders can be questionable:

> Where some authorities speak of the 'computer criminal' in a manner which implies a uniformity of personal characteristics and background, most contend that there is only a broad outline which serves principally to distinguish the users of computers in crime from more traditional criminals (Sokolik, 1980: 365-366).

Even though little consensus exists concerning the statistical profile of "computer crime" or the attributes which best characterize the "computer crimimal", most researchers would agree that, it is an area of criminology which deserves greater academic attention.

Research Objectives:

The primary objective of this thesis is to describe computer-related crime in relation to variables which will facilitate a general appreciation of this form of criminality (Chapters II-IV). The three descriptive variables selected for study: 1) technical skill and knowledge; 2) motivation; and 3) opportunity; are examined according to research indicators which take into consideration basic computer-related crime concepts. Initial observations derived from this descriptive analysis provide a foundation for the conceptualization of an exploratory research design which incorporates white-collar crime theory (Chapter V).

The purpose of proposing an exploratory research design is to enhance the scope of future research by providing a framework for the collection and organization of cases for statistical observation. The need for such a design is clearly stated by the incongruous conclusions drawn by the House of

Commons Sub-Committee on Computer Crime (1983) concerning the necessity for legislative action to combat this form of criminality:

> A comprehensive study has never been undertaken in Canada to estimate the occurrance rate and we do not feel that one is necessary at this time. In our opinion, the fact that relatively little is known about the incidence and seriousness of computer crime is not a justification for legislative complacency. We must still have regard for the potential harm to society. Legislative action is needed to proscribe crimes and deter offenders (Canada. House of Commons, 1983: 18, 14).

This reactionist orientation is puzzling in light of the relatively few actual cases of computer-related crime reported in Canada. The Sub-Committee's observations are, however, an accurate reflection of the present state of computer-related crime research, and provide little insight into the nature or extent of this form of criminality. Commenting on the Sub-Committee's findings, Webber (1983) notes the absence of reliable statistics to support the opinion that computer-related crime constitutes a "potential harm" to society:

> To paraphrase the subcommittee's views would result as follows: `We do not know how much computer crime there is nor how serious it is; none the less, we intend to create criminal sanctions to deter it'. One might query that, if the incidence rate and seriousness of the subject-matter are not known, then how might the legislators determine the `potential harm' so to tailor the Criminal Code to protect society?... we must assume that law reform in Canada is not based solely on views and opinions but, rather, is founded on in-depth study and analysis of the most appropriate approach to reconcile the problem. Unfortunately, the subcommittee makes no mention of the analytic

> tools used to reach the conclusion that even harmless `trespassers' who penetrate someone else's system without the intention of altering or destroying data should be subject to criminal sanctions (Webber, 1983: 244-246).

Such dissenting views indicate that computer-related crime has not yet been adequately addressed in relation to a research design which can provide a mechanism for statistical observation. As the second objective of this thesis, the development of an "appropriate approach" to measure the nature of computer-related crime is an important first step in the appraisal of this form of criminality.

The last objective of this thesis is to identify possible avenues for future research, based upon the application of the proposed design (Chapter V). A number of different areas of interest (e.g., computer system vulnerabilities, victimization, etc.) may be examined in relation to the four research indicators providing enhanced capabilities to determine the quality of this form of crime. The perspective taken in this thesis is directed toward a "field" orientation which will enable practioners to collect and examine cases according to a number of different research questions; while still retaining a measure of proportion to the totality of cases collected for analysis.

**The Research Design:**

Based upon the observations of Quinney (1964) concerning the nature of white-collar crime, a basis for **content analysis**

is identified. Expanding upon his concepts of crime and deviation occurring within the occupational environment, the enhanced design includes situational violations. Such types of crime and deviation originate "outside" of the occupational setting and are often committed without the application of occupational knowledge. Because computer-related crime, is not necessarily restricted to, or a function of occupational activity, the inclusion of situational violations within the research design greatly increases the researchers ability to examine the general nature of this form of criminality.

The basic structure of the design is comprised of two conceptual variables which have been extrapolated from the descriptive analysis of motivation and opportunity presented in Chapter IV. Combining the two variables results in four research indicators which are used to organize cases according to major categories. The progression from conceptualization to operationalization principally concerns the selection of indicators which best characterize the variables under study, and stating them in terms which permit observation. In respect to content analysis, such indicators represent the operational definitions by which a coding scheme is devised. Based upon this research design a number of other variables may be examined in relation to the original data base.

To illustrate the utility of the design for data collection and organization a content analysis is performed on a limited sample of cases. As a basis for case selection the three criminological definitions which will be described in Chapter II

are used as a criteria for defining the units of analysis. A simple sampling strategy is employed in the selection of the 40 examples of computer-related crime contained in the case study. Based upon the definition of "computer-related crime", each case presented within this thesis is assessed according to a demonstration of technical skill and knowledge. Cases which fulfill this definitional requirement are selected for analysis. Such a strategy is often called "purposive" or "judgmental" sampling, and the selection of cases for study is founded upon the researcher's knowledge of the population under study (Babbie, 1979: 195). Since the case examples are described throughout the thesis a technique was identified which could be used to organize them for the content analysis. Each of the 40 examples of computer-related crime included in the case study presented in Chapter V are footnoted and assigned a case number (e.g., CRC-01), which are referenced for clear identification. This method of case organization not only enables the reader to appreciate the quality of the case in the context in which it is presented, but it also provides an effective cross-reference technique for the content analysis. The following three sections of this Chapter will detail the strategy taken in the literature review, the analysis of documents, and possible future theoretical considerations of the research.

**A. The Research Approach: Literature Review**

As noted by Cooper (1984: 12-14) the research review contains five basic stages of social scientific inquiry: 1) the problem

formulation stage; 2) the data collection stage; 3) the data evaluation stage; 4) the analysis and interpretation stage; and 5) the public presentation stage.[1] In association with these stages of inquiry, the researcher must identify the research channels which will assist in the review of the relevant literature. Cooper (1984) presents three possible research channels which may be used in the review: 1) informal research channels; 2) primary research channels; and 3) secondary research channels.

---

[1] Cooper (1984) describes the processes directing these research stages as follows:

**the problem formulation stage.** During problem formulation, the variables involved in the inquiry are given both abstract and concrete definitions. At this stage the researcher asks: `What operations are relevant to the concepts that concern the review?' More broadly, the researcher must decide what distinguishes relevant from irrelevant material (Cooper 1984: 12).

**the data collection stage.** The data collection stage of research involves making a choice about the population of elements that will be the focus of the study. Identifying populations for research reviews is complicated by the fact that the reviewer wants to make inferences about two targets. First, the reviewer wants the cumulative result of the review to be based on all previous research on the problem. Second, the reviewer hopes that the included studies will allow generalizations to the population of individuals (or other units) that are the focus of the topic area (Cooper, 1984: 14).

**the data evaluation stage.** After data are collected, the inquirer makes critical judgments about the quality of individual data points. Each data point is examined in light of surrounding evidence to determine whether it is contaminated by factors irrelevant to the problem under consideration (Cooper, 1984: 14).

**the analysis and interpretation stage.** During analysis and interpretation, the separate data points collected by the inquirer are synthesized into a unified statement about the research problem. Interpretation demands that the inquirer distinguish systematic data patterns from `noise' or chance fluctuation (Cooper, 1984: 14).

**the public presentation stage.** Creating a public document that describes the review is the task that completes a research endeavor (Cooper, 1984: 14).

## Informal Research Channels

Informal research channels are often used in literature reviews because of their ease of location and accessibility to the researcher. One source of informal communications has been termed the "invisible college" and includes the researcher's association with others who are engaged in similar research (Cooper, 1984: 39). Through correspondence and the exchange of revelant literature the researcher is kept informed of the state of current studies. Such colleges are based upon a small group of influential members with less prominent members contributing from the outside of the close group. Cooper (1984: 39) notes the obvious bias which may result from such associations: "information from an invisible college is probably more uniformly supportive of the findings of the central researchers than evidence based on more diverse sources". Another informal research channel includes the researcher's participation in professional societies and interest groups which provides access to information relevant to specific areas of study (Cooper, 1984: 39-40). Once again the bias is that such information may be selectively incorporated into the researcher's own study.

## Primary Research Channels

Primary research channels will usually include the researcher's own personal libraries of a particular subject and may be comprised of a wide array of different information sources

such as, scholarly books, journals, and other forms of academic publication. Using these sources of information as a primary channel, the researcher can then retrieve previously cited information which may be relevant to the area of study. This reference-tracking technique has been termed the ancestry approach, which essentially entails the search of citations and bibliographies (Cooper, 1984: 41). As Cooper (1984: 42) points out, a major problem facing researchers who employ this approach is that it often "introduces bias by overrepresenting the paradigms and results that are contained in the reviewer's chosen journal network reference group".

## Secondary Research Channels

Secondary research channels probably present the least amount of bias when conducting a literature review, since the information is obtained from all publicly available research (Cooper, 1984: 42). Sources include, published bibliographies[2] and indexing and abstracting services[3] which provide the researcher with little restriction as to the types of studies under review. Cooper (1984: 42) maintains that such channels

---

[2] The Natural Research Council Research Information Service publishes a bibliography of bibliographies in psychology which lists over 2,000 bibliographies (Cooper, 1984: 43).

[3] An index or abstracting service will focus on a certain discipline or topic area and define its scope to be an explicit number of primary publication outlets. Each article that appears in the primary outlets will then be referenced in the system (Cooper, 1984: 43).

"should form the backbone of any systematic, comprehensive literature search". While biases may exist in the researcher's selection of material from the bibliographies and abstracting services, the biases contained within informal and primary research channels are greatly reduced.

The method employed to conduct the literature review for the thesis comprised a combination of secondary and primary research channels. First, a computerized abstracting service (secondary channel) was used to determine the extent of information available on computer-related crime. Criminological abstracts were queried on key terms such as, computer crime, computer-related crime, computer abuse, and technological crime. After a listing of the relevant literature was obtained it was reviewed and a further listing of literature was derived from a search of citations and bibliographies (primary channel). Because computer-related crime has only been recently addressed in the related literature the sample of articles, books and journals was relatively limited in scope, yielding a possibly biased representation of research stimulated by the original studies conducted by the Stanford Research Institute (this problem is typically associated with the ancestry approach). The review of the available literature not only provided the foundation for the examination of the three descriptive varables of analysis, but also a sample of cases which were used for the content analysis.

## B. Content Analysis of Documents

Applying the methods mentioned above the literature was scanned for all cases involving computer-related crime and indexed for the case study. As noted earlier cases meeting the definitional requirements for the content analysis were selected, while the others were excluded from the analysis. The cases included within the thesis were primarily used to clarify and document the descriptive variables of analysis, however, their utility was also demonstrated for the content analysis of documents.

It should be acknowledged at this point that many of the cases cited throughout the thesis represent "images" within documents and may only be reflections of reality. How such images are portrayed in the related literature can greatly impact our perceptions of crime and deviance and should be viewed with a measure of caution. As noted by Sutherland (1950: 143) in his examination of sexual psychopath laws, such images are often maintained "after a state of fear has been aroused in a community"; which may lead to the enactment of "dangerous and futile laws". In his analysis of the diffusion of sexual psychopath laws, Sutherland states:

> Implicit in these laws is a series of propositions which have been made explicit in an extensive popular literature, namely, that the present danger to women and children from serious sex crimes is very great, for the number of sex crimes is large

> and is increasing more rapidly than any other crime; that most sex crimes are committed by `sexual degenerates', `sex fiends', or `sexual psychopaths' and that these persons persist in their sexual crimes throughout life; that they always give warning that they are dangerous by first committing minor offences; that any psychiatrist can diagnose them with a high degree of precision at an early age, before they have committed serious sex crimes; and that sexual psychopaths who are diagnosed and identified should be confined as iresponsible persons until they are pronounced by psychiatrists to be completely and permanently cured of their malady (Sutherland, 1950: 142).

Similar types of propositions have been made concerning other forms of criminality. For example, in her book The Black Candle, Emily Murphy (1922) describes in lurid detail the evils which will befall men who partake in the pleasures of opium. As noted by Solomon who wrote the introduction to her book:

> Her research was irrevocably tainted by her strict personal morality and was specifically writen in a biased, sensationalist fashion to arouse an apathetic Canadian populace... Of equal importance was Mrs. Murphy's impact on the public's perception of drug use and users. She created a series of women-seductive villains, primarily non-white and non-Christan, who threatened the Anglo-Saxon way of life. Driven to insanity and crime by hopeless addicition, these cunning `dregs of humanity' more than deserved the harshest penalties. All prohibited drugs were addicitive poisons which destroyed the body and the inhibitions of a good Christan upbringing. Although her more outrageous claims have been dismissed, many of her erroneous assumptions are still accepted by segments of the Canadian public (Murphy, 1922: 2-3).

Considering the historical context by which perceptions of criminality may be shaped, it is important to recognize the impact such studies can have on future research efforts. The

portrayal of criminal cases in a sensationalist or dramatic manner is sure to arouse public interest, often at the expense of academic creditability The pioneering studies conducted by the Stanford Research Institute have greatly influenced the manner in which other authors view computer-related crime and have provided many of the cases presented within the thesis. In this respect, the "images" (cases) presented in the thesis may not neccessarily reflect an accurate picture of reality. While their utility as descriptive examples of computer-related crime have assisted in the examination of the three major variables of analysis, they cannot be deemed representative of all computer-related crimes. The content analysis of documents was expressly used to demonstrate the applicability of the research design for future studies, not to provide generalizations concerning computer-related crime.

C. Theoretical Considerations

When examining any aspect of criminal activity, two possibilities exist for theoretical speculation. First, the researcher may wish to gather facts then generalize to theory (inductive reasoning); or may wish to apply a theory to a particular set of facts (deductive reasoning). Each mode of reasoning provides the researcher with a mechanism by which to incorporate theoretical considerations into a study. For the stated objectives of the thesis an inductive reasoning approach was applied, where facts and observations were complied which

could then be generalized to theory. While a number of theoretical aspects of computer-related crime are discussed throughtout the thesis, no one distinctive theory was adopted as a foundation for the following analysis, although a number of possibilities are considered in the conclusion to the thesis. Before the basic objectives of the thesis can be addressed, it is first necessary to acquire an initial appreciation of the topic under study. The next Chapter will be directed toward a general examination of computer-related crime concepts including: 1) an analysis of criminological definitions; and 2) an overview of crime characteristics.

## II. Computer-Related Crime Concepts

### A. Computer Crime Defined

Computer crime, computer-related crime, computer abuse, and computer fraud are commonly used terms which are used to describe a form of technological crime. In order to intelligibly distinguish the many different concepts expressed by the term 'computer crime', it is necessary to organize them into clearly identifiable categories. In many instances, researchers have used these concepts interchangeably, which has led to inconsistency not only in interpretation but also in application.

Determining what constitutes 'computer crime' as opposed to 'computer-related crime' or 'computer abuse' has until recently been based upon criminological concepts, rather than on criminal statute. McNiff (1982) comments on the difficulties involved when attempting to define 'computer crime' in legal terms; he states:

> There are two important distinctions here, the first being the distinction between crime and abuse. In a generic sense the words are, and can be, used interchangeably unless precision in respect to criminal illegality is, as it is here, in issue. When the primary orientation is the proscriptive definition of a particular criminal system, computer 'crime' becomes a highly technical term. On the other hand, other discussions can utilize the terms loosely or, in preference, the word 'abuse' can be equated with the sociologists' use of the term 'deviance' to avoid the definitional problems of 'crime'. The second important distinction [concerns] the difference between

> crime against the computer (a target) and crime by computer (a tool). The dichotomy of computer targeted and facilitated offences is not mutually exclusive. By way of example, manipulation of software may be done in order to obtain control of an external asset - crime by computer - but may also be an offence in itself, despite the intention that the abuse be incidental to, or simply a means to, the gain of the ultimate asset (McNiff, 1982: 5).

McNiff's comments are valuable in pointing out the problems which can result when attempting to apply legal conditions to a form of activity that is still relatively obscure. More importantly, McNiff notes the distinction between 'crime by the computer' and 'crime against the computer'; this aspect is a primary element in the process of identifying those conditions which can be used in the assessment of criminological definitions.

Because 'computer crime' has only just been addressed by legislation, criminologists are still relying upon criminological characteristics for analysis. These characteristics have become the conceptual bases by which crime and abuse have been distinguished, and effectively lend themselves to criminological research.

## Criminological Definitions

In describing computer crime in criminological terms, every effort should be made at variable specification, which would greatly increase the research utility of the concept. In this respect, a number of authors have proposed different definitions

of computer crime, all of which have revolved around similar terms, but have not adequately addressed its fundamental elements.

For instance, Penrose (1979) proposes a definition of computer-related crime in which he indicates what activities computer-related crimes should incorporate, but goes no further. His definition reads:

> Computer-related crime can be said to cater for any unlawful act in which a computer is used. Perhaps the definition should be contained to those allegations involving either some falsification of input and/or unauthorized program change or other manipulation by electronic data personnel rather than the falsification of source documentation by persons unconnected with the computer, which, because of the system of operation, in turn gives rise to computer input documents (Penrose, 1979: 13).

A similar type of definition, although aimed at a different concept, was proposed by Carroll (1977):

> [computer crime can be 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 the EDP system, negotiable instruments stored or created at the facility, and critical resources required by the EDP system to render service (Carroll, 1977: 15).

As illustrated in both of these definitions, there appears to be an abundance of extraneous information, such as the

delineation of types of computer crimes and types of losses. These aspects tend to obstruct the basis upon which definitions should be formulated, that is, the identification of features which would characterize the hierarchical nature of computer-related crimes with respect to the computer's involvement in the commission of crime.

The three definitions proposed by Parker (1980) have proven to be effective in covering the range of criminological concepts. Distinctions between these definitions are based upon: the extent of involvement of the computer in the commission of the crime; and the level of technical skill and knowledge demonstrated by the offender. Each definition will be examined in relation to a specific form of computer-related crime clasification: physical acts. This class of violation generally involves the physical destruction of computer-related resources.

i. Computer Crime

> True computer crime implies direct involvement of computers in committing a crime (United States Department of Justice, 1980: 3).

This definition assumes the highest level of restriction regarding the types of offences which may be included under the concept. It requires that the computer be used directly as the primary tool in the commission of the offence. Such crimes often involve sophisticated techniques not witnessed under other definitions.

Dentay (1980) describes a case of true computer crime which he considers "poetically just". It concerned a promise made to a programmer that, if he developed a successful personnel-function program for a large corporation, he would be hired for a permanent position after his one-year contract expired. The corporation received the program, but denied making such a promise to the programmer. After his contract ended, he was released from his occupational duties (Dentay, 1980: 44).

Unknown to corporate officials, the programmer had anticipated such an action and inserted a 'logic bomb' into the program he had developed which would destroy the program at the issue of his final pay cheque. At the bottom of the programmer's cheque appeared an eloquent, yet simple statement of fact: Final Pay: Program Terminated (Dentay, 1980: 44). This particular case illustrates a true computer crime in the strictest sense of the concept. Not only did the programmer use the computer as the primary tool for the destruction of the program, but he also used extensive technical skill and knowledge in inserting the logic bomb which is one of the more advanced computer-related crime techniques.[1]

ii. Computer-Related Crime

> Computer-related crime is any illegal act for which knowledge of computer technology is essential for successful prosecution (Parker, 1980: 334-335).

---

[1] Case number CRC-01: see Chapter V.

Computer-related crime can be distinguished from true computer crime by the fact that the computer does not necessarily have to be used directly in the commission of the offence. This definition is probably the most adaptable for criminological research purposes, since it does not limit investigation to those offences which involve the computer as the primary tool. Yet it excludes crimes which are questionable or only superficially computer-related.[2]

An example of a computer-related crime which also involved a destructive attack is described by Carroll (1977). The offence occurred in Denver in 1972 where a computer operator was arrested for repeatedly short-circuiting a computer disk drive with a screwdriver. His actions caused extensive downtime of the computer system, which subsequently cost his employer about $500,000 over a two-year period trying to locate the recurring trouble. When asked the purpose of his activities, the operator claimed he had an overpowering urge to shut down the computer (Carroll, 1977: 18-19).[3] This offence may not be classified as a true computer crime, since the computer was not used as the instrument of the crime. However, it may be considered a computer-related crime since the perpetrator demonstrated adequate technical skill by attacking a specific component of the computer system which allowed him to escape detection for a two-

---

2 The term computer-related crime will be used throughout this thesis to denote all forms of criminal conduct involving computers.

3 Case number CRC-02: see Chapter V.

year period. The computer served as the object of attack rather than the instrument of attack, and thus played a passive role in the commission of the crime. It is this aspect of computer involvement which distinguishes computer-related crime from true computer crime.

iii. Computer Abuse

> Computer abuse is any intentional act involving a computer where one or more perpetrators made or could have made gain and one or more victims suffered or could have suffered a loss (Parker, 1980: 333).

The parameters of this definition are the least restrictive for the types of offences which may be included under the concept. The definition specifies that the offence must involve a computer and that it must be intentional, but no mention is made of the fundamental elements witnessed under the other two definitions. Computer abuses can, therefore, span the complete range of offences involving computers, incorporating all true computer crimes as well as all computer-related crimes. Since the variables of this definition are not specific, little concrete analysis is required in determining the computer's role in the commission of the crime. Parker (1980) maintains that this particular definition is the most applicable for research purposes since it "relates to computers in the most general way possible", which he feels best serves in the "exploratory selection and collection of

unanticipated types of cases" (Parker, 1980: 333).[4] Bequai (1978) considers such definitional problems:

> If a computer is stolen in a simple theft where based on all circumstances it could have been a washing machine or a milking machine and made no difference, then a knowledge of computer technology is not necessary, and it would not be a computer-related crime (Bequai, 1978: 2-3).

Bequai's comments are valid in light of the fundamental elements identified in the other two definitions. However, they still leave much room for speculation regarding the fine line which distinguishes computer-related crimes from computer abuses. For example, a Canadian case illustrates the problems which may arise when attempting to classify offences according to these definitional categories.

Sir George Williams University in Montreal was the scene of a large student riot. The students occupied the university's EDP computer center for two weeks before setting fire to a $1.6 million computer (Carroll, 1977: 16). The offence was obviously intentional and it involved a computer, quite clearly a

---

4 As noted by Parker (1980), the objective of using this definition is to encompass as many different types of cases as possible for analysis. Parker (1980: 333) maintains that this particular definition is the most applicable for research purposes since it "relates to computers in the most general way possible". What Parker may have failed to consider when making this statement is that along with the collection of unanticipated types of cases, many irrelevant cases may also be included, further clouding the issue of variable identification. While "computer abuse" cases assist in the descriptive analysis of violations which may encompass the exploitation of computer technology, they do not demonstrate a sufficient application of technical skill and knowledge to be considered for analysis. For this reason, cases involving simple forms of physical destruction or theft are excluded from the case study presented in Chapter V.

computer abuse. But, depending upon the circumstances, it may be considered a computer-related crime if a number of assumptions can be made: first, that the students appreciated the possible losses the university might accrue with the destruction of the computer; second, that the students used the threat of destruction as a tool to achieve their objectives; and last and most important, that the students selectively discriminated between valuable property and property which was only incidental to the proper functioning of the computer system.

Based upon these assumptions, this particular offence may be considered computer-related, if technical knowledge was necessary for the students to appreciate the nature of their actions with respect to their original objectives. By reviewing the facts of the case, it seems that the students were intent upon disrupting the normal functioning of the university by physically destroying the facilities. It is not evident that the students possessed the necessary technical capability to do so in a selective manner, which would have greatly increased their relative power over the system while, at the same time, still presenting their 'cause' to the university authorities (Reid & Reid, 1969: 42). Similar to the methods employed by the students, terrorists also rely upon physical acts to demonstrate their cause. However, unlike the students they generally control the system through technical knowledge (e.g., selective destruction which inflicts maximum disruption to computer service). Thus, the 'action' taken by the students must be considered a computer abuse even though it involved a traditional form of crime.

## B. Characteristics of Computer-Related Crime

Computers possess numerous elements which allow them to fulfill a myriad of different functions, including criminal activities. Because of the diversity of criminality possible through the manipulation of computer technology, computers have been used for a number of different criminal roles. Such roles are, to a large extent, dependent upon the specific criminal application for which the computer will be used and, in this respect, often revolve around two unique characteristics which distinguish this form of criminality from other types of white-collar crime.

### i. Four Roles Computers Play in the Commission of Crime

Computers can serve as the object, the instrument, the subject or the symbol of criminal activities. Each role is distinguished from the other by specific environmental conditions which determine the computer's involvement in the commission of a crime.

#### Computer as Object

The computer may be considered the object of crime if physical destruction of the computer, or any hardware or software utilities associated with the proper functioning of the computer, are the goals of the perpetrator (Parker, 1976: 17). These

types of crimes are easily prosecuted under traditional statutes, since physical destruction is blatantly apparent. Computer-related crime techniques used in such offences include: physical damage, storage media damage, logical damage, and communication damage.[5] The majority of these crimes concern some form of destructive activity directed against corporations by disgruntled and fired employees, or terrorist groups wishing to demonstrate their grievance (Carroll, 1977: 29). However, the more interesting types of cases involve the destruction or theft of computer facilities by competing corporations. For example, in 1975, a computer parts manufacturer in Santa Monica charged a competitor with hiring an arsonist to set fire to his facilities, disrupting production and destroying complete inventories (Carroll, 1977: 16). Such crimes aptly illustrate the extensive pressure which can result in criminal activity when corporations bid for contracts in a lucrative market.

Computerized data stored on magnetic tapes and disks or printouts of valuable trade information can also serve as the objects of crime when they are stolen and held for ransom for their market value. In such cases, other computer-related crime techniques may be used in the appropriation of the data, such as: scavenging, piggybacking, impersonation, data leakage, and wiretapping. In one case, a computer operations supervisor who

---

[5] The computer-related crime techniques which are mentioned throughout this chapter (e.g., **scavenging, piggybacking, impersonation, data leakage, wiretapping, trojan horse, salami techniques, asynchronous attacks, simulation methods, and system hacking**), will be more fully described in Chapter III.

was employed in a large data processing facility in Rozenburg, Netherlands, stole and held 594 tapes and 48 disks for a ransom of 275,000 pounds sterling, after he was fired from his job (Carroll, 1977: 19). The scope of technical skill and knowledge used in such offences can range from relatively simple schemes to highly complicated hardware and software manipulations, depending upon the nature of the information and the extent of security maintained by the computer facility.

### Computer as Instrument

This category requires that the computer be used directly in the commission of the crime so that the offence could not occur without the assistance of a computer. Many researchers (MacIntosh, 1983; Taber, 1980) consider this aspect of computer involvement the only true form of 'computer crime', since such offences involve complex software manipulations which require extensive specialized knowledge and skills (United States Department of Justice, 1979: 4). Crime techniques used in this type of offence include: the trojan horse, salami techniques, asynchronous attacks, simulation methods and hacking techniques. The majority of these techniques will be used in sophisticated financial schemes which may include the embezzlement of business assets through program manipulation. For example, deliberate misposting with lapping is an effective program manipulation technique which can be initiated in any accounting program that controls the recurrent payment of funds (Krauss & MacGahan, 1979: 81).

The accounting program must be modified to cause a misposting which either fails to apply a charge to the programmer's account (the charge is applied to another account), or credits the programmer's account with a payment (the account which should have been credited is not posted). This process of deliberate misposting is accomplished with a technique called 'lapping', which requires precise time management. The program is altered to modify only those accounts specified by the programmer, and are misposted at regular intervals to demonstrate identical modification. If the programmer fails to lap the accounts (make sure they sustain continual modification) he/she is at risk of audit detection, since the discrepancy in the original account and that of the next misposting will appear in the next legitimate transaction (Krauss & MacGahan, 1979: 81-82).

The computer can also be used as the instrument of crime when program code is modified which will execute a series of unauthorized instructions at a specific time (time bombs), or when certain conditions are established in the target file (logic bombs). The level of technical skill and knowledge used in such offences can be very sophisticated, and as a result, few actual cases of computers being used as the instrument of crime have been reported, although there is much speculation about the extent of such activities (MacIntosh, 1983).

**Computer as Subject**

In this category, a computer can serve as the site or environment where unique forms of assets can be created which are

subject to illicit gain (Parker, 1980: 333). The rapid processing capabilities afforded by computer technology can lead to the development of schemes which would not normally be possible under manual manipulation techniques. Input manipulation methods are the prevalent techniques used in such schemes, although some program modification schemes have been reported (Parker, 1976: 19). To illustrate the computer's role as the subject of crime, two schemes will be described.

The first case occurred in 1975, where a group of students at the California Institute of Technology programmed the university's IBM mainframe computer to create 1.2 million entry blanks in a sweepstakes sponsored by the McDonald's Corporation (Carroll, 1977: 35). The students eventually possessed 33% of the total entries and won almost every major prize and the majority of the smaller prizes (Ball, 1982: 25). The computer's rapid power of creation enabled the students to acquire assets which normally would have been impossible to obtain through manual manipulation methods. The only questionable activity the students engaged in was the fraudulent use of the university's computer system, for which they were subsequently disciplined.[6]

The second case also involved the creation of a unique form of asset which could be provided only in a computer environment. It concerned a computer operator who registered winning tickets at a Florida greyhound racetrack (Taber, 1980: 298). The operator

---

[6] Case Number CRC-03: see Chapter V.

capitalized on the time delay between when the tickets were recorded and when the winning payoff was made public (Ball, 1982: 25). His primary target was the "trifecta" races which required bettors to pick the exact order of the top three dogs. The payoff was usually high, with thousands of dollars at stake in each race. At the beginning of each day, the operator would calculate which race would provide the greatest rewards; he would wait for the race to be run, then fraudulently record in the track's computer that several more winning tickets had been sold. Since the computerized selling machines were not inspected until the end of the day, the operator could punch in the winning sequences and obtain the ticket stubs which he gave to an accomplice to cash (Ball, 1982: 25). The case demonstrates the capabilities of computers being used as the site or environment of crime[7] where unique forms of assets can be created.

Computer as Symbol

In this category, the computer is used to create records and transactions which, at face value, appear legitimate, but are, in fact, fraudulently created (United States Department of Justice, 1980: 7). This category utilizes many of the same crime techniques noted under "computer as subject", but can be theoretically separated from the latter by the fact that the

---

[7] Case number CRC-04: see Chapter V.

manipulated records themselves do not necessarily represent immediately exploitable assets. When these records are presented to potential victims, they serve to intimidate or deceive them into parting with something of value (Parker, 1980: 334).

One of the greatest corporate frauds in American history involved the use of computer-generated print-outs to defraud the public of an estimated $2 billion (Bequai, 1978: 64). The Equity Funding Corporation of America was one of the largest insurance firms in the U. S. until it ran into serious financial difficulties and had to fraudulently create 60,000 of the 90,000 policies which it held. Gleeson Payne, the California State Insurance Commissioner, notes:

> This massive fraud was particularly a crime of the computer. The computer was the key to the fraud... The insurance industry assumed computers were always accurate; computer fraud wasn't expected (Canada, 1976: 16)

Because the print-outs of policy holders were handed over on demand to the coinsurers and, in most instances, were in order, little was made of the discrepancies that were found. The symbolic nature of computerized data combined wth the plausible excuse of computer error reinforced the integrity of the Equity Funding caper and the fraud continued to run smoothly for about a decade (Comer 1977: 187).[8] Other examples of

---

[8] The case of Equity Funding will be more extensively examined in Chapter III.

computer-generated information being used to deceive people into parting with something of value could involve the false advertising of nonexistent services, such as dating bureaus or other consulting agencies (Parker, 1976: 21).

### ii. Temporal and Spatial Aspects of Computer-Related Crime

Regarding the four roles computers can play in the commission of crime, two technological aspects of the computer environment provide offenders with the opportunity to develop schemes that are extremely difficult to detect.

#### Temporal Aspect

Ever since the business community realized the potential for computers to enhance financial transactions, it has exerted extensive pressure on the computer industry to develop faster and more efficient machines. Such pressure has resulted in an upward spiral effect, where the industry creates more intricate machines, only to become obsolete the next year by continuing demands for improvements in technology. Intense competition within the computer industry has led to heightened expectations from scientific, business, and educational institutions for the development of machines that are capable of processing data at rates of speed which are becoming more difficult to comprehend.

As the components within computers get smaller, so does the

time it takes for electronic pulses to travel within the complex circuitry, establishing astonishing rates of speed. New terms have been created to describe the time dimensions which are used to transmit data from one circuit to another.[9] Microsecond, nanosecond, and picosecond are representative of such new time dimensions, and are contingent upon the sophistication of data processing capabilities of specific computer systems. Secondary storage devices, such as disk drives and disk drums, were designed to handle as much of this internal processing speed as possible[10] but, in most instances, fell short of maintaining the same rate of transmission (Stabley, 1982: 5).

Such internal processing capabilities not only enhanced scientific and business applications, but also provided extensive opportunities for criminal activity. In traditional forms of criminality, the perpetrator usually had to anticipate the length of time he would have to remain at the scene, in order to reduce the possibility of detection or arrest. The time dimension is, therefore, an important factor in the decision to commit a crime.

---

9 A Microsecond represents one millionth of a second. A nanosecond represents one billionth of a second. One nanosecond is to 1 second as 1 second is to 32 years. A picosecond represents one trillionth of a second, or 10** -12 seconds (Sippl, 1976: 302, 317, 356).

10 For the IBM System/360, disk storage devices were developed that could provide data transmission speeds of 312,000 characters per second, with drum storage speeds of 1,200,000 characters per second. The IBM System/370 possesses transmission speeds ranging from 1,198,000 to 3,000,000 characters per second depending upon the type of secondary storage device utilized (Stabley, 1982: 5).

However, in computer-related crimes, the temporal aspect takes on a vastly different perspective, revolving around the actual duration of criminal activity. The high processing speeds previously discussed are usually applicable only to examples involving sophisticated program manipulation schemes, such as the trojan horse, simulation and asynchronous attack. Such techniques rely upon the speed of computers to process the unauthorized instructions in a manner which effectively renders detection impossible. As noted by Perry (1986: 185), "... whereas the fastest traditional criminal acts are measured in minutes, some computer crimes are being perpetrated in less than 3 milliseconds. The mere speed of its execution makes computer crime different from others".[11] The United States Department of Justice (1980) also addresses this aspect of computer-related crime:

> Establishing the timing of a computer related crime is often impossible. Computers can be instructed by electronic impulses to add, transfer or, as in case of detection, destroy key bits of information within a matter of milliseconds (United States Department of Justice, 1980: 9).

Even if the crime is detected, the programmer can greatly hinder

---

11 This particular aspect of computer-related crime has tended to be overstated in the literature, since the same point can be simiarly argued for other forms of crime. For instance, it has been noted that a shooting takes only milliseconds once the trigger has been pulled.

investigation and prosecution by inserting a 'logic bomb' at the end of the string of unauthorized instructions. Such a strategy will erase all traces of illegal entry, thereby undermining any investigative attempts. In traditional forms of criminality, the determination of the timing of a criminal offence is often a straightforward process. The 'reactive' nature of police response calls, the interviewing of witnesses, and the analysis of physical evidence all help in specifying the timing of the event. However, in computer-related crimes, there are usually no complaints (unless they are made after the fact), there are no witnesses and, in cases of program manipulaton schemes, the programmer will take care to erase any electronic evidence. Thus, the timing of a computer-related crime can often be difficult for investigators and prosecutors to determine.

Spatial Aspect

Another distinctive technological aspect of computer-related crime concerns the interactive relationship between the offender and the victim. In traditional forms of crime, (including other types of white-collar crime) the criminal will inevitably enter into contact with the victim. Such contacts often revolve around a differential power relationship, where the offender possesses some form of domination over the victim. Letkemann (1973) discusses this type of victim/offender interaction:

> The skills required for crimes involving the avoidance of the victim are significantly different from the skills required for crimes involving victim confrontation. Surreptitious crimes tend to revolve around mechanical competences, whereas crimes involving victim confrontation revolve around victim management. The bank robber relies on surprise to bring about momentary mental and physical paralysis of bank employees (Letkemann, 1973: 274-275).

Victim management is, therefore, an important skill in street crime confrontations. However, in the majority of computer-related crime cases, such interactions are virtually non-existent. This spatial aspect also tends to hamper investigative attempts. The United States Department of Justice (1980) states:

> Computer crimes are generally of low visibility and, consequently, are difficult to detect. As a former U.S. Attorney General noted with regard to such offences, '[t]here are no smoking pistols, no blood-stained victims; often the crime is detected by sheer accident' (United States Department of Justice, 1980: 8).

Geographical distance from the scene of the crime eliminates victim/offender confrontations, which may provide investigators with valuable evidence. It also tends to isolate the offender from the criminal nature of the violation, since the immediate consequences of crime are not readily observable.

Computer telecommunications have enabled criminals to develop

and implement highly complex strategies from unlimited distances, often crossing international boundaries. This factor also distinguishes computer-related crime from other forms of criminality. The United States Department of Justice (1980) notes:

> Computer related crimes can be committed over vast distances and across many intranational and international jurisdictional lines. Through the use of a remote computer terminal and telephone hook-up, a knowledgeable computer felon can, provided he knows how to access the system, give illicit instructions to a computer literally anywhere in the world (United States Department of Justice, 1980: 8).

The House of Commons Subcommittee on Computer Crime (1983) maintains that it is extremely difficult to prosecute offenders who have accessed data bases in other countries. Jurisdictional authority is often problematic, especially in light of the recently amended federal statutes to combat this form of unauthorized access:

> If in fact you were dealing with a trans-border situation, the real question would be, presumably, was it an offence to do what you did in the United States that was an offence to do in Canada? If the critical action took place in the United States, the data base was in the U.S and if the computer that was accessed, if the services that were diverted, were in the United States, presumably you would want to look at prosecution under American law as opposed to Canadian law (Canada. House of Commons, 1983: 16: 20-21).

This spatial aspect, combined with the temporal attributes of computer-related crime, present researchers with numerous areas for criminological investigation.

Although the temporal and spatial aspects of computer-related crime demonstrate unique technological characteristics in relation to other forms of criminality, they are only applicable to a small percentage of actual cases. The convergence of research on such cases has resulted in a disparate analysis which ignores vast areas of criminal activity.

To the layman, the concept of "computer crime" represents a highly sophisticated form of criminal activity requiring advanced technical skills and knowledge. While some types of computer crime do illustrate such characteristics, the majority are relatively simple, necessitating only a basic understanding of computer technology. The term is, in itself, a misnomer which was undoubtedly coined for lack of a better descriptive label. In reality, few activities involving the manipulation of computers can be ascribed the status of computer crime. A concept better suited for criminological research is "computer-related crime", which enables researchers to distinguish between the different types of criminality associated with computer technology without extensive definitional restriction. In addition, the concept introduces a 'measure of proportion' when assessing the nature of crime characteristics. For example, the statistics derived from the Stanford Research Institute (SRI) studies were criticized because they included cases which were not considered appropriate for analysis:

> SRI defines computer abuse to mean an `intentional act in which one or more victims suffered, or could have suffered, a loss and one or more perpetrators made, or could have made a gain'. The definition is impressive, but many of SRI's cases simply do not fit. The SRI collection includes cases that do not even invlove computers. The most glaring of these is 7248N, were telephone equipment was falsely wired to allow outside calls to be placed from certain phones. The reason this case was included was because SRI was toying with the idea of classifying telephone systems as computers. Part of SRI's difficulties are no doubt definitional, namely: what is crime (or abuse); what is a computer; and finally, what is a computer crime (Taber, 1980: 288-289, 292, 295).

On the other hand, the U.S. General Accounting Office (GAO) only considered cases for analysis which had been "officially" verified as computer-related crime by government agencies which used rigidly defined parameters as a basis for sample selection. Regardless of what form of criteria are used to specify the units of analysis, it is vital to retain a high level of definitional consistency in application. In this respect, the definition of "computer-related crime" described earlier will be employed as the basic criteria for case selection; and when combined with the four research indicators will provide the mechanism to perform a content analysis. The next two chapters will be directed toward examining the nature of the three major descriptive variables 1) technical skill and knowledge; 2) motivation; and 3) opportunity, the last two of which will facilitate the conceptualization of the research design, and the former providing a secondary variable of analysis.

## III. Technical Skill and Knowledge

The objective of this chapter is to provide a brief introduction to the basic techniques employed in computer-related crimes. Many of the techniques described here are highly sophisticated, and would require the technical expertise of a computer specialist to be thoroughly addressed. The Chapter is thus admittedly limited in scope, since it lacks the strict technical competence which is necessary for such an analysis. The purpose of presenting these techniques is not to develop a step-by-step resource manual on crime strategies, but to acquaint the reader with the diversity of criminal activities afforded by an expanding technology.

This Chapter will illustrate some of the different types of vulnerabilities contained within computer systems, and possible techniques which can be utilized to exploit them. The majority of information used in the preparation of this Chapter was drawn from studies conducted by the Stanford Research Institute, which has received international recognition for its efforts in computer-related crime research. The 13 computer-related crime techniques described here are by no means exhaustive, and should be viewed only as a representative subset of methods that may be used for criminal activities. Many of the "cases" that will be cited to illustrate these crime techniques cannot be substantiated by actual case law and, in this respect, may contain as much fiction as fact. Because of the

apocryphal nature of many of these cases, a number of authors (MacIntosh, 1983; Rhodes, 1979; Taber, 1980) have rejected their authenticity outright. However, although some of the cases may be questionable, they do provide descriptive examples of the possible methods of computer-related crime.

## Computer-Related Crime Techniques

Computer-related crimes generally fall into five major types of classifications, each requiring different levels of technical skill and knowledge. These include: 1) physical acts; 2) transactional acts; 3) programming acts; 4) electronic acts; and 5) system hacking. Each classification contains a number of sub-techniques which enable offenders to exploit different types of computer system vulnerabilities.

### A. Physical Acts

#### i. Destructive Attacks

Destructive attacks include all acts which render computer systems inoperative by physical means. These activities can be categorized according to the type of attack, and include four areas of concentration: physical damage, storage media damage, logical damage, and communication damage. Of the four different areas, physical damage is the least specific, and can include variations of the other types of physical acts, (which tend to require a greater application of technical skill and knowledge).

## Physical Damage

Physical damage can be accomplished by anyone remotely involved in the operation of a computer center. Such acts are directed toward all forms of computer-related equipment and materials,[1] including hardware,[2] software, and data.[3] The perpetrators of such acts usually do not discriminate between different objects of attack; their sole purpose is to deprive users of the continued use of the computer facility. Their objective is not the covert alteration or modification of equipment which would lead to eventual destruction, but simply to destroy as much computer-related material as possible to render the center inoperative.

Few if any, computer-related skills are needed in

---

1 The term hardware is often used to denote physical equipment, such as the mechanical, magnetic, electronic, or electrical devices or components from which assemblies are made, or the assemblies themselves; for example, the assembly of material that forms a computer, as distinct from data, routines, or programs (Weik, 1970: 152).

2 Software is comprised of the various programming aids that are frequently supplied by the manufacturers to facilitate the purchaser's efficient operation of the equipment. Such software items include various assemblers, generators, subroutine libraries, compilers, operating systems, and industry-application programs (Sippl, 1976: 446).

3 A general term used to denote any or all facts, numbers, letters, and symbols, or facts that refer to or describe an object, idea, condition, situation or other factors (Spencer, 1968: 19). Data is not synonymous with information although it is used interchangeably in many instances. Information is that which the data conveys or tells a person. Data may be called selective information, while in the ordinary sense of information we mean semantic information; that is, information is the meaning derived from data (Weik, 1970, 96).

physical attacks; the only significant technical requirement is access to the center itself. In this respect, physical damage can not be considered a true computer crime, unless the application of 'high-level' programming knowledge is used in the commission of the act (i.e., CRC-01, p.13).

Examples include attacks initiated by protesting students, terrorist groups, laid-off or fired employees, and a wide range of individuals with a grievance against the 'system' for one reason or another (Carroll, 1977: 16,17,29). One notable case, however, concerned a computer operator who worked the night shift at a large computer facility in a high crime rate area. As insurance against mugging, the operator was in the habit of carrying a gun to work. One night, while performing his assigned tasks, the computer encountered numerous errors which frustrated the operator to the point where he shot the computer to eradicate the recurring trouble (Parker, 1976: 18). While this case was not intentionally directed toward criminal activity, it does illustrate the often inane reasons some individuals offer as justification for their destructive attacks against computers.

Because of the sensational nature of destructive attacks, and the resultant media coverage, more international terrorist groups may become involved in physical acts against computer centers. One of the most alarming trends in terrorist attacks against computer centers is the recruitment of 'insiders' of the target organization as an intelligence source. It has been

estimated that, of the 27 facilities attacked in Italy between 1974-1983, the majority involved assistance from inside sympathizers (Bruschweiler, 1985: 169).

## Storage Media Damage

These destructive acts are directed toward all forms of storage media, including punched cards[4], computer hardcopy[5], and magnetic tapes[6] and disks[7]. The objective of such damage is not the physical destruction of the medium per se, but rather the removal or erasure of the information contained within the medium. Before the development of magnetic storage devices, the punched card was the primary means of documenting and recording data and, in some circumstances, is still used by certain computer centers for specific applications.

Punched cards are susceptible to a large range of destructive acts, but the most effective is selective damage (Carroll, 1977:

---

4 The preparation of input data by transcribing data into machine-readable form. (Davis, 1965: 14) The punched holes are sensed electrically by wire brushes, mechanically by metal fingers, or photoelectrically by photocells (Sippl, 1976: 253).

5 Hardcopy represents a printed copy of machine output in readable form, for example, reports, listings, documents, summaries (Spencer, 1979: 88).

6 A storage device consisting of metal or plastic tape coated with magnetic material. Binary data are stored as small, magnetized spots arranged in column form across the width of the tape (Sippl, 1976: 282).

7 A storage device on which information is recorded on the magnetizable surface of a rotating disk. Data are stored on the surface of each disk as small, magnetized spots arranged in circular tracks around the disk (Sippl, 1976: 137, 281).

29). Such attacks can be more detrimental to an organization than the outright destruction of a complete card inventory. In one such case, a computer programmer removed and destroyed every fifth card from a master program deck. The subsequent confusion caused by the improperly processed data resulted in extensive down-time[8] of the facility and lost resources in attempting to locate the processing error (Carroll, 1977: 29). Even the destruction of only one or two cards could have brought about the same effect, since the removal of specific cards would have caused a 'ripple-change' throughout the processing of data which required the information provided by the removed cards.

The most sensitive forms of storage media are magnetic tapes and disks. These storage devices are susceptible to contamination by adverse conditions or the application of almost any substance (Parker, 1983: 42). For instance, strong magnetic fields can be used to erase data if the electrical current is applied over the complete surface of the tape or disk (Beardsley, 1973: 47). One example of magnetic damage occurred in 1969 when an anti-war group protesting Dow Chemical's manufacture of napalm penetrated the company's computer center. The group destroyed a number of valuable tapes by using powerful electrically charged magnets (Carroll, 1977: 29).[9] The application of such hand-held magnets is often unreliable in obtaining total erasure of data since the

---

8 The period during which a system is inoperative due to a hardware malfunction (Maynard, 1975: 62).

9 Case number CRC-05: see Chapter V.

electrical field is not consistent, but can be an effective means of causing sporadic error (Beardsley, 1973: 47-48).

The development of degaussers[10] has made the use of magnets obsolete for destroying data. Degaussers are not usually used by outside perpetrators since their bulk could be easily detected by physical security procedures (e.g, closed-circuit monitors, etc). However, with the increased miniaturization of computer components, they may be used more often in the future by individuals or groups who wish to destroy corporate assets.

At present, such devices are limited to employees of large computer centers who use degaussers as an efficient means of neutralizing voluminous amounts of unwanted data (Beardsley, 1973: 48). If a disgruntled employee can gain access to the on-line tapes,[11] as well as the tape storage library, he/she can effectively render the company completely inoperative by erasing all data with a degausser (Beardsley, 1973: 48). Such a strategy can be even more damaging if duplicates of the tapes are made before destruction. The illicit sale and ransom of duplicated information has always been a profitable venture; it becomes even more so when the massive storage capabilities of computer tapes are taken into consideration.

In one such case, an employee of Encyclopedia Britannica

---

10 A coil that has been momentarily energized by an alternating electrical current that disarranges the impulses on a magnetic tape or disk when it is placed close to the coil (Sippl, 1976: 124).

11 Pertaining to equipment directly controlled by the central processor. An on-line system usually involves the use of data transmission facilities to remote terminals (Maynard, 1975: 134).

stole the master-file list of 800,000 customers and sold the information to Business Mailers Inc., who then rented the list to Curtis Books Inc., a competitor of Encyclopedia Britannica. The list was used to advertise the cheaper subscription rates Curtis Books offered. The total loss sustained by Encyclopedia Britannica from the sale of the list has been estimated at $3 million (Carroll, 1977: 21).

## Logical Damage

Logical damage concerns all destructive acts directed toward the internal and external labels identifying the contents of magnetic disks and tapes (Parker, 1983: 42). This type of damage differs from storage media damage in that the information contained within the tapes is not destroyed, but the labels are removed, rendering the tapes ineffective if specific data are requested (Beardsley, 1973: 48).

External labels are used to describe the contents of tapes and disks by visual examination. The labels are attached to the exterior of the tape reel or disk cover allowing for identification without the necessity of reading the files (Parker, 1983: 42). External labels can be easily damaged by anyone involved in the handling or transport of tapes and disks. In one case, which occurred in 1971 at a large New York computer center, an employee who had just received his

two-week lay-off notice, removed the external labels from 1,500 tape reels. The company was forced to run many of the tapes to re-identify the data, since some of the tapes did not contain back-up labels. The removal of the external labels effectively tied up the system, and the loss in wasted man hours and computer time cost the company thousands of dollars (Carroll, 1977: 30).[12]

Internal labels are data file names,[13] stored magnetically, which identify the contents of tapes and disks to the computer. Internal labels can be damaged in two different ways. The first involves the complete erasure of all file names that identify specific blocks of information. This type of logical damage can be accomplished by destroying the file directory[14] which lists all the files within a disk or tape. Such damage can be extremely disruptive to computer operations which do not back-up their internal file directory with external labels.

The second type of attack is much more insidious. It involves the covert destruction and modification of file names which would

---

12 Case number CRC-06: see Chapter V.

13 A named set of records and, often, access-related information. Though the term may be applied to a set consisting of source documents, punched cards, or other media, it is usually understood to be a magnetic disk or tape. By this definition, a file is a basic unit for storing and accessing user data; ('a master file'; 'the NSFX file'; 'a payroll file'). [the term also refers to] individually accessible units of storage (code, data, or empty locations). It is this definition that is implicit in such terms as 'file access', 'file transfer', and 'file protection' (Galland, 1982: 100).

14 A list of the files and their locations on a particular storage device or volume is kept in a reserved area (sometimes a system control area) on the device or volume (Galland, 1982:101).

eventually affect the results of computer output and the subsequent activities based upon the results (Parker, 1983: 43). A potentially dangerous situation occurred in New Jersey in 1970 when a fired employee of a pharmaceutical manufacturer scrambled all the company's files, which could have led to distributors receiving improper prescriptions if the damage had not been discovered (Carroll, 1977: 30).[15]

Communication Damage

Many large computer centers are well protected from direct physical attack from outside sources. Electronic doors, check-in procedures and visual identification precautions prevent unauthorized personnel from entering restricted access areas (The Ombudsman Committee on Privacy, 1976: 14-15). Even though techniques exist which can be used to breach such security procedures, most perpetrators intent on destructive acts do not possess the skill necessary to use them. However, if the organization under consideration relies on a telecommunication network, other avenues are open for destructive acts.

As more corporations are using the rapid communication power afforded by telecommunication networks, the potential for destructive acts is increasing dramatically. The targets of communication damage are telephone lines and switching offices which usually possess little or no protection from external

---

15 Case number CRC-07: see Chapter V.

attack. Telephone lines can be easily destroyed by anyone with a rudimentary knowledge of the local system and the specific lines to be sabotaged. The traditional method used in such attacks is fire bombing, which produces immediate disruption of services, but, because such lines are quickly repaired, more effective strategies can be directed toward telephone switching offices (Parker, 1983: 43).

Although the destruction of a switching office would cause great inconvenience for regular users of the facility, the resultant long-term communication damage sustained by the target computer center could be irrevocable. If the potential for destructive attacks is ever realized by terrorist groups, many more corporations and institutions may become victims of communication damage. In a report conducted by the Stanford Research Institute for the American Telephone and Telegraph Corporation, it was found that determined terrorists could effectively shut down the entire U.S. telephone long lines system by destroying only twenty trunk lines (Parker, 1983: 43).

ii. Input Manipulation

Input manipulation or "data diddling" is unquestionably the most common technique employed in the commission of computer-related crimes (Taber, 1980: 282). Many researchers regard this form of crime as no different from other forms of crime, since the majority of preparation takes place without the aid of the computer (Myers, 1979: 71). They maintain that the only significant difference lies in the fact that the fraudulent

scheme is processed by the computer rather than by manual manipulation (MacIntosh, 1983: 8).

However, another significant difference which distinguishes input manipulation from other types of fraud revolves around the implicit trust the victims place in the integrity of computer output (Business Electronics: 1980: 94). Many people tend to consider information generated by the computer as infallible. The criminal relies upon this victim confidence and simply changes previously verified data before or during their input into the computer to make it appear legitimate (United States Department of Justice, 1979: 9). The acceptance of such fraudulent information is further reinforced by the other skills used in the commission of the crime, such as, balance accounting procedures, inventory control, and banking knowledge. Input manipulation may be considered an 'occupational crime', since the fraudulent scheme would not possess any credibility without the authority of specific job-related knowledge (Tassel, 1972: 29).

The Equity Funding Case illustrates this specific type of knowledge application in input manipulation schemes. Equity Funding was a major insurance firm that ran into serious financial difficulties in the early 1960's (Bequai, 1978: 64). The exact reasons for the firm's dismal financial situation are not clear, but some analysts speculate that it may be attributed to a 'special class insurance policy' that was offered to employees (Bequai, 1978: 64). The program entitled employees to free life insurance policies for the first year, which they

could 'cash in' if they desired. Many did, and the firm found itself struggling to survive.

In order to overcome these financial problems and present an aura of well being to its stockholders and the public, upper management officials embarked on an unprecedented input manipulation scheme that eventually cost the public $2 billion. Equity Funding possessed approximately 90,000 insurance policies, of which 60,000 were fraudulently created. The objective of the scheme was to inflate the firm's assets, then sell large blocks of the insurance policies to other firms. The coinsurer would then collect the majority of the premiums, and Equity Funding would collect a consignment fee (Bequai, 1978:65).

The massive fraud could never have succeeded without the rapid creation power afforded by the computer. Every year new fictitious insurance policies had to be created to cover the normal attrition of premiums on the previous year's policies. If manual methods had been used to develop the data files on 60,000 fraudulent policies, the possibility of detection would have been much greater due to the vast number of people involved in the fraud. By using the computer, the number of individuals involved was kept to a manageable limit.

The credibility the coinsurers placed in the computer print-outs also ensured the continual success of the fraud. Equity Funding was often asked for a listing of its policies, which they handed over for examination. When discrepancies were found in the policies, Equity Funding responded with the believable

excuse of 'computer error', which was accepted as the truth by the coinsurers, once again reinforcing the symbolic nature of computerized data. Equity Funding is only one example of the potential for input manipulation to subvert businesses that rely upon the integrity of computerized information.[16]

Krauss and MacGahan (1979) identify a number of input manipulation techniques:

### Extraneous Transactions

This technique involves the insertion of additional extraneous monetary transactions which require the specific modification of fraudulently created files. Typically, these manipulations require the substitution or alteration of the indicative data about a person (i.e., name, address, social security number, etc.), or the alteration of an entity (e.g., customer, shareholder, employee, department, etc.),(Krauss & MacGahan, 1979: 264).

One example of an extraneous transaction scheme entails the addition of an entirely new master-file record which involves recurring payments. By developing the indicative data file of an imaginary employee or shareholder and inserting the information into the payroll file, the perpetrator can collect regular cheques for extended periods (Brandt, 1975: 85). Both businesses

---

16 Case number CRC-08: see Chapter V.
For further detail on the Equity Funding case, see: Sobel and Dallos (1975); Smith (1974); and Woofe (1977).

and government agencies are susceptible to losses by extraneous payments.

**Failure to Enter Transactions**

By failing to enter authorized transactions, a number of different schemes can be developed which are based upon a method known as interception. One noted case involved a cheque processing clerk who intercepted his own canceled cheques, and failed to enter them before they were debited to his account (Krauss & MacGahan, 1979: 267).[17] A more sophisticated variation on this scheme involves interception with status change alteration.

To illustrate this method of input manipulation, Krauss and MacGahan use a pension system as an example. Normally, when a pensioner dies, the information is recorded and the cheques are terminated. However, if a perpetrator is in a position to intercept the pensioner's status-change file before the death is permanently documented, he/she can fail to enter the death, while substituting a fictitious name and address for that of the deceased. Cashing the deceased's cheques could be accomplished easily by assuming the identity of the fictitious pensioner (Krauss & MacGahan, 1979: 267-268). In one case that occurred in West Germany, a data processing clerk, who was responsible for updating a large pension system, discovered a number of weaknesses in the way in which deaths were recorded. The

---

17 Case number CRC-09: see Chapter V.

information enabled him to collect pension cheques for an extended period of time, then systematically "kill off" deceased recipients at appropriate intervals (Brandt, 1975: 86).[18] A similar case occurred in Canada in 1975 when an employee of an insurance company updated "deceased" files to active status, changing account numbers and addresses in order to collect the pension cheques (Leibholz & Wilson, 1974: 38).[19] Government services, such as unemployment insurance, social security, and medical programmes, are often the victims of this type of fraud (Guncheon, 1982: 104).

## Modification of Transactions

This technique incorporates many of the methods employed in extraneous transactions, but it also requires the modification of existing data which have been properly authorized. Such schemes are most effective when file-maintenance transactions are being recorded, such as changes in credit limits, new accounts, or account renewals (Krauss & MacGahan, 1979: 269-270).

For example, one modification transaction scheme may involve the alteration of the name and address on a credit card account renewal application. By inserting a fictitious name and address for that of a customer, and leaving the original account number unchanged, the perpetrator could purchase goods to the credit

---

18 Case number CRC-10: see Chapter V.

19 Case number CRC-11: see Chapter V.

account limit, while the original customer is charged for the purchase (Krauss & MacGahan, 1979: 270). Any company or corporation offering such credit services may be subject to such fraudulent schemes.

### Misuse of Adjustment Transactions

Adjustments are usually made to correct errors in monetary transactions which have resulted from physical loss or exchange. Department stores and other retail and wholesale vendors are often victims of such adjustment frauds. This technique requires that adjustments are made to accounts when no real transaction has taken place.

For example, a perpetrator working in collusion with an accomplice may make adjustments to a department store charge account indicating that goods charged to the accomplice's account have been returned, when in fact they have not. Another scheme involves the physical theft of inventories and supplies, then entering adjustments indicating that the goods were lost or re-directed to another location (Krauss & MacGahan, 1979: 271). In one case that occurred in 1971, an employee of a catering service entered false account numbers and invoices for $120,000 worth of goods. Using a grocery store owner as an accomplice, the goods were delivered, but recorded to the false accounts which were maintained and effectively hidden by the clerk (Leibholz & Wilson, 1974: 37-38).[20]

---

[20] Case number CRC-12: see Chapter V.

## Misuse of Error-Correction Procedures

In some instances when corporations or other institutions undertake error-corrections, they do not necessarily include them in the permanent records of an account. As a result, many effective strategies have been developed which exploit this system weakness. Lack of internal controls over the authorization of error-corrections can lead to extraneous file maintenance transactions which may include: entering extra error-corrections when no error actually exists, failure to enter necessary corrections, and modification of properly authorized error-corrections. One of the simplest schemes used by individuals who possess access to error-correction input involves creating an error that will reject a legitimate transaction (Krauss & MacGahan, 1979: 274-275).

## File Alteration Schemes

Such schemes usually require the perpetrator to possess complete access to a live master file for an extended period of time. The file must then be copied either in-house or at another location. Using a specially written program as a modifier, changes can be made to the file so that all the indicative data demonstrate identical alteration (Krauss & MacGahan, 1979: 278). The newly modified file is then substituted for the original and runs the fraudulent scheme the next time the program

is used. In one case, a computer programmer altered all the indicative data files in an accounts payable program with a balance patch program.[21] The scheme added ten cents to every service charge less than ten dollars, and one dollar to those larger than ten dollars. The excess service charges were directed to the programmer's account, which was drawn down once a month to keep the accumulating funds at a reasonable level (Brandt, 1975: 87).[22] In another case which occurred in 1973, a computer update clerk modified a dividend calculation program to generate cheques to all former shareholders, then erase the records of payment at the end of each monthly cycle (Leibholz & Wilson, 1974: 39).[23]

### iii. Scavenging

Scavenging is basically a technique of obtaining privileged information which has been discarded by other computer users as useless material, or through carelessness. Scavenging techniques can be categorized into three fundamental methods: visual, physical, and residue.

#### Visual Scavenging

Visual scavenging is probably the most elementary, since it simply requires 'over-the-shoulder eavesdropping', while someone

---

21 A temporary correction added to a routine or program. Usually supplied in the form of 'object coding' and sometimes entered from the operator's console (Maynard, 1975: 142).

22 Case number CRC-13: see Chapter V.

23 Case number CRC-14: see Chapter V.

is signing-on to the computer (Walker & Blake, 1977: 7). If conducted carefully, visual scavenging can provide the account numbers[24] and passwords[25] of several different privileged user groups[26] when users are working in an interactive environment. Such environments are designed to allow different users to discuss computing projects, productive programming and other aspects of their jobs in an open and creative atmosphere. But, they also lend themselves to abuse through scavenging techniques, since the very nature of such environments is intended for increased employee collaboration (Miller, 1984: 107). More covert visual scavenging involves the scavenger entering the operator's console, or other restricted area, to inquire about some imaginary problem and visually scan terminals for any valuable information which may be on-line.

## Physical Scavenging

Physical scavenging is the process of collecting anything and everything that may be discarded in or around a computer room,

---

24 A one-to-eight-character symbol identifying a system user, abbreviated USERID (Sippl, 1976: 516).

25 A unique string of characters that a program, computer operator, or user must supply to meet security requirements before gaining access to data. In systems with time sharing, a one-to-eight-character symbol that the user may be required to supply at the time he logs on the system. The password is confidential, as opposed to the user identification (Sippl, 1976: 351).

26 An indication of the access rights of a user or user program to the data of a computer system. If given a numeric value, it may be termed an 'access control system' (Galland, 1982: 220).

printing office, or company trash cans (Walker & Blake, 1977: 7). Items which can usually be found in these areas include old print-outs, carbon paper from multi-part forms, used carbon ribbons from printers, and outdated computer manuals and operating guides (United States Department of Justice, 1979: 23). The majority of the waste material will, in fact, prove useless but, with diligence, the scavenger may obtain enough valuable information to initiate a computer-related crime.

Such was the case in Los Angeles in 1971, when Jerry Neal Schneider discovered a method of stealing large quantities of equipment from the Pacific Telephone and Telegraph Company supply office (Parker, 1976: 59). One day, while walking to school, he observed that the trash cans outside of the supply office contained bundles of interesting documents which he collected for further examination. After a couple of years of scavenging, Schneider had in his possession a complete library of Pacific Telephone and Telegraph Company operating guides, including, guides to ordering parts, computer program listings to distributing offices, and instructions describing how Pacific Telephone and Telegraph Company orders supplies from Western Electric Company. However, the most important document Schneider obtained was the access code guide which enabled him to gain on-line terminal entry for inventory control and parts distribution.

By studying the operating manuals and other documentation, it was easy for Schneider to start ordering equipment to be delivered to different parts of the city where they would be later picked up and brought to his own company warehouse. The

equipment was then sold to smaller independent parts distributors. The estimates of loss to Pacific Telephone and Telegraph Company range between $125,000 and $800,000. The real loss will probably never be known since the fraud was so ingenious (Parker, 1976: 60-64).

## Residue Scavenging

Residue scavenging requires more preparation and is more risky than other forms of scavenging, since this type of eavesdropping can be detected by an alert systems operator who may be monitoring the system at the time of scanning. Essentially, residue scavenging is the reading of another user's job after he/she has signed-off the computer (Walker & Blake, 1977: 7).

Many computer systems possess buffer areas, which are storage devices where data are assembled temporarily during data transfers.[27] Computer users adopt buffer areas as an efficient means to temporarily store input while they are on-line. When the user signs-off, the buffer should be automatically erased. However, some computer systems are not designed to erase the buffer storage areas, but simply write over them with the execution of the next job. With sufficient technical skill and

---

[27] An area of storage where data is held temporarily to facilitate transfer between devices operating at different speeds or on different time cycles; for example, an area of main storage that holds incoming messages and outgoing replies in a transaction processing system or a memory in a line printer that holds one line of characters to be printed (Galland, 1982: 29).

knowledge, it is possible to read the residue data left in the buffer storage before it is replaced by a new job (United States Department of Justice, 1979: 23). Perry (1986) describes a case of residue scavenging involving a covert acquisition scheme, which is generally associated with system hacking techniques:[28]

> In one case, a time-sharing service had several oil companies as customers. The computer operator noticed that every time one particular customer used the service, his job always requested that a scratch tape be mounted on a tape drive. When the operator mounted the tape, he noticed that the read-tape light always came on before the write-tape light came on, indicating that the user was reading data from a temporary storage tape before he had written anything on it. Simple investigation revealed that the customer was engaged in industrial espionage, obtaining seismic data stored by various oil companies on the temporary tapes and selling this highly proprietary, valuable data to other oil companies (Perry, 1986: 223).

This type of activity can be a highly lucrative past-time, especially in competitive markets where secrecy of information is imperative. Organizations possessing trade secrets, industrial designs, patents and other classified data are all susceptible to scavenging techniques.

---

28 Case number CRC-15: see Chapter V.

## B. Transactional Acts

### i. Data Leakage

Data leakage is a technique specifically used to remove or leak sensitive data from a secure computer center. The extreme methods used in some data leakage schemes are only necessary in centers which maintain a high degree of physical and electronic security to protect classified information stored on magnetic tapes and disks. Data leakage methods can be used in many different circumstances, but are most effective in operations involving classified data, such as military information (United States Department of Justice, 1979: 244, 25).

Many sophisticated software manipulation schemes are so well hidden within computer programs that they necessitate data leakage methods to convert the illegal act to financial gain. Because computer output is often screened by operators or other clerical staff, specific information must be removed by using a number of different techniques, many involving communication traffic analysis.[29] Data leakage is accomplished by the pattern in which information is conveyed, rather than the alteration of the information itself (Parker, 1983: 97).

These techniques can range from relatively simple schemes to extremely complex software manipulations, all depending upon the

---

[29] The obtaining of information from a study of communications traffic. Includes statistical study of message headings, receipts, acknowledgments, routing, and so on, plus a tabulation of volumes and types of messages with repect to time (Sippl, 1976: 502).

extent of security procedures maintained by the computer facility. The most rudimentary form of data leakage concerns 'masking schemes', which require the displacement of the target information within otherwise innocuous data (United States Department of Justice, 1979: 26). For example, one masking scheme would require the programmer to merge the user file catalogue into reports which are commonly removed from computer centers. Every fifth or tenth paragraph in the report will contain the classified data. When the programmer leaves the ~~facility~~, security personnel may be satisfied to check only the print-out cover sheets which would not reveal the contents of the document.

Other data leakage schemes involve 'encoding strategies', which use more extensive computer programming skills.[30] These techniques require modifications in the pattern in which blocks of data are transmitted. The leakage of classified data is accomplished by formatting computer output, so that the user file catalogue can be deduced from the different lengths of printer lines, number of words per line, locations of punctuation, or the use of code words in specific line locations. Once the programmer has removed the file catalogue from the computer center, it can then be retrieved by the use of specified code sequences that are used in the transformation analysis (United States Department of Justice, 1979: 24-25).

---

30 Cryptography is the science or practice of changing the representation of data for security purposes; it consists of placing data in a form (code) that prevents its correct interpretation without special knowledge or equipment (Galland, 1982: 55).

The above examples of data leakage pertain to situations which allow for the removal of hardcopy from computer centers. However, more exotic schemes can be used in circumstances which restrict the removal of any documentation, such as in classified government installations. These schemes involve the acoustic recording of the movement of equipment parts which can then be converted into meaningful data. Tape reels are especially susceptible to such recording, since they move clockwise and counterclockwise in a pattern representing binary digits 0 and 1, which are then revised in the transformation analysis (United States Department of Justice, 1979: 24-26). Acoustic recording schemes are extremely risky and time-consuming and are warranted only if the computer center is highly secure, or the information is such that it can not be removed by other conventional methods.

ii. Impersonation

As the name implies, impersonation is the process of assuming the identity of another individual in order to gain access to restricted areas or privileged information. The perpetrator must possess some sort of knowledge which can be verified as legitimate in order to successfully impersonate a privileged user. Usually such knowledge is gained through scavenging techniques, then converted to illicit gain by use of impersonation (Cooper, 1984: 37).

In the majority of impersonation cases, verifiable knowledge

represents computer identification numbers, passwords, and access code sequences (United States Department of Justice, 1979: 26). However, a simple understanding of the computer system which is being considered for penetration may be enough for a successful impersonation.

As well as scavenging, Jerry Neal Schneider also used impersonation in the Pacific Telephone and Telegraph Company fraud. He approached Western Electric Company officials posing as a journalist and indicated that he would be interested in writing an article on its computerized equipment ordering system for a well known local magazine. He was so convincing in his impersonation that company officials went out of their way to describe how the system operated, and gave him as much documentation on the system as he needed to write the "article" (Parker, 1976: 60-61). The manuals gained from the scavenging provided Schneider with the technical background to initiate the fraud. However, it was his second impersonation of an authorized 'parts order clerk' (using the scavenged access codes) which enabled him to successully circumvent security controls.[31]

Becker (1980) describes a noted case of impersonation which involved the theft of $10.2 million from the Security Pacific National Bank in 1978. Stanley Mark Rifkin planned one of the greatest bank thefts in history around a single code access sequence which he used in his impersonation. Rifkin was an employee of the National Semi-Conductor Company which was

---

[31] Case number CRC-16: see Chapter V.

involved in the development of a 'back-up' system for Security Pacific's communication software. Rifkin's target was the wire-room which transferred billions of dollars a day in electronic assets. Since he was a principal designer of the back-up system, he was allowed access to the wire-room to check the functioning of the software. On one of these occasions, Rifkin scanned (visual scavenging) the access code which allowed authorized personnel to make electronic fund transfers (Becker, 1980: 473-474).

The code sequence was openly displayed on the wall of the wire-room, and he copied it without being detected. Rifkin then walked to the nearest pay phone, called the wire-room and impersonated a representative of the International Department of the Security National Bank. The impersonation was successful and permitted Rifkin to transfer $10.2 million to an account in the Irving Trust Company in New York City. He then called the Wozchod Handels Bank in Switzerland. Rifkin realized that it would be impossible to withdraw the funds without creating suspicion, so he devised a scheme of converting the funds into another form of asset by purchasing a little over 8 million dollars worth of Russian diamonds though a fake New York City diamond brokerage (Becker, 1980: 474).

Rifkin was as surprised at the success of his crime as were the bank officials at Security Pacific. He had not made any provisions for masking his escape, such as developing false identification, transportation out of the country, or means of selling the diamonds. Rifkin was arrested in California, not because of any faults in the planning or execution of the crime, but because he lacked the confidence in his own ability to

actually succeed. At his trial, Rifkin confessed that he never thought that he would get the diamonds, illustrating the inadequate planning and preparation which often precedes amateur criminality (Becker, 1980: 484).[32]

iii. Piggybacking:

Most computer centers maintain a certain degree of physical security in order to restrict individuals from entering controlled access areas where privileged clearance is required. Such safeguards can range from electronically operated doors and complex check-in procedures to simple visual identification of legitimate users (United States Department of Justice, 1979: 26).

The objective of the piggybacker is to breach physical security through staging credible scenarios which will grant access without presenting documentation. Most piggybackers will try to keep the scenarios simple because the more complex they become, the higher the chance of discovery. A proven piggybacking strategy is for the perpetrator to stand in or around a restricted access area where electronically locked doors are used. With arms full of computer paraphernalia, such as computer print-outs, tape reels, or other computer-related material, the piggybacker waits for an authorized individual to use the door while fumbling for a key or access card and apologizing for the delay. The authorized user, noticing

---

32 Case number CRC-17: see Chapter V.

the perpetrator's distress, opens the door, allowing the piggybacker to simply follow into the restricted area (United States Department of Justice, 1979: 25).

**Electronic piggybacking** is accomplished in much the same fashion as physical piggybacking, in that the perpetrator must wait for the victim to do something which will allow for unauthorized access. There are basically three different types of electronic piggybacking: traditional piggyback entry, between-the-lines entry, and spoofing (Carroll & McLellen, 1973: 140).

In **traditional piggyback entry**, the perpetrator will usually select a number of target terminals which are often used by privileged users. The perpetrator will then modify one of them to read the communications of the others. Such modifications may only require direct connections to the other terminals through communication lines, but, more often, they require hardware alterations to CPU components and other computer equipment (The Ombudsman Committee on Privacy, 1976: 10). Once the legitimate user activates the target terminal, the piggybacker can then read everything displayed on the screen through their own modified terminal, including passwords, code access numbers, and any other information the victim may be inserting at the time. The victim's files can then be accessed at a later date, using the passwords and code numbers obtained through the piggybacking.

**Between-the-lines entry** is accomplished in the same manner as traditional piggyback entry, except that, when the user wishes to sign-off, the piggybacker cancels the command and continues to operate in the user's name (The Ombudsman Committee on Privacy,

1976: 10). The piggybacker inserts the commands between-the-lines given by the legitimate user. Since the central processor only detects one terminal on-line rather than two, it will process both the authorized instructions of the legitimate user, and the unauthorized instructions of the piggybacker (United States Department of Justice, 1979: 26). Once again, the victim's files can be selectively modified, or copied at a later date, using the passwords and codes obtained through between-the-lines entry.

Spoofing, also known as pseudo sign-on, is a method in which the legitimate user is tricked into believing that he/she is conversing with the central processor when, in fact, he/she is communicating with the piggybacker (The Ombudsman Committee on Privacy, 1976: 10). This method involves software modification as opposed to hardware alteration witnessed under the other two techniques. Spoofing is only effective in computer systems which require the user to activate the terminal by hitting a carriage return key that will display the sign-on procedures[33] (Walker & Blake, 1977: 15). A program must be written that imitates the system's sign-on procedures which is then inserted into the computer's file directory.

The terminal is left in an active mode[34] and, when a user hits

---

[33] The process of establishing communication with and verifying the authority to use the computer during conversational programming (Spencer, 1979: 108).

[34] A condition of real-time communication between one or more remote terminals and a time-sharing computer, in which each entry from a terminal elicits an immediate response from the computer (Sippl, 1976: 305).

the carriage return, the simulation program is called from the directory and displays the pseudo sign-on procedures which the user performs, giving an identification number, priority code number, and password. After this information is obtained and recorded in another file, the simulation program then indicates that the system has undergone a 'crash'[35] and that the user should sign-off and try again. In the process of signing-off, the user deactivates the simulation program, and successfully signs-on to the real system on the second try without any problems.

## C. Programming Acts

### i. Trap Doors

Trap doors are not actual crime techniques but, rather, are opportune tools by which other techniques can be employed in software alteration schemes. If discovered or created by programmers, they allow for the implementation of other methods and strategies that do facilitate crime. A trap door is a

---

35 A failure which is total or nearly so, such as: breakdown of power supply, making all circuits inoperative. Any type of failure which renders the useful performance of the computer to zero (Sippl, 1976: 174-175). The term 'crash' may be applied to a system as well as to software; when applied to a system it can indicate either a hardware or a software failure. A system or functional unit in which a fault or failure prevents continued operation is said to be 'down' and when it is corrected it is 'up' or 'back on line' (Galland, 1982: 97).

legitimate debugging device[36] which is included in the normal development of computer application and operating system programs (United States Department of Justice, 1979: 19). Debugging routines are coded breaks which allow programmers to access the software to ensure that corrections or additional codes can be inserted if the application of the program sustains specification modifications (Stark, 1975: 229). Large computer programs generally undergo a number of editing checks before the trap door is removed in the final edit, which, theoretically, should make the program secure from software manipulation (United States Department of Justice, 1979: 19). However, if the trap door is purposely left in the program after the final edit it may be exploited to gain access at a later time. This strategy allows the programmer to penetrate and subvert other protective devices implemented to defend the proper functioning of the computer system (Petersen & Turn, 1973: 78).

If a programmer is in a position to access an operating system program through a trap door, rather than just through an application program, the potential damage can be much more extensive. Operating system programs are designed to run the computer by establishing the parameters of control over other programs and data bases being used (Spencer, 1968: 40). They can

---

36 The operating statements provide a wide and flexible variety of methods for manipulating the program itself. The user may: (a) insert or delete statements; (b) execute selectively; (c) print changes of values as the change occurs and transfer control as the transfer occurs; (d) obtain a static printout of all cross-reference relationships among names and labels, and dynamic exposure of impartial or imperfect execution (Sippl, 1976: 121).

also be designed to limit access only to those individuals who are authorized to use the system by defining sign-on procedures, priority access codes, and identification numbers. By using a trap door, a systems programmer can compromise these requirements by removing all limitations to his/her account, which would permit access to every priority group and gain wider access to restricted data bases (The Ombudsman Committee on Privacy, 1976: 22).

ii. Trojan Horse Techniques:

The covert input of unauthorized instructions into a program that will perform fraudulent procedures is known as the 'trojan horse' technique.[37] The trojan horse will carry out the unauthorized instructions without inhibiting the functions of the program's intended purpose (United States Department of Justice, 1979: 11-12). Trap doors are often used in implementing trojan horses, since space must be found in the target program to insert the unauthorized instructions. Trap doors will allow entry into the program without compromising the structured code which, if tampered with, may default the entire program.

The complexity of the trojan horse technique is limited only

---

37 The term 'trojan horse' derives its meaning from the classic attack method used by the Greeks in their war against Troy to rescue Helen from Paris. The method involved the placement of a large, hollow wooden horse filled with Greek soldiers and left at the gates of Troy; it was brought inside the gates, thus leading to the destruction of the city.

by the imagination of the programmer. For instance, if a program has been accessed through a trap door, a programmer can develop a trojan horse which will create another trap door elsewhere in the program. When the original trap door has been removed in the final edit, the programmer will still possess access while others believe the program to be secure.

Both application and operating system programs are susceptible to trojan horse attacks. The trojan horse can be hidden amongst the 100,000 computer instructions contained in an application program, or the possible 5 million instructions for operating system programs (United States Department of Justice, 1979: 11). Of the many variants on the trojan horse technique, two are most notable.

Logic bombs are specific trojan horse instructions which are executed when particular conditions in the computer are established. Such conditions are determined by the parameters of programming logic which are inherent in the design of computer programs. Logic bombs rely upon the strict rules that govern program routines,[38] since their effectiveness depends upon the predictability of controlled events (United States Department of Justice, 1979: 21). For example, a programmer can instruct a logic bomb to search for particular data symbols and, once found, alter the data to the specifications of the fraudulent scheme.

Another variant on the trojan horse technique is known as the time bomb. This method is similar to the logic bomb, but it

---

38 A series of computer instructions which performs a specific, limited task (Sippl, 1976: 418).

differs in one major respect. The time bomb will run only when synchronized with the internal clock of the computer.[39] Only computer systems which possess this capability are susceptible to this form of trojan horse attack. The instructions are calculated to be set off at a previously specified time which is inserted in the target program. The computer operating system will count-down the time from seconds to years, and when the specified date is reached, the time bomb will be activated and the instructions executed (United States Department of Justice, 1979: 21). Time bombs are usually employed to place the perpetrator at a geographical distance from the scene of the crime or when immediate execution of logic bombs is impractical (Solarz, 1981: 37).

Superzapping[40] is another means of inserting a trojan horse into a secure program. This method involves the manipulation of the 'superzap' program which is used by many programmers as a 'fail-safe' device to bypass all controls in computer operating systems. The program is usually applied in situations where the computer malfunctions, and can not be restarted by normal recovery procedures. This universal access program will be

---

39 This built-in clock is used for a wide variety of program-timing purposes. It can be used to log the receipt times of periodic real-time input data. Each input message and its receipt time may be recorded together. This clock is also used in connection with the preparation of statistical and analytical reports dealing with the frequency of certain transactions (Sippl, 1976: 64).

40 The term derives its name from superzap, a macro/utility program used in most IBM computer centers as a systems tool (United States Department of Justice, 1979: 17).

used to open the system to inspection and, if necessary, modify the error which precipitated the malfunction.

However, if used for criminal objectives, the superzap program can be applied as an effective tool in the penetration and control of secure operating systems. By entering a system through the superzap utility program, it is possible to insert a number of trojan horses, making changes to application, production, and operating system programs (United States Department of Justice, 1979: 17). Perry (1986) describes one of the few documented cases of superzapping:[41]

> A classic example of superzapping occurred in a bank and resulted in a $128,000 loss. The computer operations manager was using a superzap program legitimately to make changes to account balances to correct errors as directed by management. The regular error-correction process was not working correctly because the demand-deposit accounting system had become obsolete and error ridden as a result of inattention during a conversion. The operations manager discovered how easy it was to make changes without the usual controls or journal records and transferred money to three friends' accounts. They engaged in the fraud long enough for a customer to find a shortage: quick action in response to the customer's complaint resulted in the perpetrators' indictment and conviction. Because the superzap program left no evidence of changes to the data files, it was highly unlikely that someone would discover the fraud through technical means (Perry, 1986: 218).

---

41 Case number CRC-18: see Chapter V.

### iii. Salami Techniques

Salami techniques[42] are directed toward the appropriation of small fractions of sums from numerous accounts (Kelly, 1984: 251). The effectiveness of this technique is assured by the insignificant loss each account sustains (United States Department of Justice, 1979: 13). Because individual losses are so small, usually fractions of a cent, victims are rarely aware they have been cheated. Salami techniques are not overly complicated; however, in most instances they are restricted to individuals with some accounting experience.

Traditionally, these techniques were used through manual manipulation methods, where the accountant would alter each file by hand, then carry over the discrepancy to the next account. This gradual method would continue until the balance sheet was in check. Many man hours were devoted to manual manipulation for limited gains, but with the speed of automation the process has become infinitely more simple.

If a trap door is discovered or created in an accounting program, the structured code can be modified by the use of the trojan horse technique to initiate the recurrent theft of small amounts. Only a few lines of code are required to bring

---

42 Also known as 'rounding': to delete the least significant digit(s) of a numeral and to adjust the part retained in accordance with some rule. The last digit displayed in an answer is increased by one if the following digit would have been a 5 or greater (Sippl, 1976: 418). The term 'salami' denotes taking small slices without noticeably reducing the whole (United States Department of Justice, 1979: 13).

about the necessary changes in the program (The Ombudsman Committee on Privacy, 1976: 22). The salami technique can be used in a number of different accounting applications, including: the computation of applicable service charges, commissions on sales, retirement benefits, and interest on savings (Krauss & MacGahan, 1979: 277).

Salami techniques do not seem to be worth the risk of detection, but considering that a few lines of code can be easily written and hidden in a program some programmers may be willing to take a chance (United States Department of Justice, 1979: 15). The only recorded example of a salami fraud is based upon an actual case which occurred in France in 1971, when a payroll clerk was authorized to round salaries down to two decimal places. However, instead of distributing the accumulating remainers to various other accounts, he collected them in his own; the total loss sustained by the corporation is unknown (Leibholz & Wilson, 1974: 37).[43]

iv. Simulation

Most complex program alteration schemes require extensive planning and meticulous implementation. Simulation is the process of testing crime strategies prior to actual execution. Each stage of the scheme is defined and operationalized to determine the possible disruptive effects on the system. The number of

---

[43] Case number CRC-19: see Chapter V.

influencing variables which must be taken into consideration in program frauds often exceeds the capability of manual preparation. By testing the scheme during development, all consequences of the event may be analyzed and corrected by the computer before the crime is initiated.

Simulation is generally employed when the complexity of the fraud may cause the system to 'crash'. In this case, the modified program defaults and causes the operating system to temporarily shut down due to unrecognizable error. The discovery of the modified code would be inevitable, since the program must be examined by the program analyst[44] to determine the reason for the crash. However, in most instances, crashes can be avoided when care is taken in the preparatory stages of crime development strategies.

Simulation can be used in two different types of criminal applications. In the first instance, they can be instrumental in the analysis of sophisticated frauds which require exacting accounting procedures or other specific knowledge qualifications. For example, one computer programmer of a large merchandise shipping firm simulated the company's accounting system for the purpose of a million dollar embezzlement which took place over a six-year period (Brandt, 1975: 82). He copied the original program, then inserted the modified transactions with the correct transactions and ran the program in reverse to determine if the

---

44 An analyst responsible for refining systems plans and diagrams into completely detailed steps necessary to give a digital computer unequivocal instructions for each minute step in a data processing operation (Sippl, 1976: 375).

modified entries in accounts payable and accounts receivable would match those of the original balance sheet (United States Department of Justice, 1979: 28). Once he had determined which accounts could be manipulated without audit detection, he then changed these accounts with programmed purchase orders and receipts which controlled the recorded differences on the original accounting sheet. All the funds were filtered into an associated 'dummy' company which he had established for the purpose of the embezzlement (Brandt, 1975: 82). The objective of the simulation was to test the viability of the scheme prior to actual execution.[45]

In the second instance, simulation techniques are often used to augment manual manipulation schemes which may be so intricate that they would not succeed without the direct assistance of the computer. In these cases, the simulation is not only used in the development and testing of crime strategies, but also in their implementation. Illustrative of this type of simulation application is a form of fraud known as "check kiting".

Parker (1983) explains the dynamics of this type of fraud, with a simple two-bank example:

> Check kiting in a two-bank fraud requires opening a checking account in each bank with small amounts of money. A check is then written for a large amount on one account and deposited in the other where it is immediately credited. Before the check is processed back to the first bank and it is discovered that there are insufficient funds to cover it, a check is written on the second bank and deposited in the first bank to

---

45 Case number CRC-20: see Chapter V.

> cover the first check when it arrives. This process is repeated several times with increasingly larger checks (kites flying higher and higher), relying on the float time needed to process the checks. When the account balances are large enough, the money is quickly withdrawn from both accounts in cash, the fraudsman disappears, and the fraud is completed (Parker, 1983: 99).

Another such check kiting scheme described by Parker, occurred in London, England and was much more extensive. The twelve individuals involved opened multiple accounts in a number of different banks. The perpetrators realized the organizational problems would be substantial, so they recruited a computer specialist to direct their activities. With the aid of a microcomputer and a modified inventory control simulation prorgam, the fraud was planned and executed (Parker, 1983: 99).

The computer specialist altered the standard simulation program by substituting banks for warehouses and assets for stored commodities. The computer served as a central communication base where transactions could be monitored and recorded in the simulation program. As the other members of the group opened accounts all over London, the computer specialist documented each transaction and directed their activities for withdrawing the funds. The timing of withdrawals was extremely important, since a miscalculation would result in immediate detection. The simulation program functioned perfectly and the check kite was operating smoothly until the computer encountered an error and sustained a crash. In the resulting confusion, some members of the group were apprehended attempting to withdraw

funds that had not yet been processed. Subsequently, the kite collapsed and the computer specialist was arrested while still trying to discover what went wrong (Parker, 1983: 99-100).[46]

Even though the processing time of cheques has been greatly reduced, (it can take as little as two hours in some circumstances), there is still the potential for such schemes.

### v. The Asynchronous Attack

The last and, possibly, most sophisticated form of software manipulation is the asynchronous attack. This technique requires extensive knowledge of computer operating systems and programming skills. In order to fully appreciate the quality of the asynchronous attack, a rudimentary understanding of computer operating systems is necessary.

A computer is designed to perform sequences of internally stored instructions synchronously, in a fixed order, according to an internal clock (Parker, 1983: 94). Such instructions are based upon stored program arithmetic which establishes the parameters that specify the operations to be performed (Sippl, 1976: 80). These coded instructions can be distinguished from the logical instructions performed by the computer's operating system. In essence, an operating system is "an integrated collection of service routines for supervising the sequencing and processing of programs by a computer" (Sippl, 1976: 335). It controls all resources, including: storage management, peripheral devices, and

---

46 Case number CRC-21: see Chapter V.

language translation (Maynard, 1975: 135).

The operating system manages these resources asynchronously, "in which each operation starts as a result of a signal generated by the completion of the previous operation or by the availability of the equipment required for the next operation" (Spencer, 1979: 29). As each new job requests resources to perform specific instructions, the operating system assesses current demands on the system, then either delivers them immediately or causes the job to hold until the resources become available (Parker, 1983: 94). Therefore, even though the computer must function according to established internal instructions (synchronously), the operating system possesses the capability to assess current resources and distribute them according to demand or availability (asynchronously).

The asynchronous attack is directed toward the inherent weaknesses contained in the asynchronous functioning of computer operating systems, in that established conditions can be altered so that the changes are not recorded by the operating system. When these changes occur, the operating system performs instructions under false conditions and completely or partially loses control (Parker, 1983: 95).

Parker (1983) describes one type of asynchronous attack which utilizes the checkpoint restart capabilities commonly provided in large production programs. A checkpoint is a specific location in a routine where a check, or a recording of data, is made to provide a back-up copy of the processed data in case of system failure or error (Sippl, 1976: 57). Such checkpoint

recordings can take place every ten or fifteen minutes, or can be specified by the systems operator. This facility provides a copy of the production run up to the point of the last breakpoint dump.[47] Should a failure occur, the job can be resumed from the last checkpoint rather than from the very beginning. Checkpoint restart capabilities can save considerable time and money if an error in the system does occur, but they can also be exploited to obtain unauthorized access within the system (Parker, 1983: 95).

Such attacks are often prepared far in advance of the actual execution. The perpetrator knows when the target program will be run and has already created a modified back-up copy which will be installed at a specific checkpoint restart. If this information can not be obtained, then a reason must be created to crash the computer at the time of production that allows for the insertion of the modified back-up copy. Once the back-up copy has been installed, it will run the unauthorized instructions without obstruction from the operating system. The asynchronous functioning of the operating system has now been breached, since the original program parameters can no longer circumvent the unauthorized instructions of the modified back-up copy (The Ombudsman Committee on Privacy, 1976: 23).

Unauthorized instructions can include: changes to storage locations, which enables the perpetrator to access other areas

---

47 Also called 'dynamic dump', which is performed under the control of an application program during its execution. Such breakpoints are specified by 'dump routines' contained within the production or application program (Galland, 1982: 79).

previously classified; changes to the mode of operation, which will allow access to privileged user levels; and changes to the production program, which will permit access to protected data files used only by the operating system (Parker, 1983: 95).

## D. Electronic Acts

### i. Wiretapping

Wiretapping was once considered too risky and time consuming to be effective as a means of obtaining classified information, when other more conventional methods are available (Carroll, 1969: 155-158). It places the perpetrator at a distinct strategic disadvantage since he/she must remain at the scene while the interception of the desired data is in progress. However, with the expansion of computer telecommunications in the area of electronic funds transfer systems (EFTS), wiretapping is becoming more appealing as the potential gains outweigh the risks.

The quality of information being transmitted over such systems is taking on more serious dimensions as banks, brokerage houses, and stock exchanges are transferring billions of dollars each day in electronically stored assets over communication lines (Parker, 1979: 654). Wiretapping comprises two different methods of interception. Active wiretapping, involves direct connection to a communication line to obtain unauthorized access, and passive wiretapping involves the detection of electromagnetic signals emanating from a computer

through radiation. (Petersen & Turn, 1973: 77). What distinguishes the two types of interception is that, in passive taps, the perpetrator only listens to transmissions but, in active taps the perpetrator actually interferes with the transmission, either at the end of the legitimate processing or in its place (Whiteside, 1978: 135).

In active wiretapping, the interception of the information is, in itself, a straight-forward process but it can also create serious problems if the equipment being used is not capable of subverting the electronic security maintained by the computer facility. Since the interception and recording of data will inhibit the flow of transmission to the receiver, the pick-up device must possess buffer storage areas which will back up the information, then re-send it at the original speed (Walker & Blake, 1977: 9). Without such capability, the wiretap may be electronically detected through the differential staggering of transmission flow. Another method of avoiding detection may be to intercept the transmission, then send an error message indicating that the system is undergoing modifications and that the user should sign-off and try again.

If the target information has been successfully intercepted and recorded, the last stage of the process is the encoding of the data which may have been transformed by encryption techniques (Hoffman, 1977: 69-70). The procedures used in active wiretapping are uniform throughout a number of different interception applications. However, they will be exceedingly

more complicated and expensive if the wiretapper is attempting to intercept microwave or satellite communications (United States Department of Justice, 1979: 27).

Passive wiretapping is much more restricted in its capability than active wiretapping, but what it lacks in potential it makes up in safety and simplicity. Such techniques are more common as a threat to non-time-sharing computer systems, since the isolation and subversion of communication lines is not necessary. Passive wiretapping involves a method called electromagnetic emanation pick-up, which works on an entirely different principle than active wiretapping (Walker & Blake, 1977: 9).

The interception unit functions on the electromagnetic emanations of low-powered, shortwave radio transmissions, resulting from changing magnetic fields within the target component. (Walker & Blake, 1977: 9). The wiretapper installs the unit to his terminal, gains legitimate access to the system and directs the unit to intercept the transmission from other terminals without direct connection.

Such units are capable of detecting emanations from as far away as 75 yards (Walker & Blake, 1977:9), but are most effective in situations within 20 feet (Hsiao et al, 1979: 99). If the wiretapper is strategically located, he/she can possibly pick up transmissions originating from the system operator's console, which often involves sensitive or classified data (Miller, 1971: 241). The only possible means of protecting terminals from emanation interception is by the use of circuit supressors and filters. Because such safeguards are often expensive and

cumbersome to install, most corporations are unwilling to invest in this kind of protection, although it would greatly reduce the possibility of system penetration.

## E. System Hacking

System hacking[48] cannot be contained in any one type of computer-related crime technique previously discussed. Essentially, it is a form of electronic window-shopping, where the hacker attempts to discover methods to penetrate telecommunication networks by subverting security password procedures. Unauthorized entry is accomplished through remote terminals (which are usuallly small microcomputers) that are physically separated from the mainframe, but can be connected by communication facilities (Marbach, 1983: 43). The strategies for subverting computer systems can span the complete range of crime techniques depending upon the ingenuity of the hacker. However, the vast majority of hackers cannot afford elaborate technical equipment to breach secure systems, so they are often restricted to an educated form of 'trial-and-error' scanning. The identification of specific hacking techniques would require an extensive understanding of computer principles; for this discussion, some general characteristics are noted which are common to such an activity.

---

[48] Webster's Dictionary defines "hack" as: to cut or chop irregularly, in a bungling or aimless manner.

In most instances, individual hackers do not possess the technical skill or knowledge to penetrate a secure system, although, by combining their limited talents with others of similar objectives, they can effectively develop enough information to initiate a successful penetration. The hacker's primary sources of direction for breaking into different computer telecommunication systems are electronic bulletin boards (Cheney, 1984). Hackers generally work alone in the actual subversion of a computer system, but they rely heavily upon the pooled knowledge stored in specially created electronic bulletin boards. These boards are computerized mail drops, where users can communicate with one another on a wide range of topics (Enright, 1983: 52). Electronic bulletin boards can serve as both the object and the instrument of crime, but in either case, they provide the hacker with an invaluable intelligence source for developing strategies to penetrate computer systems. These illegal boards are often christened with names which clearly demonstrate their intended design, such as, "The Bandit Board", "Pirate's Cove", and "Teledungeons" (Marbach, 1983: 43).

Once an illegal bulletin board has been created and has become functional, it instantly becomes the exclusive domain of a select group of individuals. Not only can hackers post passwords and code access numbers of previously penetrated systems, but they can also develop complete strategies to penetrate unexplored systems with the aid of the application and utility programs supplied by the host computer (Cheney, 1984).

An ironic aspect of illegal bulletin boards is that they are often penetrated by other hackers. Because of this potential threat, hackers must protect their own systems by developing security programs to mask their illegal activities. A hacker who attempts to subvert another underground system is known as a TWIT,[49] an individual who is completely devoid of any ethics, even for fellow hackers (Sanders, 1983: 66). Their primary objective is to destroy or tie-up systems so others can not gain access. As a precautionary defence against such penetrations, all files will be protected by specially developed security programs. The protection of illegal files can, at times, reach ridiculous proportions yet, in some cases, for good reason. One of the most highly prized and guarded files in the hacker's inventory is that which contains information outlining the procedures employed in password subversion strategies.

The majority of password subversion strategies revolve around two basic methods: trial-and-error techniques, and covert acquisition schemes, each of which possess countless variations.

i. Trial-and-Error Techniques

Passwords are the most widely used procedures in access control security. They can comprise any combination of numbers, characters, or words, and are aimed at establishing the accountability of the user. Passwords are usually preceded by an

---

[49] Acronym for: TeleWizard at Inducing Termination.

identification number which allows the computer to determine the priority access level the user has been assigned, and the privileges to which he/she is entitled (Cooper, 1984: 38). Trial-and-error techniques consist of a number of different methods used in the actual breaking of ID numbers and passwords. The procedures used in such subversions are based upon simple forms of logical elimination and probability analysis. The hacker is aware that most computer networks require users to sign-on to the system by providing an ID number and password comprised of no more than eight digits (Walker & Blake, 1977: 54). For a hacker to successfully penetrate a computer network or time-sharing system, he/she must break both codes in sequence, usually using different techniques. The most commonly used password structures are fixed, functional, changeable, and random codes, which are used in relation to the extent of electronic security maintained by the computer network (Beardsley, 1973: 51).

Trial-and-error techniques always begin with the logical elimination of commonly used sign-on phrases, such as, SYSTEM, USER, SECRET, SIGN, PROG, etc, which are often quite effective in producing passwords (Parker, 1983: 60). If the hacker knows, or can obtain information on the victim, the elimination procedure can also include personal data, such as: names of friends, pet names, favorite sports teams, telephone numbers, etc. By testing the different combinations of letters within key words, a subversion is almost inevitable, since most users can not be bothered to memorize the long and often confusing code sequences they were originally assigned, changing them to simple,

straightforward passwords which are easily recalled (Beardsley, 1973: 51-52). Only after the hacker has exhausted all the possibilities afforded by logical elimination will he/she concentrate on the eight digit formula as a random entity.

Even in this respect, the hacker is not working completely blind. Many studies have been conducted which examine the frequency of alphabetic and numeric characters, the length of codes, and the use of different letter combinations in password construction (Kahn, 1967: 726). In one study that investigated password integrity, it was found that, of the 2339 passwords surveyed, 15 used only one character, 72 used only two characters, 464 used only three characters, 477 used only four characters, and 1,311 only five or six characters. If this study is typical of the length of passwords, it indicates that 44% of all passwords are composed of four digits or less (Parker, 1983: 59-60). If such probability analysis is used in combination with logical elimination, the chances of successful password subversion are greatly increased.

ii. Covert Acquisition Schemes

Covert acquisition schemes use a host of different crime techniques which are all directed toward obtaining passwords by guile and deception, rather than by enciphering code. Such schemes include, impersonation, scavenging, passive wiretapping, and piggybacking techniques. An example, using a variation on the pseudo sign-on attack, illustrates covert acquisition

schemes.

This possibly apocryphal case involved a group of computer students at a large American University who developed an effective scheme to obtain the ID numbers and passwords of all remote terminal users. The students sent notices to all remote computer users in the University indicating that the MODEM dial-up number used to access the computer system had been changed. The new dial-up number directed callers to the students own microcomputer, which displayed a simulation of the University's sign-on procedure. The simulation sign-on would initiate every time a user requested service. After the ID number and password of the user were recorded, the simulation program would indicate that the original dial-up number was, in fact, operational, and that the user should sign-off and try again, using the other number (Parker, 1983: 59).[50]

Students are notorious for their password subversion schemes. During the initial implementation of the Multics system[51] at the Massachusetts Institute of Technology, it was estimated that 90% of the password subversion schemes were the work of students under the age of 25. The Multics system also has the 'dubious distinction' of being the most penetrated time-sharing system in the United States, courtesy of the inquisitive students at M.I.T (Beardsley, 1973: 63).

---

50 Case number CRC-22: see Chapter V.

51 A general-purpose, multiple-user, interactive computer system developed by M.I.T. Project MAC (Beardsley, 1973: 63).

Both trial-and-error techniques and covert acquisition schemes can be used in combination in the penetration of any computer networking system. Many large corporations and government installations realize the potential of these methods to access classified data bases, and have taken extreme measures to ensure that their systems are secure from such subversion attempts. One such method is the development of "tiger teams" which are granted official approval to penetrate secure systems and discover programming flaws which allow for unauthorized access. Gillard and Smith (1983) comment on the objectives of tiger team security methods, and state:

> After observing how vulnerable those systems are firms are now forming 'tiger teams' to find holes in their computer security systems. These teams are composed of computer experts in systems, operating systems, applications programming, and physical security. They take a 'no holds barred' approach and attack the integrity and security of an entire computer system in order to find exposures and vulnerabilities (Gillard & Smith, 1983: 400).

One of the best documented cases involving the subversion of a secure operating system by a tiger team is the penetration of the Univac 1108 Exec VIII, conducted by the United States Naval Research Laboratory.[52] The tiger team was granted unclassified

---

52 The Univac 1108 Exec VIII used a "Multilevel Security System" MLS (i.e., unclassified, classified, secret) which restricted access to specified privileged users. Because the Univac's operating system contained over 500,000 lines of assembler code, it was inevitable that the tiger team would eventually discover a flaw and strip all limitations to the MLS (Whiteside, 1978: 157-158).

and unprivileged access to the computer system through remote terminals, and was directed to penetrate the system without aid from 'inside' intelligence sources (Whiteside, 1978: 124-125). The tiger team's first objective was to discover weaknesses contained within the Univac's operating system. Once found, they were exploited to modify the executive program, which controlled 'user access' to shared programs. The team then inserted trap doors into the shared programs which enabled them to read the identification numbers and passwords of classified users.[53] Once this breach had occurred, the team possessed complete access to any user files that were on-line at the time of the subversion attempt, regardless of privileges controlled by the MLS (Whiteside, 1978: 158). This successful penetration of a military computer installation clearly demonstrates the potential for hacker subversion schemes. Any computer system using remote access, time-sharing facilities, or multiple-access terminals is susceptible to hacker penetration.

A difficult task for the researcher who endeavours to examine the nature of technical skill and knowledge is to retain a sense of perspective on the types of violations which may be committed through the manipulation of computer technology. At one

---

53 The team used only thirteen seconds of computer time in the actual subversion of the Univac computer; however, it took eight hours to print-out the target data intercepted during the penetration. The team eventually copied over two million words of text, and possessed the capability to: steal all assigned user files; destroy all assigned user files; selectively rewrite user files; terminate the user run; control any device assigned the user; and use all the machine time allocated to the user (Whiteside, 1978: 125, 161).

end of the spectrum, sophisticated programming techniques, such as the trojan horse, the salami technique, and the asynchronous attack make full use of the computer's potential to serve as the instrument of crime. At the other end of the spectrum, crime techniques, such as scavenging, impersonation, and input manipulation tend to require less technical skill and knowledge, but seem to be much more prevalent, and in the long-term possibly more damaging. The question arises: what is the extent of each form of crime in relation to the totality of cases? The question may in part, be answered by categorizing computer-related crimes according to major indicators and organizing them in relation to a research design. The five crime classifications described (i.e., physical acts, transactional acts, programming acts, electronic acts, and system hacking) represent a general scheme which may be utilized for content analysis.

While technical skill and knowledge will not employed as a primary variable in the construction of the research design, it will serve as a secondary variable of analysis for the case study. The following Chapter describes the motivational and opportunity factors which also affect an individual's decision to engage in computer-related crime. The combination of these two variables will provide the basis upon which a research design may be developed.

## IV. Motivation and Opportunity

### A. Motivation

The concept of motivation is undoubtedly the single most difficult variable to examine in respect to criminal behavior. It possesses countless subjective attributes, and is susceptible to extreme psychological(internal) and environmental(external) fluctuations which can directly influence an individual's decision to commit a computer-related crime (Silverman, 1971: 315). As Horoszowski (1981) notes, the term motivation comprises different elements which are all instrumental in the decision-making process:

> The word chosen for the intellectual antecedent of the decision to act is motive, and the name for the emotional component is impulsion. Motive can be defined as an idea or thought of a given state of facts - in the past, present, or future - under the influence of which we make our decision to act in a certain way. Impulsion is the emotion that accompanies the motive in the process of making a decision. Motivation can be reserved for the much wider area of all of the psychological aspects of any causative factors (Horoszowski, 1981: 51).

Motive and impulsion are theorized to be the two fundamental components that direct an individual's behavior in relation to any desired objective.[1] However, motives can also

---

[1] Other authors use different terms to describe similar processes; for example, Silverman (1971: 315) uses the terms needs and drives to isolate the two components in motivation.

include "hundreds of different factors, most of them of a psychic nature" (Horoszowski, 1981: 51). Concentration on these factors has dominated criminological theory and, to a large extent, shaped the way we have come to view the criminal in relation to specific forms of crime.[2] A confusing aspect in the analysis of criminal motives is the relationship between motivation and intention.

> The arousal of a motive and impulsion before making a decision (which is reflected in the intent to act in thoughts concerning methods for the performing of the action) is a complex psychic process (Horoszowski, 1981: 52).

Although the specification of motives is invaluable in examining criminal behavior patterns, they are of less concern to the legal community, who only wish to specify the intention to act.[3] Motives are only indirectly addressed in the application of statute, since they are not instrumental in the determination of criminal responsibility. As Sutherland and Cressey (1978) note, "in most instances, however, motivation is

---

2 For example, the motives directing the mass murderer are vastly different and more difficult to analyze than those directing a common thief. The latter is principally motivated by financial gain; the former may be motivated by a number of psychological and even biological factors that can not be examined in light of any single criminological theory.

3 The legal definition of **crime** comprises two elements: **mens rea** (mental element) and **actus reus** (physical element). The coincidence of these two elements is fundamental to the study of criminal law. However, motivation **per se** is irrelevant to the definition of criminal responsibility (Parker, 1977: 124, 134).

ideally taken into account only in the **administration** of the criminal law, that is, in making a decision as to the severity of the punishment which should be accorded a criminal". Parker (1977) quotes the observations of Hall (1960) which effectively describe the distinction between motivation and intention:[4]

> ... when we ask questions about a person's motives, we are asking for data relevant to evaluation of his character or at least of the morality of a particular act. Given a motive, a relevant intention can be inferred. But the converse does not apply, i.e. one may be positive that certain conduct was intentional without knowing any motive for it (Parker, 1977: 133).

Although such distinctions are necessary in the determination of criminal liability, they are not overly relevant to the study of criminal motivations. As Hall (1960) noted, the study of motives is principally suited to the analysis of the character of the criminal, rather than the culpability which can be associated with a specific activity.

The following discussion on motivational concepts provides only a brief glance into those processes which influence individuals to engage in computer-related crime. In order to organize the numerous characteristics which may be applicable to such an examination, the Motivational-Control Taxonomy proposed by Straub and Widom (1984) will be used as a descriptive framework for analysis.

---

[4] See: Hall (1960)

## The Motivational-Control Taxonomy

Straub and Widom (1984) propose in their **Motivational-Control Taxonomy** that the majority of computer-related crime offenders can be classified into one of four motivational types, each of which can be distinguished by the different circumstances that precipitated the commission of the crime. They maintain that the structure of their taxonomy provides a suitable framework in which existing sociological and criminological theories can be demonstrated in relation to 'individual/environment fits.'[5]

The primary focus of their taxonomy specifically concerns the identification of the different types of offenders who participate in computer-related crimes based upon motivational factors. Their **Motivational-Control Taxonomy** describes 'ideal types' (which they admit are gross measures of actual offender models), that are not completely mutually exclusive, since specific forms of computer-related crimes may be committed by a number of different types of offenders. Nonetheless, their taxonomy does contain the necessary structure which will permit the inclusion of sociological and criminological theory as a descriptive basis in examining the motivational factors which influence individuals to engage

---

[5] Straub and Widom use the term 'individual/environment fits' to refer to specific offender models they have identified in their taxonomy, and the likely environments for criminality.

in computer-related crime. Table 1 presents the relationship between motivation and offender groups.

Table 1

**Motivation-Security Response Taxonomy**

| Type | Motivation | Groups |
|---|---|---|
| I | Ethical Ignorance | Professional abusers |
| II | Personal Gain | Amateur criminals<br>White-collar criminals<br>Embezzlers |
| III | Anti-Social Motives | Career criminals<br>System hackers<br>Deranged individuals |
| IV | Corruption | Corrupt high officials<br>Corrupt experts |

Table 1 Reprinted from Straub and Widom (1984) **NOTE:** Table 1 with modifications. p. 93

The basic characteristics of each motivational type will be first briefly described, then discussed in relation to those aspects which best clarify the processes preceding individual forays into the realm of criminality.

i. Type I (Ethical Ignorance)

Straub and Widom (1984) suggest that this group of offenders are characterized by their inability to assess the ethical responsibilities of their occupational positions, and are thus termed professional abusers. The majority of these individuals do not possess a sense of wrongdoing, and therefore lack the criminal intent to deprive the asset owner of anything of value. The primary motivational factor directing such individuals into the realm of criminality is ethical ignorance. This ignorance stems from a lack of understanding concerning the security procedures and safeguards established by corporate policy. Professional abusers do not view their unethical conduct as criminal, and rationalize their activities as simple gameplaying or folly.

Since professional abusers usually occupy highly technical positions, they maintain an "elitist attitude" concerning their capabilities and their rights to use the computer for challenging intellectual exercises (United States Department of Justice, 1979: 56-57). Such ethical violations have resulted in millions of dollars a year in lost man hours and wasted computer time and resources, and have led to debates regarding the utility of

criminal sanctions to control these activities. Sokolik (1980) states:

> In considering these motivations, one needs to remember that many persons in the electronic data processing field currently give effect to these motivations in what are commonly accepted today as playful, 'innocent incidents'. Such 'harmless' activities as making a Snoopy calendar or entering one's bowling scores into the computer can obscure what is correct, proper and legal. At the same time, these acts can, and have, spilled over into uses which provide a source of remuneration for the unauthorized user. They have also been a ready excuse for what is more surely a criminal act (Sokolik, 1980: 368).

Although Sokolik's views may demonstrate the general attitude of corporate managers, they are not necessarily illustrative of those in the legal community, who maintain that legislative restraint is a more prudent policy. Webber (1983) comments on the changes to the Canadian Criminal Code, and the resultant legal ramifications of criminalizing the activities of professional abusers:

> Do we need to make criminals of those who, without permission, programme chess games or create graphical displays of the 'Mona Lisa'? Present practices in the EDP community include such unauthorized computer antics as programming games, designing 'Snoopy' calendars, creating graphical 'pin-up' girls and so forth. Proposed changes to the Criminal Code 'Mischief' section would make criminals of these playful programmers. Such a criminalization regime would result in tyranny - the integrity of the criminal law would suffer (Webber, 1983: 226, 249).

The ethical violations of the professional abuser have become the focal point in the debate regarding legislative revision, and have directed considerable attention toward the lack of consistency in corporate policy concerning occupational behavior. Not all ethical violations revolve around simple gameplaying; they can also include more destructive activities that can escalate into professional 'one-upmanship' competitions which may result in substantial losses (United States Department of Justice, 1979: 56).

In one such case in California, programmers from competing firms were accessing each other's accounts through a time-sharing service. The innocent 'prank' soon intensified into a civil suit, when one programmer was charged with theft of trade secrets (Straub & Widom, 1984: 94). At the trial, it was discovered that such unauthorized accesses were common practice among the programmers from the two firms, and that, between the time of the programmer's arrest and trial, another 16 violations were reported (United States Department of Justice, 1979: 56).[6] The Canadian case of R. v. Marine Resource Analysts Limited 41 N.S.R. (2d) 1979 is another good example of how the unethical conduct of professional abusers can lead to criminal charges. The case concerned a group of researchers who were employed by the Department of Fisheries to develop a number of programs for the

---

6 Case number CRC-23: see Chapter V.

Marine Fish Division. After their contract expired, the researchers formed their own consulting company, specializing in marine analysis. In order to establish their position in the field, they required the programs that were developed for the government. Using their previous access codes they gained remote entry to the computer center and copied the programs without formal approval. The unauthorized access was detected by department officials and the researchers were charged with theft.

During the trial, it was noted that, although they received verbal approval to copy the programs, no official confirmation was granted, resulting in the violation of their contract. Even though such violations may result in civil or even criminal charges, it is often difficult to prove that the offender(s) intended to deprive the asset owner of something of value.[7]

Other ethical violations, such as making Snoopy calenders or playing chess on the computer during company time, can be attributed to a disrespect for corporate policy or an indifferent attitude concerning occupational responsibilities. In more serious cases, the professional abuser may enter into criminality by association with other individuals who regularly participate in such activities for personal gain or through criminogenic pressure. In these cases, the offender will then be classified as a Type II or Type IV violator, since the occupational

---

[7] Case number CRC-24: see Chapter V.

circumstances leading to the commission of the crime have been altered by a different set of motivational factors.

ii. Type II (Personal Gain)

This group of offenders is characterized by a wide array of different self-serving motivations which are all directed toward some form of personal gain. Both tangible benefits (monetary rewards) and intangible benefits (power, prestige, etc.) are the objectives of Type II offenders. Straub and Widom (1984) have separated these offenders into three categories: amateur criminals, embezzlers, and white-collar criminals.

Amateur criminals comprise a group of individuals who are motivated to commit computer-related crimes for economic reasons which are often beyond normal means of redress. In the majority of cases, amateur criminals resort to criminality as a means of alleviating personal problems which have been stimulated by financial difficulties. Krauss and MacGahan (1979) identify a number of different motivational factors which can lead to amateur criminality. These are presented in Table 2. Such individuals engage in criminality only when they perceive their personal circumstances reaching intolerable levels, and turn to crime in a sporadic fashion when no other possibilities exist for the resolution of their problems. As illustrated in Table 2, there is a preponderance of motivations directed toward the solution of personal problems created by financial difficulties. Although amateur criminals realize their

## Table 2

### Causative Factors for Employee Fraud

| M E N | |
|---|---|
| Living beyond one's means | 24.8% |
| Criminal character | 13.5% |
| Gambling | 13.0% |
| Alcoholism related | 10.1% |
| Influenced by women who benefited | 6.6% |
| Irresponsible | 4.0% |
| Extravagance of spouse or children | 3.9% |
| Bad business management | 2.9% |
| Family illness | 2.8% |
| Accumulation of debts | 2.8% |
| Bad associates (being a dupe) | 2.8% |
| Grudge against employer | 2.7% |
| Other causes | 10.1% |
| Total | 100.0% |

| W O M E N | |
|---|---|
| Living beyond one's means | 19.8% |
| Family expenses | 11.5% |
| Extravagance of spouse or children | 10.3% |
| Criminal character | 10.3% |
| Influenced by men who benefited | 9.0% |
| Desire for new start elsewhere | 5.1% |
| Family illness | 5.1% |
| Alcoholism related | 4.5% |
| Own illness | 3.8% |
| Bad associates (being a dupe) | 3.2% |
| Mental problems | 2.7% |
| Grudge against employer | 1.9% |
| Other causes | 12.8% |
| Total | 100.0% |

Table 2 reprinted from Krauss and MacGahan (1979) NOTE: The above statistics were based on a study conducted by the U.S. Fidelity and Guaranty Company, which included a sample of 845 men and 156 women (Krauss & MacGahan, 1979: 36) The authors failed to include the total number of cases in the above table.

abuses constitute criminal behavior, they will often seize available opportunities until their problems have been solved. For example, in 1973, a teller at New York's Union Dime Savings Bank, used input manipulation techniques to embezzle $1.5 million. The crime was uncovered only when police raided a bookmaking house and discovered that the teller was an habitual gambler who bet up to $30,000 a day on sporting events (Carroll, 1977: 24).[8]

Embezzlers comprise a greater threat to corporations and other financial institutions, since their activities are usually well planned and executed. Unlike amateur criminals, embezzlers are not generally 'opportunists', and will initiate criminal activities rather than wait for available opportunities. Embezzlers may be motivated by many of the same concerns as the amateur criminal (see Table 2), but are usually not directed into criminality by pressing financial need. A key motivating factor in most embezzlement schemes is the offender's confidence in his/her ability to execute the scheme without being detected. Such an attitude results from the 'monopoly of knowledge' many technicians possess over a specific form of asset, often with no internal checks (Tassel, 1972: 32).[9] The criminal activities of embezzlers are more likely to be better planned and executed than those of amateur criminals since they are not solely motivated

---

8 Case number CRC-25: see Chapter V.

9 Most embezzlement schemes involve the exploitation of assets by input manipulation techniques.

by pressures resulting from financial difficulties which can lead to hastily prepared schemes. For example, a group of employees of the Human Rights Administration in New York City created a fictitious labour force of 40,000 workers through input manipulation techniques. Over a nine-month period, $2.7 million was embezzled in fraudulent pay cheques. It has been estimated that as many as 30 employees may have been involved in creating the records and cashing the cheques. The scheme was discovered only when a police officer found a bundle of un-cashed pay cheques in one employee's illegally parked car (Van Tassel, 1970: 10).[10] The extent of collusion and the depth of planning enabled the embezzlers to hide their activities from administration officials and avoid detection for over 9 months.

White-Collar Criminals can include both amateur criminals and embezzlers. However, a primary distinguishing element in this group of offenders is the extent of collusion in the commission of the crime. White-collar criminals are more likely to be involved in computer-related crimes which necessitate a wide range of knowledge and skills, requiring the expertise of a number of individuals.[11] Because white-collar criminals are more likely to require assistance, there is a higher degree of

---

10 Case number CRC-26: see Chapter V.

11 Offenders have been found to require assistance in one-half of all known computer-related crimes, whereas ordinary white-collar crime, embezzlement for example, involves a low degree of collusion according to a study of 271 bank frauds and embezzlements (United States Department of Justice, 1979: 56).

association between those individuals involved in the commission of the crime than if the individual acted alone as in amateur criminality. For example, in 1971, the vice president of computer systems, the senior computer operator and three data entry clerks embezzled over $120,000 by input manipulation techniques in the transfer of dormant computerized accounts from the National Bank of Trenton in New Jersey (Carroll, 1977: 33). Motivations for white-collar criminals do not differ greatly from those of amateur criminals and embezzlers. However, they also tend to include intangible benefits such as the acquisition of power, prestige, and status through the manipulation of specific types of assets.[12] Straub and Widom's distinction between the three different offender groups in the Type II classification, is not based upon white-collar crime principles, but rather on the motivational factors that influence individuals to commit computer-related crimes.[13] Each offender group is motivated by different situational circumstances in environments that can be as diverse as their occupations. In attempting to apply theory to such

---

12 Such intangible benefits are those obtained in the Equity Funding fraud, in which public and stockholder confidence was maintained when policy making officials fraudulently created 60,000 insurance policies to cover the firm's dwindling assets (Bequai, 1978: 64).

13 The distinction between the four offender groups identified by Straub and Widom are not based upon any particular white-collar crime study. However, for the purpose of this examination, they will be used to clarify the motivational processes leading to criminality.

subjective indicators, it should be noted that any examination will be only a general reflection of the actual processes that lead to specific instances of criminality.

iii. Type III: (Anti-Social Motives)

Unlike the motivations witnessed under Type I and Type II classifications, the anti-social offender is led into criminality by a wide array of different motivational stimuli, many of which do not revolve around ethical ignorance or financial gain. Straub and Widom have identified three types of anti-social offenders: career criminals, system hackers, and deranged individuals.

Career criminals are, in many respects, similar to white-collar criminals in that their criminality is directed toward some form of personal gain. However, unlike white-collar criminals, this group of offenders may not occupy a position of trust within an organization that provides available opportunities for computer-related crime. The motivations directing career criminals (professional criminals) specifically revolve around a value system which solely concentrates on crime as a way of life. This 'professional' aspect of career criminality provides the offender with a value system that defines motivations, rationalizations and attitudes concerning the nature of the occupation. In this respect, the motivations directing career criminality are not overly different from those of other 'professional' occupations, since the behavior pattern becomes

homogeneous to a specific group. Sutherland and Cressey (1978) note:[14]

> The term **professional** when applied to a criminal refers to the following things: the pursuit of crime as a regular, day-by-day occupation; the development of skilled techniques and careful planning in that occupation; and status among criminals. The rationality of a professional criminal extends beyond acquisition of the manual and social skills necessary for executing the crime itself. It includes planning, prior location of spots and victims, and prior preparation for avoiding punishment in case of detection. It is the rational system for making these arrangements, as well as the use of technical skills, which distinguishes professional thieves from ordinary thieves (Sutherland & Cressey, 1978: 277-278).

The extent and nature of career criminality in relation to computer-related crime has not yet been determined, since available statistics on this offender population are inconclusive. However, some authors have speculated about the future potential for career criminals in computer-related crime. Sokolik (1980) states:

> The mere fact that increasingly large sums are being stored in computers, and that they are exposed to relatively undetectable thefts, leads some to predict greater interest and involvement by career criminals. Certainly, the capability to commit these crimes is readily available to them. Amassing the specialized talents, such as those of programmers, accountants, wiretappers and burglars, would also not be new to them (Sokolik, 1980: 367).

---

[14] See: Sutherland (1937). Sutherland's analysis of the professional thief includes a descriptive discussion of the value system which directs this form of criminality.

Although there is no evidence indicating that career criminals have attempted to enter into the area of computer-related crime, they may soon represent a growing threat to financial institutions which are unprepared to deal with the problem of professional crime.

**System hackers** are often characterized as young, middle-class males, who participate in computer-related crime as a means of expanding their knowledge and skills in computer technology. The initial motivating stimulus directing this offender population is the subversion of computer telecommunication networks for the purpose of academic or intellectual challenge (Gillard & Smith, 1983: 403). The motivational characteristic of subverting computer systems for 'challenge' tends to be unique to this group of offenders, and although their behavior is often viewed as delinquent, there is some question as to whether the activities of system hackers can be considered criminal.[15] Beeler (1983) comments on the benign motives of system hackers:

> Most hackers are a reasonably responsible, admirable bunch whose actions are motivated mainly by curiosity and seldom pose a serious threat to the objects of their scrutiny (Beeler, 1983: 8).

The majority of system hackers are not motivated by direct financial gain; however, in some instances they have caused

---

15 See: Webber (1983). Specifically his discussion on the utility of deterrent legislation regarding unauthorized access attempts.

some damage to valuable data and information.[16] As a result, much media attention has been directed toward the 'playful antics' of system hackers, particularly when computers have been used to subvert classified data bases or used as a means of intimidation.[17] Although many system hackers are motivated by the 'challenge' of subverting computer systems to demonstrate their skills and capabilities, they also require the recognition that accompanies a successful penetration. The continuation of the initial motivation (challenge) is provided by the reinforcement and approval given the individual hacker by his/her immediate reference group. The sociological process is similar to that of white-collar criminality. However, the primary motivating impetus is not directed toward personal financial gain.

Deranged individuals comprise the most unpredictable offender population, since their activities often revolve

---

16
Illustrative of such unintentional destruction is the Dalton School case which occurred at a private New York City school in 1980. Twenty-one Canadian data bases were accessed via modem by a group of students resulting in extensive damage to the data base of Canada Cement Lafarge (Canada. House of Commons, 1983: 7: 31). Case number CRC-27: see Chapter V.

17
The notoriety of a young group of individuals calling themselves the 414s has prompted the greatest media attention. The group has been suspected of accessing at least 60 businesses and government installations, including; the Los Alamos National Laboratory, Security Pacific National Bank, and New York's Memorial Sloan-Kettering Cancer Center (Marbach, 1983: 42).
Case number CRC-28: see Chapter V.
Also of note is the 'technological revenge' taken against Richard Sandza, a Newsweek reporter, who wrote an article concerning a number of hacker groups which found his story inaccurate and highly insulting. The hackers accessed a number of different data bases, changing Sandza's credit file history and other personal information (Sandza, 1984: 81). One of the few "hacker cases" that clearly demonstrates criminal intent.
Case number CRC-29: see Chapter V.

around motivations that do not directly benefit the individual offender.[18] Such individuals engage in computer-related crime for the purpose of upholding a moral or social position, which they feel can be best demonstrated by destructive attacks directed toward computer installations.[19] Carroll (1977) notes a number of such cases which have all concerned some sort of 'revolutionary cause'. Once again, the continuation of the initial motivating stimulus is a group process, which involves the recruitment of specific types of individuals who possess similar concerns and aspirations as the immediate reference group, and are willing to participate in computer-related crime as a means of acceptance.

Deranged individuals can also comprise a wide group of offenders, including protesting students, laid-off or fired employees, and those engaging in computer-related crime as a

---

18 Straub and Widom use the term **deranged individuals** to refer to offenders who are "unsocialized in their motivations... Expressive crimes, exemplified by psychopathic computer criminals, cannot be deterred inasmuch as it is the criminal act itself which is the motivating factor, not any financial gain that accrues from the act" (Straub & Widom, 1984: 95-98).

19 In 1971 the **Revolutionary Force** attempted to destroy IBM's computer center in New York City by a bomb attack which caused extensive physical damage (Carroll, 1977: 16-17)
**Case number CRC-30: see Chapter V.**

Similarly, in 1976, the **Red Guerrilla Family** bombed the integrated circuit laboratory of the Hewlett-Packard Co. in California, causing $75,000 worth of damage (Carroll, 1977: 17).
**Case number CRC-31: see Chapter V.**

Also in 1976, the **People's Forces** detonated fire bombs in close proximity to the data processing center of the Central Maine Power Co. The group was protesting the role of computers in the expansion of nuclear power (Carroll, 1977: 17).
**Case number CRC-32: see Chapter V.**

means of obtaining personal satisfaction by undermining the organizational policies of the corporation or institution. These offenders possess motivations which are uniquely distinct from those involved in revolutionary or terrorist activity, and often engage in computer-related crime as a sole agent without the reinforcements provided by the group. Chalmers and Edwards (1982) note the distinction between the motivations of disgruntled employees and those of terrorists:

> Ideological goals - Motives in this category may range from a nihilistic desire to destroy "the system" to highly sophisticated terrorist efforts in support of foreign ideologies. Individuals with this type of motive can be extremely dangerous, since their motivation may be difficult for others to understand or predict.
> Revenge - An individual may have a vendetta against a former employer or an organization if the individual feels he or she has been wrongly treated. Like those who seek to do damage for ideological reasons, these individuals can be very dangerous because their actions are governed by malicious emotions (Chalmers & Edwards, 1982: 9).

Even though the motivations for this group of offenders may be vastly divergent, they are often expressed by some form of physical destruction.[20]

iv. Type IV: (Corruption)

This group of offenders comprises individuals who possess extensive occupational power, and are capable of inducing

---

20 The use of physical destruction as a means to disrupt computer operations is the least sophisticated form of computer-related crime in terms of technical skill and knowledge, although it is the most visually expressive.

criminality in others by providing the rewards for compliance or the sanctions for noncompliance. Straub and Widom have identified two different types of offenders under this classification:[21] corrupt high officials and corrupt experts. Both types of offenders engage in criminality in a relatively 'closed' organizational environment, which is conducive to the application of criminogenic pressure to advance corporate policies. The nature and scope of collusion associated with Type IV offenders is also of importance in the analysis of criminogenic motivations. These are, to a large extent, shaped by a normative structure which stresses the benefits of conformity to the 'common good' of the corporation.

Corrupt high officials are especially capable of stimulating the environmental conditions needed for occupational criminality by promoting the rewards which accompany the fulfillment of corporate objectives. The fundamental distinction between the motivations that direct corrupt high officials and white-collar criminals is the organizational setting in which the criminality occurs. Unlike the motivations associated with white-collar criminals (e.g., personal financial gain), the criminality of corrupt high officials is directed toward corporate, rather than individual, objectives (although personal financial gain

---

21 The distinction between these two offender groups is not entirely clear. For the purpose of this analysis, they will be examined in relation to the differences in their spheres of influence. Whereas corrupt officials possess the occupational power to formulate policy concerning organizational deviance, corrupt experts possess the necessary skills and knowledge to influence others to initiate the policy.

often results from such cooperation in organizational deviance). The U.S Department of Justice (1979b) notes the manner in which corporations can influence individuals into participating in criminal behavior:

> By emphasizing its own goals, the corporation attempts to provide its members with a set of guidelines within which they act for the benefit of the corporation. A variety of justifications are available for those who are confronted with doubts or guilt feelings, and these justifications allow them to neutralize the negative connotations of their behavior (U.S. Depatment of Justice, 1979b: 8).

Ermann and Lundmann (1982: 70) maintain that corrupt high officials are provided the avenues for criminogenic influence by the internal social structure of the corporation, which (1) rewards executives for short-term successes, (2) does not penalize executives for long-term failures, and (3) shields executives from responsibility. Each condition provides the executive with incentives to pressure employees into acting in accordance with corporate objectives whether illegal or otherwise.

The primary motivating factor inducing corporate criminality is the emphasis placed upon short-term profits as an indicator of productivity. The resultant pressure within the corporation to meet such objectives can create the conditions which contribute to organizational deviance. Clinard (1983: 17) notes that it is "the diffusion of responsibility, and the hierarchical structure of large corporations", which enable executives to

avoid direct involvement in the commission of the crime, while, at the same time, receiving the benefits that accrue from such activities. Decentralization within the corporation is an important aspect of the executive's ability to disassociate himself from criminogenic policies which may result in illegal behavior:

> Decentralization is, almost by definition, accompanied by the establishment of elaborate hierarchies, based on authority position and functional duties. This allows the abdication of personal responsibility for almost every type of decision, from the most inconsequential to those that may have a great impact on the lives of thousands. Under these conditions almost any type of corporate criminality...is possible. Executives at the higher levels can absolve themselves of responsibility by rationalizing that the operationalization of their broadly stated goals has been carried out without their knowledge. No single individual at the highest levels may make a decision to market a faulty product or take short cuts on product testing; instead, such decisions are made in small steps at each level (U.S. Department of Justice, 1979b: 7).

By aligning corporate objectives with those of individual members, executives can also provide employees with the motivations which enable them to rationalize their involvement in criminal activities. Clinard (1983) states:

> Individual members in a large organization generally become linked to the organization's successes and future goals. Since the interests of the members and the organization coincide, employees may engage in behavior that is unethical or unlawful, 'using the skills, knowledge and resources associated with their position to do so' (Clinard, 1983: 14).

Although rarely engaging in the illegal behavior as key participants, corrupt high officials nonetheless provide the operational mandates for action. Instrumental to the success of any policy requiring the illegal manipulation of assets are corrupt experts, who possess the technical skill and knowledge to implement sophisticated computer-related crime techniques.

Corrupt experts occupy strategic positions within the corporation which give them considerable authority over technical personnel, support staff, and other individuals involved in the operation of a computer center. Their 'positions of trust' provide ample opportunities to recruit personnel who may be required in the illegal activity, either in an active role (participating as a key actor in the activity) or in a passive role (omitting to take action to alter the course of the activity). The decision to commit a computer-related crime originates at the management level, which eventually filters down the corporate hierarchy to those experts who actually implement the policy. Like the employees they themselves influence, corrupt experts are similarly manipulated by policy-making officials for the well-being of the corporation. The interrelationships which result from such widespread collusion often assist in perpetuating the criminal activity, which may include the entire spectrum of employee involvement.[22] The motivations associated with corrupt experts are likewise directed toward

---

22 A good example of the collusion necessary in large scale, computer-related frauds is the Equity Funding Case.

furthering corporate objectives, however, they may also include many self-serving goals. The association between corrupt high officials and corrupt experts is illustrated by a case which occurred in 1971 in Dallas, Texas. The case involved an intense inter-industry rivalry between two software development firms competing in the same market. One of the firms, Information Systems Design Incorporated (ISD), developed a sophisticated plotting program which was far superior to that of its next major competitor, University Computing Company (UCC). In order to retain its position in the market, officials at UCC deemed it necessary to obtain the code contained in ISD's program.

Working under direction from senior management, a UCC programmer gained remote access to ISD's files via a time-sharing service that was used by the firm for program design. The programmer's technical skill enabled him to copy, then transmit, the program to his terminal, were it was printed-out for analysis. The unauthorized access was detected, and the UCC programmer was eventually convicted of theft of a trade secret.[23] Without direction from upper management, the programmer would probably never have attempted the remote access; similarily, without an awareness of the programmer's technical ability, management may not have considered such a course of action (Carroll, 1977: 31).

---

23 Case number CRC-33: see Chapter V.

## B. Opportunity

A large amount of data have been collected concerning the nature of opportunity factors and how they can affect an individual's decision to commit a crime. The majority of studies conducted in this area have specifically addressed the environmental conditions conducive to criminality, and how they can be altered to deter, or at least contain, criminal behavior.[24] Such research objectives have provided valuable insights into the manner in which offenders identify criminal opportunities.

### i. Environmental Vulnerabilities

As noted in Chapter III, numerous vulnerabilities within the technological environment provide opportunities for criminal activity. Such environmental vulnerabilities often enhance other types of opportunities which are available to a number of different offender groups. Beavon (1984: 32) lists three important elements which may influence how individuals perceive criminal opportunities:

---

[24] For further reading in the area of environmental opportunities, see: Rengert (1981) and Brantingham & Brantingham (1978).

1) objective site selection; 2) spatial attractiveness; and 3) target attractiveness. All three elements are relevant when considering how opportunities are identified and exploited. Expanding upon Beavon's (1984) examination of criminal opportunity factors, the following observations can be made concerning the computerized environment.

## Ojective Site Selection

The objective selection of a site which will provide access to a susceptible asset is the first process in the identification of criminal opportunities. This can be examined in relation to two factors: 1) familiarity with the technological environment; and 2) confidence to manipulate that environment.

An individual's familiarity with the technological environment is largely based upon the level of technical expertise acquired through practical experience. Therefore, an individual with little or no technical expertise will not resort to computer-related crime, if comparable rewards can be more safely obtained in manual systems. However, even if individuals are familiar with the technological environments in which they operate, they may not possess the confidence to take advantage of available vulnerabilities. For example, a data entry clerk in marketing and sales who wishes to engage in criminality is unlikely to embezzle funds from an accounts payable file, whether he/she possesses the required access or not. Objectivity in site selection (manual or computerized) is thus a

combination of familiarity with, and confidence in manipulating, the technological environment.

## Spatial Attractiveness

Spatial attractiveness is determined by an individual's relative proximity to exploitable vulnerabilities. An opportunity to engage in criminality will demonstrate little spatial attractiveness if the individual must manoeuver into a position that creates suspicion or mistrust. In this respect, there are two possibilities of enhancing the spatial attractiveness of a vulnerability: 1) ascribed proximity; and 2) acquired proximity.

Ascribed proximity can be obtained only through such mechanisms as promotion, occupational relocation, or transfers to different operational departments. Little effort is required to develop criminal opportunities if they are presented to individuals as a result of ascribed proximity. For example, if the same data entry clerk was transferred to the accounts payable department and received sufficient instruction in accounts update procedures, not only would the spatial attractiveness of the vulnerability increase, but so would the clerk's confidence in his/her ability to manipulate the asset. Ascribed proximity is generally restricted to the occupational setting, since outside perpetrators are not in a position to receive such environmental leverage.

Acquired proximity, on the other hand, necessitates the development of conditions which, in themselves, lead either to the

attainment of ascribed proximity or directly to the environmental vulnerability. The mechanisms which may facilitate such proximity include increased technical expertise through education, collusion with others who possess ascribed proximity, or coercion. Acquired proximity can be obtained either internally or externally to the occupational setting. System hackers provide excellent examples of how acquired proximity can be achieved by 'outside' sources through the exploitation of telecommunication vulnerabilities.

## Target Attractiveness

Target attractiveness encompasses three factors which enable individuals to determine the relative worth of exploiting an environmental vulnerability: 1) assessment of the lucrativeness of an asset; 2) assessment of a successful subversion; and 3) assessment of the possible consequences of the crime.

The lucrativeness of an asset can be considered in terms of the tangible or intangible benefits which an individual will receive from acquisition. Tangible benefits which represent monetary value may include: the disclosure of confidential information for profit; the theft of physical assets and resources; or the embezzlement of electronic funds. Intangible benefits which represent non-monetary value may include: revenge (disgruntled employees); ideological causes (terrorist/radical groups); and challenge (system hackers). The desirability of either type of benefit is, to a large degree, dependent upon an

individual's assessment of a successful subversion, and the possible consequences which may result from failure.

A successful subversion of an environmental vulnerability will be assessed in terms of an individual's perception of its ease of access. The initial decision to attempt access and acquisition of susceptible assets (given that the site has been identified and proximity achieved) will be based upon the extent and quality of computer security maintained by the organization. Obviously, an individual wishing to engage in criminality will be more likely to attempt a subversion if controls are patently inadequate. For example, if an organization does not possess proper password procedures to validate the authority of legitimate users, it may be more prone to employee abuse/crime, as well as system hacking (if the organization possesses telecommunication capabilities). The possible consequences of failure can be considered in terms of a wide array of different occupational repercussions, public and professional stigma, and legal sanctions.

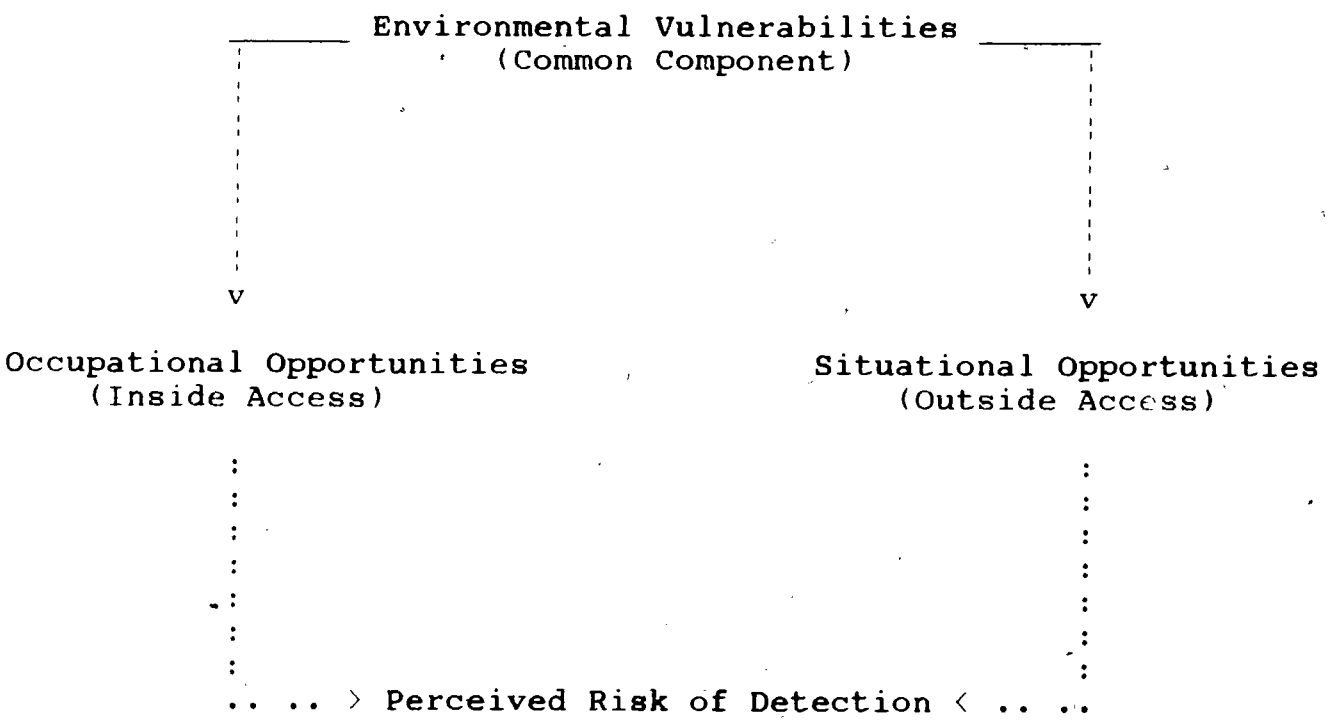
Each element contributes to the decision-making process when one assesses the opportunities contained within computer systems. Beavon (1984) maintains that, if an individual perceives any one of the variables to be nonexistent, the probability of criminality diminishes dramatically. He states:

> In a locational sense an inaccessible opportunity is no opportunity at all. Likewise, if an opportunity exhibits no target attractiveness to the potential offender then it cannot be considered as an opportunity (Beavon, 1984: 32).

By synthesizing the concepts identified by Beavon (1984) a simple opportunity relationship emerges which may better explain the dynamics of criminal opportunities. As illustrated in Figure 1, the model possesses two opportunity components which are presented in relation to environmental vulnerabilities and perceived risk of detection.

Figure 1

Opportunity Relationships



## ii. Occupational Opportunities

In many cases, the occupational position of the offender provides opportunities which would not normally be available to those outside of the organizational setting. The technical skills which accompanies certain occupational positions enable some offenders to control particular aspects of the computer environment which may provide access to isolated assets. Such assets are usually exploited through abuses of trust, which are often well hidden within the occupational hierarchy. The capacity of the offender to perpetrate computer-related crimes is not limited by the nature of the occupational hierarchy (that is, those in top management positions do not necessarily possess the greatest potential for crime), but rather, by the identification of specific environmental vulnerabilities which may lead to the discovery of internal or external opportunities. In this respect, there are three possibilities for criminality: 1) Inside access/ organizational opportunities; 2) Inside access/ non-organizational opportunities; and 3) Inside access/ criminogenic opportunities.

### Inside access/ organizational

Criminal activities involving inside access/organizational opportunities are directed toward the identification and exploit-

ation of environmental vulnerabilities through the application of specific job-related skills. When examining cases concerning organizational opportunities, two observations arise: 1) the criminal activity frequently includes a breach of professional trust, in which the offender's organization suffers a direct financial loss; and 2) the type of crime committed (e.g., input manipulation, program alteration, etc.) can usually be associated with an offender's occupational position and level of technical skill and knowledge.

In his pioneering work, White-Collar Criminality, Sutherland (1940) describes the manner in which 'economically' powerful individuals can abuse their positions of trust within organizations in the pursuit of criminal objectives (Sutherland, 1940: 3). He observed that many of the crimes committed by the 'respected' classes in society involve a violation of delegated or implied trust. A fundamental ingredient in such crimes is the 'monopoly of power' which results from the acquisition of extensive socio-economic and occupational status. Many computer-related crimes also involve a violation of trust; however, the primary ingredient in such crimes is the 'monopoly of knowledge' which often accompanies occupations of a technical nature. The technical skill and knowledge which is necessary to operate within complex computer systems presents individuals with the opportunity to commit crimes without the knowledge of their employers, thereby violating the trust granted them.

Computer-related crimes involving abuses of 'professional trust' are often facilitated by a high degree of occupational collusion, which enables offenders to exploit numerous environ-

mental vulnerabilities. For example, in 1971, the Oshawa plant of General Motors of Canada was defrauded by a group of employees who implemented an elaborate input manipulation scheme. The employees, all occupying strategic positions in different sections of the firm's accounting department, input false documents into the computerized accounting system to indicate requests for payment of products from a fictitious company. The scheme involved the creation of false purchase requisitions, purchase orders, merchandise receipts and invoices, each of which required a different level of access to the accounting system. The depth of collusion enabled the employees to off-set the accounting entries which effectively 'masked' their activities from internal auditors (Carroll, 1977: 24).[25] The above case demonstrates the manner in which employees may abuse the professional trust granted them; it also illustrates how the application of specific job-related skills can be used to perpetrate computer-related crimes.

Swanson and Territo (1980) identify four basic occupational functions which are performed within a computer system (technical capabilities) and compares them to the various types of operations susceptible to computer-related crime. Of the four basic occupational roles presented in Table 3, the systems analyst position[26] requires the most extensive background in terms of an

---

25 Case number CRC-34: see Chapter V.

26 A person who designs information-handling procedures which incorporate computer processing. The systems analyst is usually highly skilled in defining problems and developing algorithms for their solution ( Sippl, 1976: 8).

Table 3

Correlation of Technical Capabilities and Types of Operations Relating to Computer Crime

| Number of Personnel Capable | Technical Capabilities | Operations | Technical Skill |
|---|---|---|---|
| LOW | systems analysis and programming | communications and penetration of the operating system | HIGH |
| | application of programming | manipulation of auxiliary storage and programs | |
| | machine operation | operation of computer | |
| | data entry | input/output alteration | |
| HIGH | | | LOW |

Table 3 reprinted from Swanson and Territo (1980) pp.304-311

indepth understanding of computer operations. The skills required by computer programmers[27] and programmer analysts[28] are also extensive, but are generally restricted to the design, construction and analysis of computer programs. Computer operators[29] and data entry personnel[30] require only a rudimentary understanding of complex systems operations, since their positions are highly specialized and do not require a high level of diversified skills (Davis, 1965: 15). As indicated in Table 3, the number of personnel possessing the technical capabilities to perform systems analysis and programming is extremely low, yet the technical sophistication required to commit such crimes (e.g., penetration of the operating system, manipulation of programs) is relatively high. At the other end of the spectrum, the number of personnel capable of data entry is high, while the technical sophistication required to commit such crimes (i.e., input manipulation) is relatively low. There is an inverse relationship between the level of technical skill and

---

27 A person who designs, writes, and tests computer programs (Sippl, 1976: 375).

28 An analyst responsible for refining systems plans and diagrams into completely detailed steps necessary to give a digital computer unequivocal instructions for each minute step in data processing operation (Sippl, 1976: 375).

29 Usually operates the central console. May give some direction to lower level classifications. Studies run sheets. Reruns job steps to recover from machine error or program error, consulting with technical staff where necessary. Maintains machine performance and production records (Sippl, 1976: 82).

30 Data entry operators prepare and record a wide array of different data bases which are essential for corporate productivity. Their primary function is to ensure that all data have been correctly entered which will result in error-free processing.

knowledge required to commit sophisticated computer-related crimes, and the number of personnel capable of such manipulations. Table 3 would indicate that systems analysts may be capable of committing crimes at their own skill level, but also of levels below their position. However, personnel with only data entry skills would be unlikely to commit crimes involving high level program manipulations or the penetration of an operating system (Swanson & Territo, 1980: 310).

The English case of R. v. Thompson [1984] 3 all E.R. 565 (C.A.) illustrates how the application of specific job-related skills and knowledge allows some offenders to seize opportunities which are usually unavailable to others outside of the occupational setting. Thompson embezzled approximately $95,000 from the Bank of Kuwait by using high level programming techniques to manipulate computerized accounts. Employed in the Bank's computer department, Thompson used his access privileges to review dormant customer accounts which could be manipulated without immediate detection. After selecting five dormant accounts with substantial balances, he opened five corresponding accounts that would be used in the transfer of funds (Finlay, 1985: 117).

In order to ensure that he would not be associated with the illegal transfer, he programmed the computer to credit his accounts while he was on a trip to England (logic bomb). Once the transfer was complete, the program was coded to self-destruct leaving no evidence of his activity (time bomb). Cashing the funds was a simple matter of opening a number of English accounts

in various banks and requesting another transfer (Finlay, 1985: 117). Without an indepth knowledge of banking procedures and a high level of technical skill, the fraud could never have been accomplished. Fundamental to its success was the offender's familiarity with the banking environment and his strategic occupational position in the computer department, which enabled him to develop and implement a highly sophisticated fraud.[31]

Inside access/non-organizational

Criminal activities involving inside access/non-organizational opportunities are identified, planned, and implemented within an occupational setting, but are directed toward targets outside of the offender's organization. Although occupational resources such as computer time and equipment may be used in the development and execution of the crime, no direct financial loss is suffered by the organization. The majority of crimes involving non-organizational targets are often benign in nature and generally concern the activities of professional abusers. For example, in 1981, a number of Sperry Univac employees were convicted of fraud for using the firm's computer facilities and resources to create a music publishing program, which they intended to market through their own company (Thackeray, 1984: 6).[32] The activities of the Sperry Univac employees, while not intentionally criminal, were certainly unethical violations.

---

[31] Case number CRC-35: see Chapter V.

[32] Case number CRC-36: see Chapter V.

Other computer-related crime schemes involving inside access/non-organizational targets are not so benign in nature. For instance, one case that occurred in Dallas in 1971 involved an innovative programmer who developed a fraudulent billing program which charged companies for services rendered. The programmer imitated his own firm's billing procedure while on company time, but substituted the name of an innocuous sounding company, including the return address of a post office box that he had previously opened in order to retrieve the cheques. The programmer mailed the bills to a host of different companies and corporations in the Dallas area. Because the bills were printed-out by the computer and appeared to look official, many companies payed for the nonexistant services without question. Those companies which did complain that they had not received any such services were told by the programmer that the computer had made an error and the bill should be ignored. The scheme was finally uncovered when the programmer unknowingly sent a bill to an office of the Dallas Police Department which not only questionned the bill but started an investigation which eventually led to the arrest of the programmer (Canada, 1976: 20).[33]

Inside access/criminogenic

Criminal activities involving inside access/criminogenic opportunities can be expressed in two forms: 1) where management

---

33 Case number CRC-37: see Chapter V.

officials influence individuals within the organization to engage in criminality by providing the rewards for compliance or the sanctions for non-compliance; and 2) where management officials apply coercive economic market power to curtail competition through illegal business practices. In this respect, criminogenic opportunities can be applied either internally or externally, depending upon the nature of organizational goals.

In the first type of criminogenic influence, employees are directed into criminality by management officials for the purpose of furthering corporate objectives which can be realized only through illegal activity. Leonard and Weber (1970: 419-420) maintain that, where there is concentrated market power in any competitive industry, the conditions for coerced crime abound:

> Coerced occupational crime, whether performed by white- or blue-collar personnel, can be better understood when the conditions affecting the performance of occupational duties are known. In many industries and trades, criminal behavior in an occupation is conditioned by the concentrated market power of producers capable of establishing terms of employment and rewards for the occupation (Leonard & Weber, 1970: 419-420).

In one case which occurred in California in 1975, a newly hired employee of T & W Tool and Manufacturing Company (TWTM) was charged with theft and fraud for stealing computer time and programs from his former employer, Manufacturing Data Systems Incorporated (MDSI). Management officials at TWTM instructed the DP technician to gain remote access to the MDSI data base and copy a number of programs which were to be used in their

operations and accounting departments (Carroll, 1977: 31).[34] It is not uncommon for organizations to exert criminogenic pressure to obtain information or other proprietary assets from the former employees of competitors. Although the primary objective in the application of criminogenic pressure is to further organizational goals, individual participants may also obtain personal advantage through such incentives as promotion or increased benefits.

The second form of criminogenic influence concerns the exploitation of targets outside of the organization. Criminal activities are most often directed toward monopolizing specific markets through the application of illegal business practices. The threat of legal redress for instances of corporate criminality is often minimal, with little deterrent effect on the organization. As Goff and Reasons (1976: 492) have noted, the majority of investigative efforts concerning corporate crime have concentrated on small to medium range companies, leaving larger corporations free to engage in any practice without the retraint of enforcement.[35] Nowhere have such patterns of differential treatment been more evident than in the computer industry, which is saturated with a growing number of corporations competing in

---

[34] Case number CRC-38: see Chapter V.

[35] Although Goff and Reasons (1976) admit that some of the larger Canadian corporations have been investigated, they maintain that there is "an inverse correlation between the effectiveness of this government branch [Combines] and the size of the firms investigated, prosecuted and successfully convicted, finding that the largest corporations enjoyed a criminal-free record even though they engaged in much criminal activity" (Goff & Reasons, 1976: 492).

a highly centralized market. The largest computer corporations are often willing to undergo Combines or Antitrust investigation and possible conviction in order to corner a lucrative market. McCaghy (1976: 213) describes one example in which "the bigger strives to become even bigger without regard to legality or ethics":

> Few industries in the contemporary United States are quite as cut-throat as the computer industry. One of the tricks IBM has used to kill, or at least maim, competition was played on Control Data Corporation (CDC). In 1965 CDC entered the market with the world's largest computer. This announcement set CDC stock from 32 to 161 in a few months. But the stock was set tumbling and potential customers backed off when IBM announced it was coming out with an improved version of the CDC equipment. After the damage was done, the IBM machine never saw the light of day (McCagy, 1976: 212).

Although the above example did not involve any Antitrust violations, it does demonstrate the possibilities for criminogenic opportunities.

The case of Digidyne Corp. v. Data General Corp. 734 F. 2d. 1336 (1984) is a good example of how large corporations can exert coercive market power to curtail competition. The case revolved around an illegal industry technique known as "software lock-in", in which original equipment manufacturer's (OEM's)[36] are bound by contract to purchase products through tying agreements. Under

---

36 The term is used to refer to the intermediate manufacturers and distributors who purchase component hardware and software elements and then assemble them into complete computer systems (Smeltzer, 1986: 102).

such agreements, any OEM wishing to purchase one product (usually software), must, under the licensing terms, purchase another product (usually hardware) that has been specified by the developer. In this particular case, the Digidyne Corporation accused management officials of the Data General Corporation of using illegal tying agreements to prevent competitors from gaining access to the central processing unit (CPU) market (Smeltzer, 1986: 102-103).

The Data General Corporation ensured its prominence in the CPU market by licensing its powerful RDOS operating system software only to OEM's which also agreed to purchase its NOVA CPU. Because many OEM's required Data General's RDOS operating system to run their own application programs, they were "locked-in" to purchase the NOVA CPU as well. Other competitors in the CPU market could not develop similar RDOS operating systems to break Data General's hold on the market because of the prohibitive cost. Likewise, the OEM's which assembled their application programs with RDOS could not switch to another operating system without extensive and costly modifications to their programs (Smeltzer, 1986: 102-103). As Smeltzer (1986) notes:

> Thus, the power of the RDOS software copyrights ultimately restrained an appreciable degree of the competition in the CPU market. The evidence showed that 93 percent of Data General's NOVA CPU sales in 1979 were made to locked-in customers. Other CPU manufacturers could not compete for these OEM customers because the RDOS system was the only operating system that allowed the locked-in OEM's to use their own application software (Smeltzer, 1986: 103).

It was noted at trial that management officials at Data General devised the tying agreement scheme to recover the development costs of the RDOS operating system while, at the same time, generate a greater demand for its hardware product line. This case demonstrates how management officials can apply coercive economic market power to gain control of a specific aspect of the computer market.[37]

iii. Situational Opportunities

The term 'situational opportunity' is used to describe computer-related crimes that have not been facilitated by advantageous occupational positions. Such opportunities specifically concern crimes that have been planned and executed 'outside' of the occupational setting, without the leverage afforded by organizational protectionism.[38] The population of offenders engaging in situational crimes is vastly different from those identified as participating in occupational crimes, and possess a greater range of motivational stimuli. Situational

---

37 Case number CRC-39: see Chapter V.

38 Organizational protectionism can take a number of different forms. In the case of **corrupt high officials**, the organization will ensure the individual is not prosecuted, since criminogenic policies will come to light (as was the situation in the Equity Funding case). Likewise, **white-collar criminals** are rarely detected since they are afforded the protection of the occupational hierarchy, in which they can displace their criminality. Such forms of protectionism cannot be exploited by 'outside' offenders, unless they possess some type of knowledge which can be used to coerce 'inside' sources.

crimes are often unpredictable in nature, and are usually developed without the benefit of occupational skills or knowledge. Such opportunities can be separated into three types of 'outside' access: 1) independent outside access; 2) outside access through inside enlistment; and 3) outside access through inside infiltration.

Each type of outside access describes a different situational opportunity. Combined, they comprise the spectrum of possibilities permitted individuals without the aid of occupational leverage. However, situational opportunities do not preclude the exploitation of organizational weaknesses, such as enlisting inside employees or infiltrating an organization by outside sources for the purpose of criminal gain. The distinguishing factor concerning situational crimes is that the offence originated outside of the occupational setting, often taking advantage of available environmental vulnerabilities.

## Independent Outside Access

Independent outside access involves crimes which originate from sources that are completely divorced from the occupational setting. System hackers are good examples of this type of access. They rely only upon their knowledge of telecommunications and password subversion strategies to penetrate secure computer networks. In the majority of password subversion attempts, little, if any, inside knowledge is gained through

enlistment or infiltration techniques. More likely, the hacker will attempt to gather intelligence through such computer-related crime methods as impersonation, scavenging, and other covert acquisition schemes.

System hacking can be considered independent outside access, in that the anonymity afforded by remote entry shields the offender from the victim, as well as from possible detection through collusion. System hackers seldom seek the enlistment of inside personnel in penetration attempts, since such collusion places the hacker at greater risk. Although hackers actively engage in schemes that may cause the physical destruction or disclosure of valuable data, they consider the subversion and successful penetration of a computer network an academic challenge rather than an exploitable commodity. In this respect, hackers are willing to forfeit the inherent dangers of collusion for the safety of anonymity. Instances of independent outside access are usually restricted to remote entry schemes, which attempt to take advantage of the environmental vulnerabilities contained in weak telecommunication sign-on procedures.

## Outside Access through Inside Enlistment

This form of outside access is directed toward recruiting 'insiders' who may be capable of providing valuable information or intelligence[39] on the computer facility under consideration

---

[39] The term 'intelligence' is used to refer to information that will provide an outside perpetrator with valuable knowledge on possible methods of entry into the target organization (e.g., patrol guard schedules, remote terminal access codes, etc.).

for attack. Outside access through inside enlistment can be used effectively in three different types of situations:

1) In the acquisition of computer-generated information that can be sold for its illicit value: As illustrated in the case of R. v. Stewart [1983] 5 C.C.C (3rd.) 484, the accused was charged with counselling an employee of a large hotel to commit theft and fraud, by copying a computerized master-list of all hotel employees. The list was to be used in an attempt to organize hotel employees into a union to establish a bargaining unit. The list consisted of the names, addresses, and telephone numbers of 600 employees. The accused was willing to pay $6 per item, since this type of outside access is often accomplished through the bribery of inside sources.

2) In the acquisition of intelligence from inside sources which can be used to develop computer-related crime strategies: As noted by Parker (1983: 115) the majority of destructive acts directed toward computer facilities by terrorists involve some sort of assistance from inside sympathizers. Intelligence, in the form of access codes and passwords, can also be sold for its illicit value.

3) In the recruitment of inside personnel which will actively participate in the subversion of the computer facility: Inside personnel are usually recruited on the basis of their occupational skills and knowledge which can be used in the execution of computer-related crime techniques that would not normally be available to outside sources. In the case of United

States v. Jones 553 F.2d 351 [4th cir.] 1977, the accused recruited a data processing clerk who possessed the knowledge to alter data before they were entered into the computer. The objective of the scheme was to modify the accounts payable data to issue cheques to the accused's fictitious account. As the prosecutor in the case noted:[40]

> The defendent's accomplice in Jones directed an accounts payable clerk to set up computer documents under the name A.L.E. Jones that included a vendor #98844. He then altered Whirlpool Corp's vendor #99900 to #98844 to correspond to the spurious A.L.E. Jones account. Ultimately, the computer issued checks payable to the A.L.E Jones account that should have been paid to Whirlpool. The five checks thus issued authorized the payment of over $130,000 to the A.L.E Jones Account (United States v. Jones 553 F.2d [4th Cir.] 1977 353).

Because collusion is neccessary in frauds involving inside enlistment, the perpetrator is often at risk of detection. Although the outside source may be fully aware of the ramifications of his activities, the inside accomplice is usually naive about legal consequences, and may inadvertently place the scheme in jeopardy. More effective are schemes involving outside access through inside infiltration which do not require a high degree of collusion.

---

40 Case number CRC-40: see Chapter V.

## Outside Access through Inside Infiltration

Outside access through inside infiltration is the process by which the perpetrator enters into an occupational setting for the sole purpose of obtaining intelligence on the computer facility. By impersonating an employee or another individual who possesses access to the facility, the perpetrator can scavenge for valuable information that may be accessible to authorized personnel. The exploitation of physical vulnerabilities is the key to inside infiltration attempts. Physical security procedures are usually circumvented by bluff or intimidation. A classic example of inside infiltration occurred in 1972 when the president of a French software company impersonated a university professor while on tour in the United States. Visiting over 200 computer centers, the 'professor' of computer science collected numerous valuable programs, which he sold when he returned to France (Parker, 1976: 20).

The three types of outside access presented above are only examples of the possible schemes afforded outside perpetrators. Criminal activities involving situational opportunities are much more difficult to detect than occupational opportunities, since the perpetrator is often unknown to the target organization. Both occupational opportunities and situational opportunities are dependent upon weaknesses within the computer environment which provide the offender with the necessary tools to develop and implement computer-related crime techniques.

Organizations can dramatically limit such weaknesses by increasing the risks to potential offenders.

## Perceived Risk of Detection

Krauss and MacGahan (1979) maintain that an individual's perceived risk of detection is greatly influenced by the institutional policies advanced within the organization. Such policies direct occupational behavior, define professional ethics and attitudes, and clearly articulate internal controls and security measures (Krauss & MacGahan, 1979: 30). Although the enforcement of organizational policies may limit the extent of occupational criminality, it does little to deter instances of situational crime. Outside offenders are usually unaware of organizational policies and act according to different perceptions of risk. These perceptions may include an assessment of the technical skills involved in committing the crime, and the legal ramifications that may result from failure. As noted by Comer (1977):

> Stimulus conditions - including opportunities for action - presented by the immediate environment are seen (by criminals) to provide - in a variety of ways - an inducement for criminality. These are modified by the perceived risks involved in committing a criminal act; the anticipated consequences of doing so; and - in a complex and interrelated way - the individual's past experience of stimulus conditions and of the rewards and costs involved (Comer, 1977: 13).

Environmental vulnerabilities can provide attractive inducements to criminality. However, more fundamental to situational forms of computer-related crime is the offender's assessment of the costs involved in the subversion of a computer facility, which will usually include a perception of risk based upon legal sanctions.

As noted at the beginning of this chapter, criminal motivations can encompass countless psychological and environmental influences which can affect an individual's decision to participate in computer-related crime. It would prove difficult to assess each motivational influence in relation to its relative degree of importance in a highly specified classification scheme (e.g., each motivational influence treated as a separate class). The Motivational-Control Taxonomy Proposed by Straub and Widom (1984) has provided an organizational framework in which to examine major areas of influence. In this respect, the four motivational types described (i.e., ethical ignorance, personal gain, anti-social motives and corruption)[41] provide the necessary structure to account for the most general criminal motivations. More fundamentally, their taxonomy provides a mechanism to further synthesize motivational concepts based upon the expressed intent associated with different motivations. For example, the motivations of professional abusers (ethical ignorance) and system hackers (challenge) tend to illustrate benign or

---

[41] The terms used by Straub and Widom (i.e., deranged individuals) to describe offender populations does not necessarily reflect those of the researcher. Their terminology is based upon their own notions of criminality.

unintentional criminal activity. While the motivations of amateur criminals, white-collar criminals and embezzlers represent intentional violations which are directed toward financial gain. This basic distinction between the expressed intent associated with the different offender populations yields the first building block in the development of the research design.

Similarily, criminal opportunities can also present the researcher with numerous difficulties in designing research studies without a clearly defined area of investigation. The resultant interaction between the two major opportunity components stems from the underlying vulnerabilities that enable individuals to control a particular aspect of the computer environment. Both occupational and situational opportunities address the nature of the type of access, which permit computer system subversion. As the second building block, opportunity concepts may be incorporated into the research design through the introduction of white-collar crime theory.

Combining the two major components of motivation (expressed intent) and opportunity (type of access) results in a classification scheme which accounts for four areas of concern. While general in scope, the scheme nevertheless possesses the necessary research flexibility to examine computer-related crime through a number of different levels of analysis. Based upon the variables described in this Chapter, the following discussion is directed toward the development of an exploratory research design which will provide a framework for the collection and organization of data concerning computer-related crime.

## V. The Research Design

The first step in the process of examining any aspect of criminal behavior is to acknowledge the nature of the research undertaken in terms of the primary objectives of the study. The exploratory quality of this thesis is most clearly expressed in the conceptualization of a research design which can be used to organize data concerning computer-related crime. As Kidder (1976) notes:

> Many exploratory studies have the purpose of formulating a problem for more precise investigation or for developing hypotheses. An exploratory study, may however, have other functions: increasing investigators' familiarity with the phenomenon they wish to investigate in a subsequent, more highly structured study, or with the setting in which they plan to carry out such a study; clarifying concepts; establishing priorities for further research; gathering information about practical possibilities for carrying out research in real-life settings; providing a census of problems regarded as urgent by people working in a given field of social relations (Kidder, 1976: 91).

Exploratory studies are directed toward a formulative process in which research is initiated to gain insights into a particular area of analysis for the purpose of furthering academic speculation. This process proceeds from an in depth descriptive analysis of the related literature, which in turn,

provides the impetus for the conceptualization of research techniques that may be utilized in future studies. Intrinsic to this objective is the development of a research design which can provide a method for the organization and collection of raw data. Kidder (1976) states:

> Once the research problem has been formulated clearly enough to specify the types of information needed, investigators must work out their research design. A **research design** is the arrangement of conditions for collection and analysis of data in a manner that aims to combine relevance to the research purpose with economy in procedure (Kidder, 1976: 90).

The two variables described in the preceeding Chapter: 1) motivation; and 2) opportunity are fundamental conditions in the formulative process. However, before they can be employed for quantitative analysis, a research design must first be constructed. In this respect, the basic framework for a suitable design may be derived from the theoretical concepts associated with the study of white-collar crime. Specifically, the observations of Quinney (1964), who noted the distinction between occupational crime and occupational deviation.

A. Conceptualization

In his article, The Study of White-Collar Crime: Toward a Reorientation in Theory and Research, Quinney (1964) discusses

many of the theoretical problems inherent in the concept of white-collar crime, and proposes possible changes that may aid in conceptual clarity. Quinney maintains that the study of white-collar crime should be restricted to include only those violations of the criminal law that occur in the course of occupational activity, regardless of the social or economic status of the offender (Quinney, 1964: 285)[1] His reexamination of the conceptual variables used in research led him to develop his own model based upon the nature of occupational activity.[2]

Quinney suggests, that, in order to study the full spectrum of offences which occur within the occupational setting, a theoretical distinction should be made between occupational crime and occupational deviation. Although only offences in violation of the criminal law would be included under the heading of "white-collar crime", the study of occupational deviation may provide meaningful data regarding those abuses that have not yet been formulized into law, or that have become institutionalized

---

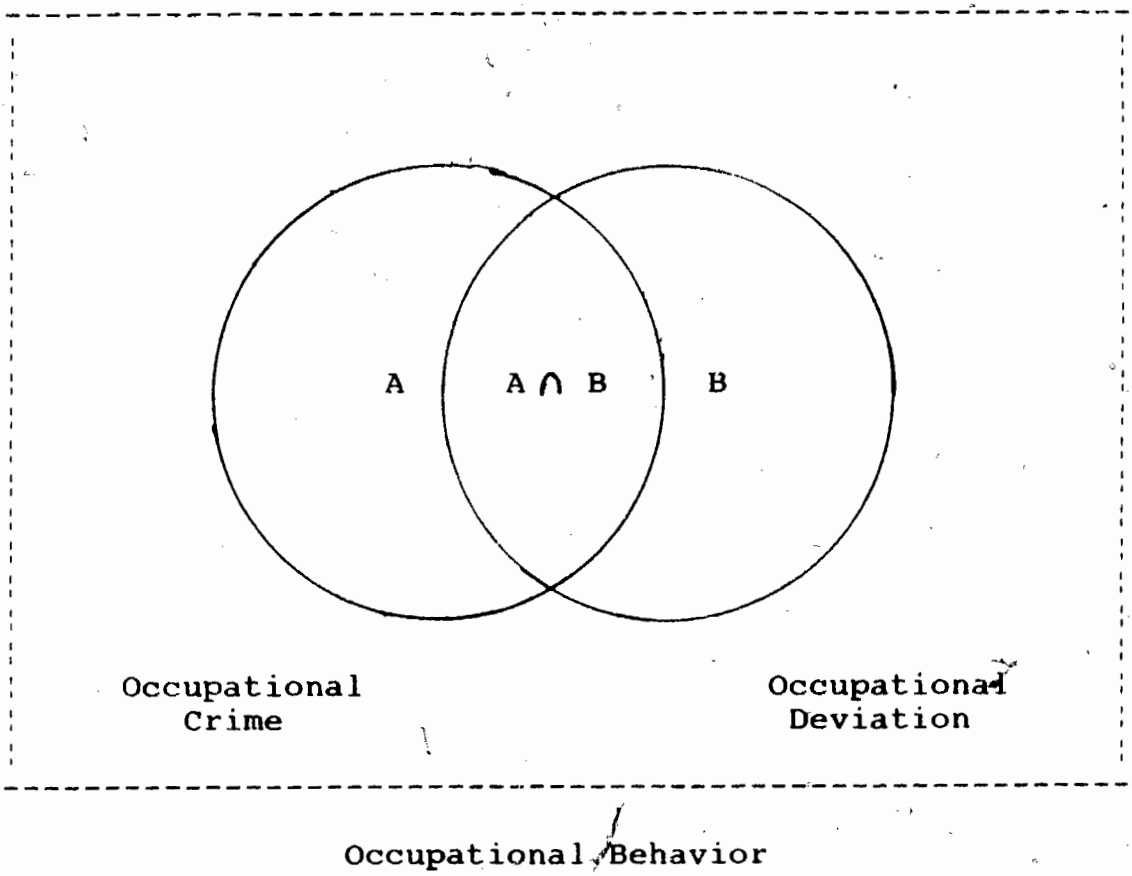
1 The majority of Quinney's criticisms concerning the concept of white-collar crime are directed toward the definition proposed by Edwin Sutherland in his 1939 Presidential address to the American Sociological Society, which reads: [a white-collar crime is ...] "A crime committed by a person of respectability and high social status in the course of his occupation, [which often involves] a violation of delegated or implied trust (Sutherland, 1940: 1, 3).

2 Quinney's observations concerning the nature of white-collar crime can be compared to those of Newman (1958) who states: "The chief criterion for a crime to be 'white-collar' is that it occurs as a part of, or a deviation from, the violator's occupational role...farmers, repairmen, and others in essentually nonwhite-collar occupations could, through such illegalities as watering milk for public consumption, making unnecessary repairs on television sets, and so forth, be classified as white-collar violators" (Newman, 1958: 102).

within a specific occupational context (Quinney, 1964: 287). Figure 2 presents the association between occupational crime and deviation in relation to occupational behavior.

Figure 2

Relationship Between Occupational Behavior, Occupational Crime, and Occupational Deviation



The variable indicators contained in this representation are illustrative of the different orders of behaviors that may be applicable to the study of white-collar crime, in which: Circle A designates all forms of activity which violate legal statutes (crime); Circle B designates activities violating occupational norms (deviation); and the intersection between Circle A and B designates activities which may be both a violation of legal statutes and occupational norms (Quinney, 1964: 288).

The relationship between crime and deviation would allow for greater flexibility in research design and would permit the researcher to hypothesize about the nature of occupational violations, thus expanding the research mandate beyond the limits designated by the criminal law (Quinney, 1964: 286). Quinney states:

> It is known that certain occupational behaviors which are usually regarded as deviant are legitimate in certain situations. There is, in addition, the fact that occupations are in a constant process of change, and occupational deviation (and sometimes crime) is a necessary concomitant of occupational change. The deviant or criminal is often an innovator. Occupational deviation and crime can be an indication of the development of new occupational norms (Quinney, 1964: 289).

Within this research design, the determination of what types of behaviors constitute white-collar crime are based upon legal definitions which have been specified by the Criminal Code, and are thus easily identified. However, the determination of occupational deviations (activities violating occupational norms) may prove more problematic to identify, since they are

often tied to the process of change. In this respect, all behaviors not defined as illegal, but nevertheless violate occupational standards of conduct, may be categorized as occupational deviations.

Conceptual limitations within the parameter of occupational activity, may prove effective in the analysis of such crimes as, employee embezzlement or price fixing, (which take place strictly within an occupational context, and illustrate changing normative patterns); but would be of marginal utility in the examination of crimes that are not solely restricted to an occupational setting. Ignoring violations which occur outside of the occupational environment would contain analysis to only one form of behavior, disregarding other valuable areas of interest. The first step in developing a suitable research design is to account for the situational forms of crime and deviance not contained within Quinney's model. By reformulating his original design to include violations which occur outside of the occupational setting, and only distinguishing between intentional and unintentional violations the basic structure of the research design emerges. The design address two major conceptual variables.

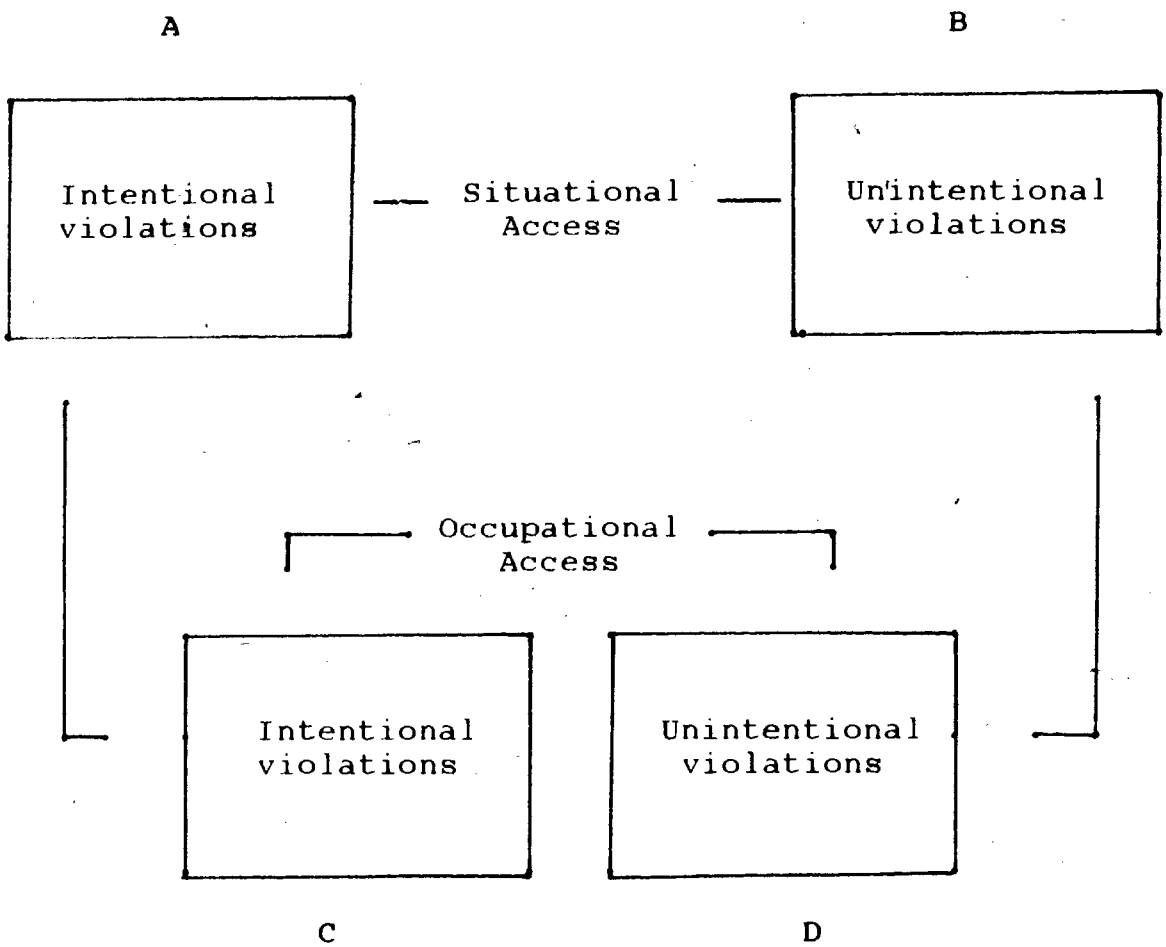
1) Type of access; and

2) Expressed intent.

As illustrated in Figure 3, the combination of the two conceptual variables results in four research indicators.

Figure 3

Relationship Between Research Indicators




Research Indicators

(A) intentional/situational access

(B) unintentional/situational access

(C) intentional/occupational access

(D) unintentional/occupational access

## i. Conceptual Variables of Analysis

Both conceptual variables have been derived from the descriptive analysis of motivation and opportunity presented in Chapter III. The first, type of access, is comprised of two indicators (situational and occupational access) which will provide a basis for the identification of principal opportunity concepts. The second variable, expressed intent, is a synthesis of fundamental motivation concepts, and is likewise comprised of two indicators (intentional and unintentional violations). The following discussion will describe the nature of these variables and their associated indicators in relation to the theoretical deficiencies contained within Quinney's original model; and demonstrate how they may better serve in the collection and organization of data concerning computer-related crime.

### Type of Access

Quinney's observations concerning the nature of white-collar crime provide the researcher with a suitable framework with which to examine computer-related crime within the parameter of occupational activity. However, in order to derive maximum utility from the concepts expressed in his model, they must be expanded to include violations which occur outside of the occupational setting. Because computer-related crime is not necessarily limited to, or a function of occupational activity, it cannot be examined under Quinney's original research design.

As described in the previous chapter, opportunities for computer-related crime are available to a number of different offender groups, both internal and external to the occupational environment. By extending the level of analysis to include both types of opportunity (situational and occupational), the new design encorporates the complete range of violations without restriction to the environment in which they occur.

**Expressed Intent**

In his model, Quinney uses the parameters of crime and deviance to identify the different orders of behaviors which may occur in an occupational setting. The distinguishing element between the two concepts is based upon legal definitions which are specified by the criminal code. In determining the legal status of any occupational violation for the purpose of analysis, Quinney suggests "that researchers must always make clear what order of behavior they are trying to describe and explain" (Quinney, 1964: 288). However, in relation to the intersection between occupational crime and occupational deviation, he notes:

> It should be kept in mind, however, that the circles representing occupational deviation and occupational crime could assume varying positions in the diagram and are likely to do so in reality. There is the possibility, for example, that the circles could be either mutually exclusive or equivalent, as well as vary in the degree of overlap. Also, either circle could contain the other, or one or both circles could be nonexistent (Quinney, 1964: 288).

The fact that one or both circles could "vary in the degree of overlap" presents the researcher with a distinct conceptual difficulty when attempting to code cases which may fall within the area of intersection. Although such a research design could yield valuable data concerning the changing nature of occupational norms, it is not particularily well suited for the study of computer-related crime. Moreover, because many of the cases presented throughout this thesis have not been judicially considered, the strict designation of "crime" as defined by legal statute cannot be applied as an indicator for the purpose of coding.

As noted in the previous chapter, the distinction between motive and intention is based upon the criminal liability that can be ascribed to a particular violation. Where motive is used to describe the character of the offence, intention is used to designate culpability. Recalling Hall's (1960) observation: "Given a motive, a relevant intention can be inferred", an alternative to Quinney's classification scheme can be proposed according to the expressed intent implied from a motivation.

Under such a scheme, cases demonstrating motives which are directed toward personal gain, physical destruction, or criminogenic influence, clearly express criminal objectives and are termed intentional. However, cases which demostrate motives which tend to be more benign in nature, such as, ethical ignorance, or intellectual challenge, may be termed unintentional. The term "unintentional" is used to denote cases which illustrate a lack of specific criminal intent to obtain or deprive

by means of destruction, disclosure or conversion anything which can be exploited for some form of gain.

### ii. Research Indicators

As presented in Figure 3, the research design is comprised of four indicators, each of which addresses dfferent aspects of computer-related crime. Using the offender groups identified in the previous chapter as a descriptive basis for analysis, the method for case organization will be discussed.

#### Intentional/situational access (A)

The most dramatic and destructive forms of intentional violations committed through situational access are acts of terrorism. Although Canadian computer installations have not yet fully experienced the disruptive impact of systematic terrorism, the European scene is much more explosive. Because of the diversity of terrorist organizations operating in Europe almost any computer facility, large or small, is a potential candidate for attack. Representative of the groups which specifically target computer installations for sabotage are: The Comite Liquidant ou Detournant les Ordinateurs (The Computer Liquidation and Hijack Committee: CLODO); The Cellules Communistes Combattants (The Fighting Communist Cells); and The Action Directe (Lamb & Etheridge, 1986: 44-45).

The intentions of such groups becomes evident when considering the underlying philosophy directing their actions. In a formal statement to the French press, CLODO expressed their views on computer technology:

> We are workers in the field of dp [data processing] and consequently well placed to know the dangers of dp and telecommunications. The computer is the favorite tool of the dominant. It is used to exploit, to put on file, to control, and to repress (Lamb & Etheridge, 1986: 44).

The perception that computers are used as tools of repression and control has enabled terrorists to recruit inside sympathizers who feel disadvantaged by the organization. Undoutedly, a contributory factor in their ability to circumvent computer security controls is the manipulation of such sources as a means of obtaining information or as active participants. More than any other offender group attempting intentional/situational access, terrorists have been the most successful. Other types of violations included under this indicator involve activities which are focused on acquiring personal financial gain. The "Schneider" case (CRC-16) is a good example of how individuals can implement computer-related crime schemes which have been developed outside of the occupational setting.

**Unintentional/situational access (B)**

Illustrative of unintentional violations involving situational access is system hacking. The origin of this form of deviant activity can be traced back to the early 1970's, when

"phone phreaking" became a popular recreation for technologically adventureous students.[3] Using the infamous "black box"[4] phone phreaks would electronically subvert telephone networks by simulating toll-switching signals to avoid payment of long-distance charges (Parker, 1983: 173). With the development of more effective detection methods, telephone companies soon inhibited the activities of phone phreaks, who responded by turning their attention toward subverting inadequately protected computer systems. However, unlike their predecessors, system hackers, are not intent on obtaining personal financial rewards from their activities. Their primary objective is to subvert computer telecommunication networks for the challenge of 'beating the machine'. As Marbach (1983) observes:

> Hackers look on breaking and entering computers merely as an intellectual exercise - a challenge to their ingenuity. The hackers' mischievous intent is a far cry from criminal intent (Marbach, 1983: 46).

For the present, system hacking is still regarded by most authorities as a deviant, rather than, criminal form of

---

3 Parker (1983: 130) notes the inception of the term phone phreak: "Slang use of the word **freak** means aficionado, maven, connoisseur, enthusiast. The alternative spelling **phone phreaks** became common when it was used in the news media about the time of an October 1971 Esquire magazine article".

4 "The tone-generating devices became known as blue boxes because the first one captured was that color, and the term **black box** was already being used to denote any electronic device. Technically, they are rather simple multifrequency oscillators that produce audible toll-switching tones" (Parker, 1983: 172-173).

behavior. However, should this type of activitiy escalate to the point where it seriously impairs the proper functioning of computer networks, prosecutors may be more inclined to seek criminal convictions. Other offences contained under this indicator include schemes which are aimed at exploiting the possibilities for financial gain without violating any criminal statute. For example, the case of the California Institute of Technology students who programmed the University's computer to generate 1.2 million entry blanks in a sweepstakes contest (CRC-03), may be considered unethical, but is not criminal.

Intentional/occupational access (C)

Intentional violations committed through occupational access probably contains the largest offender population whose activities are directed toward personal financial gain. Representative of the type of offenders included under this indicator are amateur criminals, who usually embezzle funds via input manipulation. Although only limited technical skills are required for such schemes, the offender must possess extensive familiarity with the particular computerized application to be manipulated (e.g., payroll, accounts receivable etc.). Necessary in the development and implementation of computer-related crimes within the occupational setting is the utilization of specific job-related knowledge. As noted by Beeler (1983) such knowledge is generally unavailable to outside perpetrators with similar objectives:

> Corporate insiders can gain access to sensitive data much more readily and wreak far more systems havoc than a typical outside invader for one simple reason: They are privy to all the necessary passwords and intimately familiar with the workings of their employers' computing environment (Beeler, 1983: 11).

The occupational environment not only provides enhanced opportunities for criminality, but it also enables the development of more complex forms of computer-related crime. Of the four research indicators, intentional violations committed through occupational access have been the most closely associated with the "sophisticated" computer-related crime. In the majority of cases, complex programming techniques, such as the Trojan Horse and the Asynchronous Attack can only be executed within an occupational setting. The case of R. v. Thompson (CRC-35) is a good example of how the application of specific job-related knowledge facilitated by advanced technical skills can enable offenders to exploit occupational opportunities.

Unintentional/occupational access (D)

Unintentional violations committed through occupational access can be often attributed to instances of ethical ignorance. Straub and Widom (1984) use the term "professional abusers" to described individuals who unknowingly and without criminal intent abuse their positions of trust. Many of these types of

violations concern such activities as, game-playing and one-upmanship competitions which can waste a considerable amount of computer time and resources, but do not demonstrate malice against the organization (e.g., the "California Programmer" case: CRC-23). Webber (1983) comments on the innocuous nature of the violations committed by the professional abuser:

> While it may be conceded that some behaviour, within the broad range of computer abuses, is criminal in nature, it does not follow that all behaviour in that spectrum is criminal... playing computer games, programming "Mona Lisas" or typing personal letters on the employer's word processor, all without permission, are not and should not be crimes. (Webber, 1983: 245, 242).

Although Webber's comments reflect the general direction of unintentional violations, some may result in financial gain. These types of cases involve the use of organizational resources to further business interests outside of the occupational setting (e.g., the "Marine Resources" case: CRC-24). Although such violations do not result in direct financial loss to the organization through criminal activity, they do represent ethical offences which can interfere with organizational productivity. Even though legislation has been recently enacted in Canada regarding the activities of professional abusers and system hackers there still remains significant disagreement concerning the criminal nature of such violations. Webber (1983) remarks:

> The nature of the machine itself lures both professionals and students in computer science to explore its capabilities; not to mention the challenge to their technical prowess... **Unauthorized computer accessing or use should not be included in the "Mischief" section, Part IX of the Criminal Code.** Such incidents of minor interference or mere annoyances do not pass the test of criminality formulated by the Law Reform Commission of Canada. (Webber, 1983: 226, 250).

In the majority of cases, the activities of professional abusers are not motivated by personal financial gain, and similar to system hackers, denote "deviance" rather than "crime".

Thus, the basic criteria for coding and subsequent analysis is based upon the researcher's assessment of whether the violation is intentional or unintentional, and if it originated through situational or occupational access. The aggregation of cases under such a research design will enable the researcher to examine specific forms of computer-related crime, while still retaining a sense of perspective on the totality of cases.

In this respect, the introduction of statistics derived from the exploratory case study, will serve to illustrate the applicability of the research design for data analysis. It must be emphasized that the case study does not attempt to provide an indepth examination of the procedures involved when conducting a content analysis. Nor does it attempt to fully review the many methodological concerns which accompany such an analysis. It aspires only to provide the reader with an appreciation of the applicability of the research design for data collection and organization.

## B. Content Analysis

Content analysis is highly adaptable to the investigation of criminal activity for which few data exist, since it provides the researcher with the flexibility to develop original sources of information. Content analysis also enables the quantification of information into a form which may be used for empirical analysis. As Sanders and Pinhey (1983) point out:

> Content analysis is a coding process and not any kind of statistical test. In other words, content analysis is a methodology for transforming various kinds of documents, speeches, presentations, and other recorded social phenomena into a form that social scientists can analyze by means of statistical tests. The method, though, is the transformation process and not the testing process (Sanders & Pinhey, 1983: 185).

Thus, the objective of a content analysis is to arrange the "raw data" into a form which enables the application of statistical tests.[5] Throughout the process of conducting a content analysis numerous methodological checks are implemented to ensure the validity and reliability of the research procedure. For the purpose of this examination three basic procedures are employed for the content analysis: 1) selection of the units of analysis; 2) preparation of the coding

---

[5] Content analysis can be distinguished from secondary analysis, which "uses existing data to analyze some social science question not originally posed during the collection of the data, or using new techniques of analysis to reexamine a problem for which the data was originally collected" (Sanders & Pinhey, 1981: 198).

scheme; and 3) organization of the data for empirical observation.

### i. The Units of Analysis

Units of analysis can include any form of subject matter which may be coded for data collection. The 40 examples of computer-related crime cited throughout the thesis comprise the units of analysis, which when aggregated, constitute the sample population.[6] In order for the units to possess utility for empirical observation, they must be selected according to predefined criteria. As Kidder (1981: 298) notes "it is useful to distinguish among units of analysis in regard to the levels that they may imply". In this respect, the hierarchical basis for distinguishing the different levels of criminality involving the manipulation of computer technology revolve around three criminological definitions (see Chapter II). Each successive definition extends the level of analysis to include a wider range of cases, where one definition becomes a sub-set of another, until the entire population of cases is included in the sample.

For example, the definition of **computer crime** only acknowledges cases which "implies the direct involvement of computers in committing a crime" (United States Department of Justice, 1980: 3). This particular definition assumes the highest level of restriction concerning the types of cases which may be selected for analysis. The second definition, **computer-related**

---

[6] "a **population** is the aggregate of all of the cases that conform to some designated set of specifications" (Kidder, 1981: 419).

crime not only incorporates all computer crimes, but also extends the level of analysis to include cases "for which knowledge of computer technology is essential for successful prosecution" (Parker, 1980: 334-335). This definition discriminates between cases according to an indication of the technical skill and knowledge demonstrated in the commission of crime. The third definition, computer abuse incorporates "any intentional act involving a computer" (Parker, 1980: 333). This definition is the least specific in relation to the types of cases which may be selected for analysis; and is stated in terms that are intended to encompass the complete range of criminality involving the manipulation of computer technology (Parker, 1980: 333)

Thus, under this hierarchical framework the definition of computer crime is a sub-set of computer-related crime, and computer-related crime is a sub-set of computer abuse. The application of any one of these definitions will directly impact the nature of the sample population under study.

For instance, if the definition of computer crime were used as a basis for the selection of the units of analysis, the "Denver computer operator" case: CRC-02 (physical destruction); the "Equity Funding" case: CRC-08 (input manipulation) and; the "Schneider" case: CRC-16 (impersonation) would all have to be excluded from the sample. Because none of these cases directly involved the computer in the commission of the crime, they would have to be omitted from the case study, even though they demonstrate the application of technical skill and knowledge. In this respect, unless the research study is specifically directed toward the examination of "high-level" computer crimes, in which

the computer served as the instrument of crime, this definition would be to restrictive in scope for case selection.

At the other end of the spectrum, if the definition of computer abuse were used as a basis for case selection, many irrelevant cases would be included in the sample. For example, cases involving simple forms of physical destruction, such as, the "Sir George Williams University" case, and the "night shift operator" case would have to be considered for case selection. Similarly, cases involving simple theft, such as the "Rozenburg" case, the "Encyclopedia Britannica" case, and the "Stewart" case would likewise have to be included in the sample population. As noted noted in Chapter II, while these types of cases do assist in the descriptive analysis of violations which may encompass the exploitation of computer technology, they do not demonstrate a sufficient application of technical skill and knowledge to be considered for analysis. A notable exception to the exclusion of cases involving physical destruction are acts of terrorism (e.g., CRC-30, CRC-31, CRC-32) which generally require extensive technical planning (e.g., assessment of security controls, etc.).

The final definition, and the one employed in the selection of the units of analysis for this case study is computer-related crime. This definition serves to limit the selection of cases which are only superficially related to computer technology (computer abuse), while still encompassing "high-level" cases (computer crime) which demonstrate advanced technical skills and knowledge.

### ii. The Coding Scheme

The research design contains two conceptual variables, which when combined, are used to organize cases according to four research indicators. These indicators are represented by the following symbols:

A = Intentional/situational access

B = Unintentional/situational access

C = Intentional/occupational access

D = Unintentional/occupational access

All forms of computer-related crime, whether intentional or unintentional will either originate inside or outside of the occupational setting. The basic criteria for coding under this framework requires the researcher to address two fundamental questions: 1) what was the initial intention of the offender? and 2) in which environment did the violation originate?

**Expressed Intent (Indicator Designation)**

The first question attempts to ascertain the initial motivational direction percepitating the commission of the violation. In the majority of cases cited throughout this thesis, the expressed intent of the offenders becomes obvious when the objective of their violations are taken into consideration. For example, the activities of terrorists (e.g., CRC-30, CRC-31, CRC-32) clearly demonstrate intentional violations

to deprive assets by means of physical destruction. Likewise, the activities of amateur criminals (e.g., CRC-09, CRC-10, CRC-11) engaging in input manipulation schemes for financial gain are also distinctly intentional in character. For these types of cases the coding process is greatly simplified by the pronounced criminal nature of the violations. However, difficulties in case assessment may arise when the initial intention of the offender is incongruous with the end result of the violation. The Dalton School case (CRC-27) illustrates how a benign intention such as, intellectual challenge may inadvertently result in the physical destruction of assets. In actuality, these types of cases may in fact constitute criminal offences, but under the parameters of this research design are designated as unintentional. As noted earlier, such a designation is not based upon the criminal liability associated with a particular violation, but rather on the assessment of the offender(s) initial expressed intent.

Type of Access (Indicator Designation)

The second question seeks to establish from which environment the violation was initiated. The origin of the violation, rather than where the violation was concluded is the primary distinguishing characteristic when assessing this variable. Once again, the majority of cases included in the sample demonstrate a clear distinction between the two different types of access, however, some do involve environmental interactions. For example, the case of United States v. Jones (CRC-40), while entailing the enlistment of an inside source to modify the accounts

payable file, originated completely outside of the occupational setting (situational access). Similarly, cases which originate within the occupational environment may be directed toward objectives which are external to the organization. The Data General Corporation case (CRC-39) illustrates how corrupt management policies can stimulate illegal industry practices (e.g., software lock-in) which are directed toward external markets. This case is designated as occupational access since it originated within an organization environment. The assessment of each case according to the two conceptual variables will result in the selection of a single research indicator.

By designating each computer-related crime case according the above coding scheme, it will be possible to derive more information from the sample, than would have been attainable through the application of Quinney's original model.

iii. Data Collection

The method of data collection which will be used in this case study employes the data matrix as a simple form of organization. As Sanders and Pinhey (1983) explain:

> A raw data matrix contains all the data in our data set, and because it is in "raw" form, it has yet to be boiled down for presentation. Here is a way to present the relationships or associations between variables using a single summary number similar to an arithmetic mean, median, or mode. By grouping data or performing some other statistical manipulation on them, we can make them more meaningful and easy to understand (Sanders & Pinhey, 1983: 304).

As illustrated in Table 4, The 40 computer-related crime cases have been arranged within a simple raw data matrix.

Table 4

Raw Data Matrix:
Research Indicator Selection

| Case Number | Research Indicator | Page Reference |
|---|---|---|
| CRC-01 | C | P. 21 |
| CRC-02 | C | P. 22 |
| CRC-03 | B | P. 30 |
| CRC-04 | C | P. 31 |
| CRC-05 | A | P. 46 |
| CRC-06 | C | P. 49 |
| CRC-07 | C | P. 50 |
| CRC-08 | C | P. 54 |
| CRC-09 | C | P. 55 |
| CRC-10 | C | P. 56 |
| CRC-11 | C | P. 56 |
| CRC-12 | C | P. 57 |
| CRC-13 | C | P. 59 |
| CRC-14 | C | P. 59 |
| CRC-15 | C | P. 63 |
| CRC-16 | A | P. 66 |
| CRC-17 | C | P. 68 |
| CRC-18 | C | P. 76 |
| CRC-19 | C | P. 78 |
| CRC-20 | C | P. 80 |
| CRC-21 | A | P. 82 |
| CRC-22 | D | P. 93 |
| CRC-23 | D | P. 104 |
| CRC-24 | D | P. 105 |
| CRC-25 | C | P. 108 |
| CRC-26 | C | P. 109 |
| CRC-27 | B | P. 114 |
| CRC-28 | B | P. 114 |
| CRC-29 | A | P. 114 |
| CRC-30 | A | P. 115 |
| CRC-31 | A | P. 115 |
| CRC-32 | A | P. 115 |
| CRC-33 | C | P. 121 |
| CRC-34 | C | P. 130 |
| CRC-35 | C | P. 134 |
| CRC-36 | D | P. 134 |
| CRC-37 | C | P. 135 |
| CRC-38 | C | P. 137 |
| CRC-39 | C | P. 140 |
| CRC-40 | A | P. 144 |

## iv. Data Analysis

The reduction[7] of the raw data matrix is accomplished through the creation of a summary table which enables the presentation of the data for empirical observation. Table 5 depicts the reduction of Table 4 (Raw Data Matrix: Research Indicator Selection) in summary form. Each cell contains the frequency and percentage for the indicator.

**Table 5**

**Summary Table:**
**Research Indicator Analysis**

| | Intentional | Unintentional | |
|---|---|---|---|
| Situational | 8 (20.0%) | 3 ( 7.5%) | 11 (27.5%) |
| Occupational | 25 (62.5%) | 4 (10.0%) | 29 (72.5%) |
| TOTAL | 33 (82.5%) | 7 (17.5%) | 40 (100.0%) |

---

7 Data reduction concerns the development of "appppropriate methods for boiling data down to neat summaries and frequency distributions that would give readers an understandable picture of a data set at a single glance" (Sanders & Pinhey, 1983: 303).

The totals by row pertain to the evaluation of the conceptual variable, **type of access** (situational/occupational access). The totals by column pertain to the evaluation of the conceptual variable, **expressed intent** (intentional/unintentional).

## General Observations

Taking into consideration the general concentration of computer technology within the occupational environment, it is not overly surprising to find that the majority of cases in the sample, 29 (72.5%) would occur in this setting. More revealing is the extent of situational access, 11 (27.5%) which is generally achieved without the advantage of occupational knowledge. The relatively high percentage of such cases may in part, be due to, a common misconception within the business community that a secure computer facility is immune from outside subversion attempts (a perception which often presents offenders with tempting opportunities).

The nature of expressed intent also offers expected conclusions, in which the majority of cases, 33 (82.5%) were directed toward intentional violations; and only, 7 (17.5%) involved unintentional violations. While these figures may not be generalized to the entire population of computer-related crimes, they tend to confirm the belief that the majority of violations committed are intentional (criminal). However, because many unintentional violations will remain "unreported", the true nature of this variable may never be adequately measured. Future

research efforts may include triangulation[8] which can enhance the researcher's ability to collect data concerning the extent of unintentional violations.

## Cell Analysis: Research Indicators

When examining individual cells, the most prominent figure concerns the extent of intentional violations committed through occupational access which accounts for, 25 (62.5%) of the cases in the sample. This indicator represents, what other authors have termed "occupational crime". Such violations are of concern not only within computerized environments, but also to businesses which rely upon manual information processing systems.[9] In contrast to this indicator, are intentional violations committed through situational access, which also includes a relatively

---

8 Johnson (1981: 16) notes how triangulation can assist in the research effort: "For example, survey research may be supported by participant observation and case study. All three methods may be used in a comparative study, thereby giving the advantage of cross-comparisons. The use of more than one method aids in the reduction of research error, and the less error we have, the more precise our conclusions".

9 However, computerized business environments must often implement a much wider range of security controls, than would otherwise be necessarly in manual systems to prevent employee abuse. As noted by Beeler (1983: 10) "Large organizations are adopting a wide assortment of protective measures - some based on high technology - in an effort to discourage data and systems misuse by their own employees. The measures include intensified physical security, encryption, software packages to control access to central mainframes, regular shuffling of passwords, nondisclosure agreements and educational seminars aimed at increasing upper management's awareness of potential data integrity threats".

large portion of the cases in the sample, 8 (20.0%). Considering the disproportionate number of cases occurring within the occupational setting, it is understandable that corporate managers consider "outside" subversion attempts as a minor threat in relation to the intentional damage which may be inflicted by knowledgeable employees. Unfortunately, many EDP managers equate "outside" access, with system hacking, rarely considering that their organizations may be targetted for more serious types of situational violations.[10]

The small number of unintentional violations included in the sample, for both situational access, 3 (7.5%) and occupational access, 4 (10.0%) may be indicative of the hesitation of many businesses to "officially" report instances of professional abuse or system hacking. Generally, such offences are viewed as 'part of the job' or 'acceptable within limits', which tends to suppress the nature and extent of unintentional violations.

---

10 A number of authors have also erroneously compared intentional/occupational access to unintentional/situational access, which has lead to the misconception that the majority of outside offenders are comprised of inquisitive students. As Beeler (1983) notes: "Nearly forgotten in the current media hubbub over the Milwaukee episode is a data security threat that many large user organizations and industry observers consider far more serious than the inquisitive meddling of youthful 'hackers'. The threat comes from within the user organizations themselves - or rather, from their malicious or unscrupulous employees, who can cause incalculable grief by damaging, disclosing or deleting key mainframe files". The reference made by Beeler (1983) of the "Milwaukee episode" concerned a group of students calling themselves the 414s, whose system hacking activities elicited considerable media attention. The case (CRC-28) has been included in the sample and is coded unintentional/situational access (B).

## C. Variable Analysis: Technical Skill and Knowledge

The examination of computer-related crime techniques have been the central focus of numerous contradictory research studies, each endeavoring to determine the role of technical skill and knowledge in the commission of crime. An enduring theme in the related literature concerns the "sophisticated" crime, one which requires the application of advanced technical skills and knowledge. Prevailing attitudes regarding this aspect of computer-related crime have ranged from outright paranoia to ardent denial. For example, Myers and McLellan (1979) comment on the 'horrible' impact of this form of criminality:

> Like an insidious disease, most crime committed through the manipulation of computer processes or data is difficult to detect and feared too horrible or embarrassing to mention if discovered (Myers & Mclellan, 1979: 72, 74).

In contrast to this alarmist orientation, Taber (1980) skeptically questions the actuality of 'high-level' computer-related crimes:

> ... the `sophisticated' crime is precisely the one that arouses the most fear, and in academic computer science literature enjoys the most intensive interest. In other words, the least likely type of crime, of which there is no record that it ever occurred, receives a disproportionate amount of attention (Taber, 1980: 309).

Both perspectives are probably a response to the controversial statistics reported in the Stanford Research Institute (SRI) studies conducted in 1973, which tend to portray "computer crime" as an up-and-coming growth industry.

While no discussion concerning computer-related crime would be complete without an examination of technical skill and knowledge, the primary purpose for selecting this variable of analysis is to illustrate how the research design may be used to derive more information from the original case sample.

i. Coding Scheme

Similar to the two conceptual variables of analysis, technical skill and knowledge can also be designated according to major indicators. The five computer-related crime classifications described in Chapter III best illustrate the nature of this variable, and can be represented by the following symbols.

T1 = Physical acts

T2 = Transactional acts

T3 = Programming acts

T4 = Electronic acts

T5 = System hacking

The majority of computer-related crime cases contained within this sample will demonstrate the application of one of the five major crime classifications. However, problems may arise in the designation of an indicator if a case demonstrates the use of

more than one crime technique from different crime classifications.

For example, although scavenging techniques (physical acts) may provide the perpetrator with valuable information (e.g., passwords, code access numbers, etc.), the information may not in itself, be converted to gain unless another technique, such as impersonation (transactional act) is used to conclude the crime. In this respect, it is the technique which enabled the successful conclusion of the violation which is considered for coding. The "Rifkin" case (CRC-17) and the "Schneider" case (CRC-16) both illustrate how scavenging techniques may provide access to valuable information. The conversion of that information, however can only be accomplished through the application of impersonation techniques; therefore, both these cases have been coded T2 (transactional act) indicating the predominant crime classification.

A case demonstrating similar crime classification interactions is the "time-sharing" case (CRC-15) which involved the residue scavenging of proprietary data through system hacking techniques. Once again, the case was coded according to the crime classification which enabled the successful conclusion of the violation. While the objective of this case was residue scavenging (physical act), it was coded T5 (system hacking), since the data was obtained through the use of a covert acquisition technique. Each of the 40 computer-related crime cases included in the sample were coded according to the above scheme. Table 6 presents the revised raw data matrix with the selection of the technical skill and knowledge indicators.

Table 6

Raw Data Matrix:
Technical Skill and Knowledge
Indicator Selection

| Case Number | Research Indicator | Technical Skill & Knowledge Indicator | Page Reference |
|---|---|---|---|
| CRC-01 | C | T3 | p. 21 |
| CRC-02 | C | T1 | p. 22 |
| CRC-03 | B | T3 | P. 30 |
| CRC-04 | C | T1 | P. 31 |
| CRC-05 | A | T1 | P. 46 |
| CRC-06 | C | T1 | P. 49 |
| CRC-07 | C | T1 | P. 50 |
| CRC-08 | C | T1 | P. 54 |
| CRC-09 | C | T1 | P. 55 |
| CRC-10 | C | T1 | P. 56 |
| CRC-11 | C | T1 | P. 56 |
| CRC-12 | C | T1 | P. 57 |
| CRC-13 | C | T3 | P. 59 |
| CRC-14 | C | T3 | P. 59 |
| CRC-15 | C | T5 | P. 63 |
| CRC-16 | A | T2 | P. 66 |
| CRC-17 | C | T2 | P. 68 |
| CRC-18 | C | T3 | P. 76 |
| CRC-19 | C | T3 | P. 78 |
| CRC-20 | C | T3 | P. 80 |
| CRC-21 | A | T3 | P. 82 |
| CRC-22 | D | T5 | P. 93 |
| CRC-23 | D | T5 | P. 104 |
| CRC-24 | D | T5 | P. 105 |
| CRC-25 | C | T1 | P. 108 |
| CRC-26 | C | T1 | P. 109 |
| CRC-27 | B | T5 | P. 114 |
| CRC-28 | B | T5 | P. 114 |
| CRC-29 | A | T5 | P. 114 |
| CRC-30 | A | T1 | P. 115 |
| CRC-31 | A | T1 | P. 115 |
| CRC-32 | A | T1 | P. 115 |
| CRC-33 | C | T5 | P. 121 |
| CRC-34 | C | T1 | P. 130 |
| CRC-35 | C | T3 | P. 134 |
| CRC-36 | D | T1 | P. 134 |
| CRC-37 | C | T3 | P. 135 |
| CRC-38 | C | T5 | P. 137 |
| CRC-39 | C | T1 | P. 140 |
| CRC-40 | A | T1 | P. 144 |

ii. Data Analysis:

The five indicators[11] for this variable are cross-tabulated with the four research indicators, resulting in a 4 x 5 summary table (Table 7) which depicts the reduction of Table 6 (Raw Data Matrix: Technical Skill and Knowledge -

Table 7

Summary Table:
Relationship between
Technical Skill and Knowledge
and Research Indicators

| | T1 | T2 | T3 | T4 | T5 | | |
|---|---|---|---|---|---|---|---|
| A | 5<br>12.5% | 1<br>2.5% | 1<br>2.5% | 0 | 1<br>2.5% | 8 | 20.0% |
| B | 0 | 0 | 1<br>2.5% | 0 | 2<br>5.0% | 3 | 7.5% |
| C | 13<br>32.5% | 1<br>2.5% | 8<br>20.0% | 0 | 3<br>7.5% | 25 | 62.5% |
| D | 1<br>2.5% | 0 | 0 | 0 | 3<br>7.5% | 4 | 10.0% |
| TOTAL | 19<br>47.5% | 2<br>5.0% | 10<br>25.0% | 0<br>0.0% | 9<br>22.5% | 40 | 100.00% |

---

11 Each of the five major crime classifications (indicators) is comprised of numerous sub-techniques, which are summarized as follows: **T1 - Physical acts** (destructive attacks, input manipulation, scavenging); **T2 - Transactional acts** (data leakage, impersonation, piggybacking); **T3 - Programming acts** (trap doors, the trojan horse, salami techniques, the asynchronous attack); **T4 - Electronic acts** (wiretapping); and **T5 - System hacking** (trial and error techniques, covert acquisition schemes).

Indicator Selection). The totals by column pertain to the evaluation of technical skill and knowledge; while the totals by row pertain to the evaulation of the research indicators.

## General Observations

As illustrated in Table 7, the crime classification requiring the least amount of technical skill and knowledge (physical acts) was the most predominent method employed in the commission of computer-related crime encompassing 19 (47.5%) of the cases in the sample. Parker (1983: 71) notes a number of reasons why offenders are more likely to select physical acts over any other crime classification: "In choosing methods they are interested in safety, success, and leverage - satisfying their needs for the least effort". This is probably more true of violations occurring within the occupational setting, since offenders possess a greater familiarity with the computerized environment (see, Chapter IV, Section B).

In contrast to the observations of Taber (1980) programming acts were also prevalent, comprising 10 (25.0%) of the cases in the sample. This crime classification is considered by many authors to represent the only authentic form of "computer crime", since it requires the direct application of the computer in the commission of crime. Considering the controversy surrounding the extent of programming acts, it was not unexpected to discover a relatively large number of case examples in the literature. Similarly, because of the extensive media attention system

hacking has recently received, a high concentration of cases 9 (22.5%) were included under this indicator. Both programming acts and system hacking are intriguing to the public, thus authors are more inclined to seek out and report such cases. In this respect, the sample may be a reflection of 'selective reporting' which typically results when a particular type of crime captures public interest.

More surprising, is the small sample of transactional acts which only contain 2 (5.0%) of the cases. A possible explanation for the few cases of transactional acts may be that they require a greater degree of victim/offender interaction which can impact an individual's decision to engage in criminality. All three sub-techniques contained under this indicator (data leakage, impersonation, and piggybacking) necessitiate a certain level of victim management. Whereas, programming acts and even physical acts may be accomplished without victim confrontation.[12]

While electronic acts (wiretapping) have been closely associated with computer-related crime, it is interesting to note that not one case could be found in the literature. The complete absence of any cases under this indicator suggest that either

---

12 As noted by Parker (1976: 46) an aspect of the computerized environment which tends to isolate the individual from the criminal nature of the offence is the inanimate and intangible character of the object of attack, he states: "In computer abuse not only is the act done against an organization, but it is often done to the computer which is placed in the focus of attack. It is not the organization the perpetrator is attacking, but the inanimate computer system. It can't cry, have its feelings hurt, get mad, or strike out".

such crimes have not yet been detected and publicized,[13] or that they are simply to risky to warrant implementation.[14] Although the potential for electronic acts are not outside the realm of possibility, at present they do not appear to be a threat to the security of computer installations.

## Cell Analysis: Technical Skill and Knowledge

When examining the most prevalent crime classification for each research indicator an interesting association emerges between system hacking (T5) and unintentional violations (B, D), and physical acts (T1) and intentional acts (A, C). As noted in Table 7, system hacking is the favored crime classification for both unintentional/situational access 2 (5.0%) and unintentional/occupational access 3 (7.5%). While, physical acts are the preferred crime techniques for intentional/occupational access 13 (32.5%), and intentional/situational access 5 (12.5%).

---

13 Parker (1983: 78) observes that: "Few cases of criminal, voice wiretapping have been recorded. Wiretapping of data communications and computer communications circuits are apparently even more rare. The reason may be that it can be done so successfully that few cases are ever discovered". It is unlikely that this is the case, a more probable reason it that wiretapping is to cumbersome to implement, when other more conventional techniques are avaliable.

14 However, Parker (1983: 80) maintains that "tapping" is easily accomplished by anyone with a rudimentary knowledge of telecommunications, he states: "If a telephone line used for data transmission (two-wire) can be found and isolated from other wires, inductive or passive tapping is duck soup. All it takes is a small cassette tape recorder and microphone, an AM/FM portable radio, a borrowed modem (to convert telephone noise signals to digital pulses), and a Texas Instruments printer". Stated in these terms, wiretapping seems like 'child play', realistically, its a little more complex (see, Chapter III. Section D).

One of the more unusual relationships to emerge from Table 7 is the association between system hacking and occupational access. As noted, intentional/occupational access and unintentional/occupational access combined, include 6 (15.0%) of the cases in the sample. What is commonly viewed as a crime committed by "outsiders" appears to be becoming more prevalent in the occupational setting. A fact, which may be of concern to data security administrators as computer systems progress toward greater telecommunication networking.

Also noteworthy is the association between programming acts (T3) and intentional/occupational access (C). As illustrated, 8 (20.0%) of the cases in the sample involved this form of activity, which is undoubtedly a result of the enhanced environmental vulnerabilities present in the occupational setting. Physical acts involving intentional/occupational access included 13 (32.5%) of the cases in the sample, which may also reflect the increased opportunities avaliable within the occupational setting.

The case study also uncovered a number of associations which were not so obvious, and may provide intriguing areas of study for future research. For example, the association between system hacking and occupational access presents one avenue of inquiry which has not yet been addressed in the related literature.

D. Reliability

The reliability of the coding scheme is a fundamental concern to the researcher engaging in content analysis. The operational definition of the variable (e.g., the delineation of variable indicators) must be mutually exclusive and exhaustive in order to enable a clear distinction between coding classifications. The choice of how much, or how little to measure will also determine the utility of the data derived from the study. While indicators may reflect valid and accurate measures of the variable under study, the coding scheme may suffer in terms of reliability; if the researcher does not possess an adequate understanding of the specificity required in the coding process.

In designing the coding scheme, the researcher is particularly concerned with two major issues: 1) the validity of the coding classifications (do they measure what they are intended to measure?) and; 2) the reliability of the coding process[15] (can the results of the study be replicated by an independent coder using the same scheme and classifications?).

---

15 As noted by Babbie (1979: 239) "the researcher faces a fundamental choice between depth and specificity of understanding. Often, this represents a choice between validity, and reliability, respectively. Typically, field researchers opt for the former, preferring to base their judgements on a broad range of observations and information, even at the risk that another observer might reach a different judgement of the situation...' survey research - through the use of standardized questionnaires - represents the other extreme: total specificity, even though the specific measures of variables may not be fully satisfactory as valid reflections of those variables".

The strain between the validity and reliability of the coding scheme is often determined by the manner in which the variables of analysis were operationally defined.

For example, the variable technical skill and knowledge was coded according to five major crime classifications. However, an equally valid coding scheme could be based upon each of the thirteen crime techniques described in Chapter III. Both schemes may accurately reflect the nature of technical skill and knowledge, but one may prove more reliable for coding purposes. The degree to which a variable may be operationally defined for observation can greatly impact the nature of data analysis. To much specificity (especially in relation to a limited sample population) can result in weak indicator (cell) relationships which are too indistinct to provide any meaningful information. On the other hand, if there is not a sufficient degree of specificity then meaningful indicator relationships may remain unknown.

The reliability of the coding schemes employed in the case study was determined by performing an "inter-rater" reliablity check. An independent coder was provided with the original source material from which the cases were drawn, as well as, a description of the conceptual variables and their associated indicators. The coder was first instructed to assess each case according to the four research indicators (e.g., A, B, C, D), then to assess them once again in relation to the secondary variable of analysis technical skill and knowledge (e.g., T1, T2, T3, T4, T5). For this variable the coder was also provided with a

description of the different computer-related crime classifications and their associated sub-techniques. Since much of the related literature concerning the cases contained computer-related crime jargon (e.g., trojan horse, data diddling, etc.) it was necessary to familiarize the coder with the terminology which would be encountered in the review of the source documentation. On completion of the coding process, the results of the independent coder were compared to that of the case study, which are as follows.

Research Indicator: Reliability Score

The independent coder scored on 36 of 40 cases, resulting in a 90% reliability rate for the selection of the research indicators. Disagreement was primarily found between the research indicators intentional/situational access (A) and intentional/occupational access (C). The case CRC-15 was scored (A) indicating that the coder believed this case to have originated outside of the occupational environment, but nevertheless criminal (intentional) in nature. Similarily, the case CRC-40 was scored (C) rather than (A) as in the original indicator selection. Only one instance of disagreement was scored concerning the expressed intent of a violation. The case CRC-22 was scored (A) indicating that the coder felt the case to involve intentional criminal activity which occurred external to the occupational environment. Case CRC-39 (i.e., Dignidyne Corp v. Data General Corp) was scored by the coder, but disagreement

arose concerning its applicability to the case study, and was therefore excluded from the independent coder's reliability check (resulting in a non-coded item).

Secondary Variable: Reliability Score

The independent coder scored on 37 of 40 cases, which resulted in a 92.5% reliability rate in the selection of indicators for this variable. The only disagreement which was discovered concerned the indicators, physical acts (T1) and programming acts (T3). The case CRC-04 was coded (T3) indicating that the independent coder believed this case to involve programming techniques; while case CRC-37 was scored (T1) indicating a physical act. Once again case CRC-39 was excluded from the sample, resulting in a non-coded item.

The overall high scores obtained from the inter-rater reliability check may be largely attributed to the manner in which the cases were reported in the related literature. In most instances the author would not only identify the computer-related crime technique employed, but also the environment in which it occurred. This left the independent coder with little doubt as to the selection of the appropriate indicator. In some instances the only decision the coder had to make concerned the "expressed intent" of the violation; and as indicated in the reliability check only one case was scored differently.

While the inclusion of the case study within this thesis was not intended as a "definitive" quantitative analysis, it does

serve to illustrate the possibilities for future research using the proposed research design as the primary analytical tool.

## E. Recommendations for Future Research

Although this thesis has attempted to structure the related literature in a manner which provides an organized framework for analysis, the final evaluation of the quality of research is best expressed in its utility for future studies. The proposed research design can be used to address a number of different research questions, deriving meaningful data from a wide selection of variables.

The case study presented in this Chapter only illustrates how one variable (technical skill and knowledge) may be cross-tabulated with the research indicators to obtain greater information from the original case sample. However, many other areas exist for future criminological investigation, provided that the researcher can obtain the necessary data for coding. For example, the researcher wishing to study the characteristics of the "computer criminal" could select such attributes as age, education, or vocational/occupational position as background variables for indepth analysis. Too often authors rely upon commonly accepted generalizations when examining the nature of the "computer criminal", combining vastly different offender types under an all encompassing label. While a certain degree of generalization will result when attempting to categorize divergent offender populations; the indiscriminate

acceptance of uniform characteristics does little to dispel misconceptions concerning the computer-related crime offender.[16]

For the researcher interested in computer security issues, the analysis of environmental vulnerabilities offers great potential for future research. The exploitation of computerized assets is largely contingent upon how offenders can manipulate environmental vulnerabilities, through the identification of the operational stages which are most susceptible to criminal gain. The analysis of such vulnerabilities not only permits the identification of weaknesses within the computerized environment, but it also enables the development of security planning techniques to combat certain forms of computer-related crime.[17] The resultant associations may provide a good indication of major areas of vulnerability in relation to the different research indicators.

Victimization may similarly provide an interesting variable of analysis for future research; not only in relation to the application of the proposed research design for

---

16 For example, Dennis (1979: 27) notes the characteristics of the 'average embezzler' engaging in computer-related crime: "...he is male, age 35, married with one or two children, living in a respectable neighborhood, probably buying his own home, and has been employed by the firm for about three years. He has been stealing for about eight months, is in the top 40% of the nation's income distribution, and has an average total take of 120% of his salary".

17 For example, the analysis of the vulnerabilities exploited by offenders engaging in unintentional/situational access may indicate inadequate security over telecommunication services. The computer security planning response may include the implementation of such safeguards as, callback devices, encryption devices, or unique identification number generators.

empirical observation, but also to examine existing criminological theory concerning the victims of white-collar crime. In contrast to "street crimes", the majority of computer-related crimes are directed against organizations rather than individuals and often do not possess an immediate and observable impact on victims. As noted by Edelhertz (1977:1) "The more serious the harm to the victim, the more likely it is that prosecution will result". Which in respect to large organizations is much less discernible, than if an individual were victimized by a similar form of crime. Coupled with this notion of 'observable harm', public apathy also tends to cloud the issue of victimization in relation to crimes committed against organizations:

> There is an undercurrent of public indifference, if not actual resentment, toward organizations and their property. The commonly accepted ethics applying to relations between individuals simply are not extended to corporations and governments (McCaghy, 1976: 185).

Both issues provide the researcher with numerous questions which may be addressed in a more thorough analysis.

In addition to these areas of study, the researcher may also select variables of analysis which are specifically directed toward examining the nature of computer-related crime characteristics. The most prominent of which concerns, the four roles computers play in the commission of crime (see Chapter II). This variable has been described by numerous authors including, Parker (1976); Perry (1986); and Purvis

(1979); but has not yet been subjected to empirical observation. Such an analysis would assist in the determination of the quality of computer-related crimes in respect to general crime characteristics. A major point of contention concerning computer-related crime revolves around the issue of estimated loss. As described in Chapter II, numerous research studies have attempted to ascertain the extent of computer-related crime through a measure of estimated loss, often with dubious results.[18] The analysis of this variable in relation to the four research indicators would not only enable the researcher to more realistiically assess estimated losses within a specified sample population; but would also provide a measure of the difference in losses associated with occupational and situational forms of access.

Although each of the above variables may be studied without the application of the proposed research design, the value of information derived from such an analysis would only possess marginal utility for distinguishing between the different types of criminality afforded by computer technology. The delineation of research indicators in relation to specified areas of interest greatly enhances the researcher's ability to discover associations which are not obvious from a

---

18 Taber (1980: 288) points out the logic used by the SRI to calculate their widely cited statistics concerning estimated loss: "Assume an average of 100 cases per year (reported). Assume also that only 15 percent of known cases are reported. With an average loss of $450,000, a total annual loss... would be $300 million". Taber is inclined to believe that such 'assumptions' are highly questionable and are a major source of misconceptions concerning the extent of computer-related crime.

simple 'frequency count' of variable characteristics.

In relation to the application of criminological theory, numerous possibilities exist for future research. For example, "white-collar criminals" engaging in computer-related crime may be examined according to Sutherland's differential association theory. Similarly, "system hackers" may be examined according to a number of different sub-cultural theories. While it would prove difficult to subject the entire population of computer-related crime offences/offenders to an inclusive theoretical study, possibilities exist for the analysis of specific groups and areas of interest, through the use of the proposed research design.

## Bibliography


Babbie, Earl. R. (1979) The Practice of Social Research. (2nd. ed.) Belmont, California: Wadsworth Publishing Company Incorporated.

Ball, Leslie. (1982) "Computer Crime". Technology Review, April. pp. 21-30

Beardsley, Charles, W. (1973) "Is Your Computer Insecure?" in Security and Privacy in Computer Systems. Hoffman, Lance. (ed.) Los Angeles: Melville Publishing Company. pp. 45-72

Beavon, Daniel, J. K. (1984) Crime and the Environmental Opportunity Structure: The Influence of Street Networks on the Patterning of Property Offences. (Unpublished M.A. Thesis. Simon Fraser University).

Becker, Jay. (1980) "Rifkin, A Documentary History". Computer Law Journal. Vol. 2 pp. 471-622.

Beeler, Jeffry. (1983) "Hacking" Computerworld Vol. XVII. No. 37. September 12. pp. 1-15

Bennett, M. D. (1984) The Instant Expert's Guide to the Kaypro II. New York: A Dell Trade Paperback.

Bequai, August. (1978) Computer Crime. Toronto: Lexington books.

Binder, Arnold. and Geis, Gilbert. (1983) Methods of Research in Criminology and Criminal Justice. Toronto: McGraw-Hill Book Company.

Bloom, Robert. (1980) "Computer Crime". Data Management. Dec. pp. 24-26

Brandt, Allen. (1975) "Embezzler's Guide to the Computer". Harvard Business Review. July-August. pp.79-89

Brantingham, P. J. and Brantingham, P. L. (1978) "A Theoretical Model of Crime Site Selectiion". in Krohn, M. and Akers, R. L. (eds.) Crime, Law, and Sanctions. New York: Prager. pp. 105-118

Bruschweiler, Wallance. S. (1985) "Computers as Targets of Transnational Terrorism". in Grimson, J.B. and Kugler, H. J. (eds.) Computer Security. North-Holland: Elsevier Science Publishers B.V. pp.163-177

Business Electronics. (1980) "Computer Crime: The Easiest Game in Town". British Columbia Business. Oct. pp.90-98

Cambron, Jim. (1984) The First Primer of Microcomputer Telecommunications. Blue Ridge Summit, P.A.: Tab Books Incorporated.

Canada. (1976) Personal Records: Procedures, Practices and Problems. Ottawa: Department of Communications/ Department of Justice.

Canada, House of Commons. (1983) Subcommittee on Computer Crime. Ottawa: Standing Committee on Justice and Legal Affairs. Issues 1-18

Carroll, John. (1969) The Third Listener. New York: E.P. Dutton and Company.

Carroll, John. (1977) Computer Security. Los Angeles: Security World Publishing Company.

Carroll, J.M. and McLellen, P.M. (1973) "Fast 'Infinite-Key' Privacy Transformations for Resource-Sharing Systems". Security and Privacy in Computer Systems. Hoffman, Lance. (ed.) Los Angeles: Melville Publishing Company. pp. 139-177

Chalmers, Leslie. S. and Edwards, Robert, W. (1985) "Personnel Security". Data Security Management. Vol 3. Issue 5. Auerbach Publishers Inc. pp.1-9

Cheney, Peter. (1984) "Hackers Crack Computer Codes to get Confidential Data". The Toronto Star. Dec 12 pp. 1, 7

Clinard, Marshall, B. (1983) Corporate Ethics and Crime: The role of Middle Management. London: Sage Publications.

Comer, Michael. (1977) Corporate Fraud. London: McGraw-Hill.

Cooper, Harris. M. (1984) The Interactive Research Review. London. Sage Publications.

Cooper, James. (1984) Computer Security Technology. Massachusetts: Lexington Books.

Davis, Gordon. (1965) Introduction to Electronic Computers. New York: McGraw-Hill Book Company.

Dennis, F. W. (1979) "Step 4: The Computer Criminal". Security World. September. pp. 26-27, 48.

Dentay, Ted. (1980) "The Crime of the Century it's only a Matter of Time". Computer Data. September. pp. 44-48

Edelhertz, Herbert. (1977) The Investigation of White-Collar Crime: A Manual for Law Enforcement Agencies. Washington: Law Enforcement Assistance Administration. U.S. Department of Justice.

Enright, Tom. (1983) "What is an RBBS?" Pro-Files. Nov-Dec. pp. 52-54, 59-63

Erikson, Kai. T. (1978) "Notes on the Sociology of Deviance". Deviance: The Interactionist Perspective. Rubington, Earl. and Weinberg, Martin. (ed.) New York: MacMillan Publishing Company. pp. 25-29

Ermann, David, M. and Lundmann, Richard, J. (1982) Corporate Deviance. New York: Holt, Rinehart and Winston.

Finlay, John, L. (1985) "Theft and Fraud by Use of a Computer: Problems with Territoriality". Canadian Computer Law Reporter. Vol 2. Issue 6. April. pp.116-120

Galland, Frank, J. (1982) Dictionary of Computing. New York: John Wiley & Sons.

Gillard, Colin. and Smith, Jim. (1983) "Computer Crime: A Growing Threat". Byte. Oct. pp. 398-424

Glaseman, S. and Turn, R. and Gaines, S. (1977) "Problem Areas in Computer Security Assessment". Computers and Security: Volume III. (ed.) Dinardo, C. T. AFIPS Press: Montvale, N.J. pp. 219-226

Goff, Colin, H. and Reasons, Charles, E. (1976) "Corporate Crime and Punishment". The Criminal Law Quarterly. Vol. 18 No. 4. pp. 468-498

Guncheon, Kelly. (1982) "Tracking Computer Fraud". Hospitals. Oct. pp. 104-112

Hall, Jerome. (1960) General Principles of Criminal Law. (2nd. ed). Indianapolis: Bobbs-Merrill.

Herschberg, I. S. and Paans, R. (1984) "The Programmer's Threat: Cases and Causes". in Finch, J. H. and Dougall, E. G. (eds.) Computer Security: A Global Challenge. North Holland: Elsevier Science Publishers B. V. pp.77-89

Hirschi, Travis. and Selvin, Hanan. (1973) Principles of Survey Analysis. New York: The Free Press.

Hoffman, Lance. (1977) Modern Methods for Computer Security. Englewood Cliffs, New Jersey: Prentice-Hall Incorprated.

Horoszowski, Pawel. (1981) Economic Special-Opportunity, Conduct and Crime. Toronto: Lexington Books.

Hsiao, David. and Kerr, Douglas. and Madnick, Stuart. (1979) Computer Security. New York: Academic Press.

Ingraham, Donald. (1980) "On Charging Computer Crime". Computer Law Journal. Vol 2. pp. 429-439.

Johnson, Edwin, S. (1981) Research Methods in Criminology and Criminal Justice. Englewood Cliffs, New Jersey: Prentice-Hall Incorporated.

Kahn, David. (1967) The Code-Breakers. New York: The MacMillan Company.

Kelly, Rob. (1984) The World of Computers Toronto: John Wiley & Sons.

Kidder, Louise. H. (1976) Research Methods in Social Relations. New York: Holt, Rinehart and Winston.

Kidder, Louise. H. (1981) Research Methods in Social Relations. (4th. ed) New York: Holt, Rinehart and Winston.

Krauss, Leonard. and MacGahan, Aileen. (1979) Computer Fraud and Countermeasures. Englewood Cliffs, New Jersey: Prentice-Hall Incorporated.

Lamb, John. and Etheridge, James. (1986) "DP: The Terror Target". Datamation. Vol. 32. No. 3. February 1. pp. 44-46

Leibholz, Stephen. W. and Wilson, Louis. d. (1974) User's Guide to Computer Crime: Its Commission, Detection and Prevention. Randor, Pennsylvania: Chilton Book Company.

Leonard, William, N. and Weber, Marvin, G. (1970) "Automakers and Dealers: A Study of Criminogenic Market Forces". The Law and Society Review. Vol. 4. No. 3. February. pp 407-424

Letkmann, Peter. (1973) Crime as Work. Englewood Cliffs, New Jersey: Prentice-Hall Incorporated.

Lewis, Gordon. (1983) "An Introduction to Telecomputing". Pro-Files. Nov-Dec. pp. 46-51

MacIntosh, Robert. (1983) "Myths, Sensation and Computer Crime". Canadian Banker. September. pp.6-8

Marbach, W. D. and Resener, M. (1983) "Beware: Hackers at Play". Newsweek. Sept. pp. 42-48

Maynard, Jeff. (1975) Dictionary of Data Processing. London: Newnes-Butterworths.

McCaghy, Charles, M. (1976) Deviant Behavior: Crime, Conflict, and Interest Groups. New York: MacMillian Publishing Company Incorporated.

McLellan, Vin. (1979) "Many Ways to Cheat". Duns Review. 114. August. pp. 98-99.

McNiff, Francine. (1982) Criminal Liability for Australian Computer Abuse. Frankson, Australia: Chisholm Institute of Technology/ Computer Abuse Research Bureau.

Miller, Arthur. (1971) The Assault on Privacy: Computers, Data Banks, and Dossiers. Ann Arbor: The University of Michigan Press.

Murphy, Emily, F. (1922) The Black Candle. Toronto. Thomas Allen.

Myers, Edith. and McLellan, Vin. (1979) "The-Head-in-the-Sand-Caper". Datamation. Sept. 70-82

Nettler, Gwynn. (1978) Explaining Crime. Toronto: McGraw-Hill Books.

Newman, Donald, J. (1958) "White-Collar Crime: An Overview and Analysis". Law and Contemporary Problems. Vol. 23. Autumn.

Parker, Donn. (1976) Crime by Computer. New York: Charles Scribner's & Sons.

Parker, D. B. (1976b) "Computer Abuse Perpetrators and Vulnerabilities of computer systems". Computers and Security: Volume III. (ed.) Dinardo, C.T. AFIPS Press: Montvale, N.J. pp. 13-22

Parker, Donn. (1980) "Computer Abuse Research Update". Computer Law Journal. Los Angeles. Vol. 2. pp. 329-352

Parker, Donn. (1983) Fighting Computer Crime. New York: Scribner's & Sons.

Parker, Graham. (1977) An Introduction to Criminal Law. Toronto: Methuen.

Penrose, R. (1979) "Commercial Crime and the Computer". The Chartered Accountant in Australia. April. pp. 13-14

Perry, William. E. (1986) A Standard for Auditing Computer Applications. Pennsauken, New Jersey: Auerbach Publishers Inc.

Petersen, H. E. and Turn, R. (1973) "System Implications of Information Privacy". in Hoffman, Lance. (ed.) Security and Privacy in Computer Systems. Los Angeles: Melville Publishing Company. pp. 76-95

Purvis, R. N. (1979) "A Criminological Point of View". The Chartered Accountant in Australia. April. pp. 18-22.

Quinney, Richard. (1964) "The Study of White-Collar Crime: Toward a Reorientation in Theory and Research". in Geis, G and Meier, R. (1977) White-Collar Crime. (Rev. Ed.). New York: Free Press. pp. 283-295

Reid, Tim. and Reid, Julyan. (1969) Student Power and the Canadian Campus. Toronto: Peter Martin Associates Limited.

Rengert, G. F. (1981) "A Crtique of an Opportunity Structure Model". in Brantingham, P. J. and Brantingham, P. L. (eds.) Environmental Criminology. Beverly Hills: Sage Publications. pp. 189-210

Rhodes, Wayne. (1979) "Computer Crime is no Crime at All". Infosystems. August. pp. 50-52

Sanders, Steven. (1983) "Starting a Remote System". Pro-Files. Nov-Dec. pp.66-67

Sanders, William, B. and Pinhey, Thomas, K. (1983) The Conduct of Social Research. Toronto: Holt, Rienehart and Winston.

Sandza, Richard. (1984) "The Night of the Hackers". Newsweek. November 12. pp. 79-82

Silverman, Robert, E. (1971) Psychology. New York: Appleton, Century, Crofts.

Sippl, Charles. and Kidd, David. (1975) Microcomputer Dictionary and Guide. Champaign, Il.: Matrix Publishers Incorporated.

Sippl, Charles, J. (1976) Data Communications Dictionary. New York: Van Nostrand Reinhold Company.

Smeltzer, Gerald. G. (1986) "Copyright and Market Power: The Data General Case". Canadian Computer Law Reporter Vol 3. Issue. 6. April. pp. 101-104

Smith, R. C. (1974) "Equity Funding: Implications for Auditing and Data Processing". Edpacs. Vol. 2 Oct. pp. 1-7.

Sobel, R. and Dallos, R. (1975) The Impossible Dream, The Equity Funding Story: The Fraud of the Century. New York: Putnam.

Sokolik, Stanley. (1980) "Computer Crime, The Need for Deterrent Legislation". Computer Law Journal. Vol. 2 pp. 353-383

Solarz, Arthur. (1981) Computer Technology and Computer Crime: Aetiological and Phenomenological Aspects. Stockholm, Sweden: Research and Development Division.

Spencer, Donald. (1968) The Computer Programmer's Dictionary and Handbook. Toronto: Blaisdell Publishing Company.

Spencer, Donald, D. (1979) Computer Dictionary. Ormond Beach, Florida: Camelot Publishing Company.

Stabley, Don, H. (1982) Assembler Language for Application Programming. New York: Petrocelli Book Company.

Straub, Detmar, W. Jr. and Widom, Spatz, Cathy. (1984) "Deviancy by Bits and Bytes: Computer Abusers and Control Measures". Finch, J. H. and Dougall, E. G. (eds.) Computer Security: A Global Challenge. North Holland: Elsevier Science Publishers B. V. pp. 91-101

Sutherland, Edwin. (1937) The Professional Thief. Chicago: University of Chicago Press.

Sutherland, Edwin. (1940) "White-Collar Criminality". American Sociological Review. Vol. 5. Februrary. pp. 1-12

Sutherland, Edwin. (1950) "The Diffusion of Sexual Psychopath Laws". American Journal of Sociology. Vol 56. September. pp. 142-148.

Sutherland, Edwin, H. and Cressey, Donald, R. (1978) Criminology. (10th. ed.). Philadelphia: J. B. Lippincott Company.

Swanson, C. R. and Territo, Leonard. (1980) "Computer Crime: Dimensions, Types, Causes, and Investigation". Journal of Police Science and Administration. Vol. 8. No. 3. pp. 304-311

Taber, John. (1980) "A Survey of Computer Crime Studies". Computer Law Journal. Los Angeles: Vol 2. pp.275-327

Tassel, Dennis. (1972) Computer Security Management. Englewood Cliffs, New Jersey: Prentice-Hall Incorporated.

Thackeray, Gail. (1984) "Legislative Trends in Computer-Related Crime". Data Security Management Vol 4. Issue 11. Auerbach Publishers Inc. pp. 1-15

The Ombudsman Committee on Privacy. (1976) Privacy, Security, and the Information Processing Industry. New York: The Association of Computing Machinery.

Turn, Rein. and Shapiro, Norman, Z. (1973) "Privacy and Security in Databank Systems: Measures of Effectiveness, Costs, and Protector-Intruder Interactions". Hoffman, Lance (ed.) Security and Privacy in Computer Systems. Los Angeles, California: Melville Publishing Company. pp. 270-285

United States Department of Justice. (1979) Computer Crime: Criminal Justice Resource Manual. Washington: Law Enforcement Assistance Administration.

United States Department of Justice (1979b) Illegal Corporate Behavior. Washington: Law Enforcement - Assistance Administration. National Institute of Law Enforcement and Criminal Justice.

United States Department of Justice. (1980) Computer Crime: Expert Witness Manual. Washington: Law Enforcement Assistance Administration.

Van Tassel. D. (1970) "Computer Crime". Computers and Security: Volume III. (ed.) Dinardo, C. T. AFIPS Press: Montvale, N.J. pp. 7-12

Walker, Bruce. and Blake, Ian. (1977) Computer Security and Protection Structures. Pennsylvania: Dowden, Hutchinson and Ross Incorporated.

Webber, Christopher. (1983) "Computer Crime or Jay-Walking on the Electronic Highway". Criminal Law Quarterly. pp. 217-250

Weik, Martin. (1970) Standard Dictionary of Computers and Information Processing. New York: Hayden Book Company Incorporated.

Weik, Martn, H. (1977) Standard Dictionary of Computers and Information Processing. (2nd. ed.) Rochelle Park, New Jersey: Hayden Book Company.

Whiteside, T. (1978) Computer Capers: Tales of Electronic Thievery, Embezzlement, and Fraud. New York: Thomas Y. Crowell.

Woofe, Emile. (1977) "Lesson of Equity Funding - The Ultimate Indictment". Accountant. Vol. 88. Jan. pp. 30-33, 36, 38-40.

## Cases Cited

Digidyne Corp. V. Data General Corp. 734 F. 2d. 1336 [1984]

R. v. Marine Resource Analysts Limited. 41 N.R.S. (2d.) [1979]

R. v. Stewart. 5 C.C.C. (3rd.) 484. [1983]

R. v. Thompson. 3 All. E.R. 565 (C.A.) [1984]

United States v. Jones. 553 F.2d. (4th Cir.) 353. [1977]