December 1975

# COMPUTER ABUSE PERPETRATORS AND VULNERABILITIES OF COMPUTER SYSTEMS

By: Donn B. Parker

Prepared for:

National Science Foundation
Washington, D.C. 20550

Grant No. MCS76-09183

SRI Project 5068



Approved by:

D. R. Brown, Director
Information Science Laboratory

E. D. Jones, Associate Executive Director
Information Science and Engineering Division

Abstract

Analysis of computer abuse experience is valuable in threat and risk studies performed to develop appropriate safeguards in computer use. A profile of computer abuse perpetrators has been developed on the basis of interviews with 17 offenders involved in a total of 15 cases. Common characteristics, occupations, and modus operandi are documented and analyzed. Computer systems' and user organizations' vulnerabilities that facilitated perpetrators' actions are also described, based on study of 375 reported cases of abuse. Eight main vulnerable functions and nine main vulnerable functional locations are identified and ranked by incidence of occurrence. Each vulnerability is described by examples in the form of brief case descriptions. Finally, priorities for safeguards are deduced from the results of the study.

## Introduction

Computer abuse research has been conducted over the past five years at Stanford Research Institute, supported in part by the National Science Foundation (Grants-37226 and GJ-44313). Computer abuse is defined as any 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 assessment of computer abuse and development of a case file--which now contains information on about 375 cases--are now sufficiently advanced to allow analyses that can assist security planners and EDP management. Two basic areas of concern are the sources of threats--the computer abuse perpetrators--and the vulnerabilities that facilitated their acts. With the rubric, "know the enemy to overcome him" in mind, a profile of known perpetrators was developed and documented. The admonition to be aware of the vulnerabilities of victims is the motivation for also identifying and presenting the weaknesses and functional locations of weaknesses among the known, reported cases of computer abuse.

## Computer Abuse Perpetrators

An important aim of computer abuse research is determining a typology of known perpetrators as an aid in developing safeguards. Such a typology

can be used in reducing the number of possible perpetrators and their potential for doing harm.

Interviews of varying lengths were conducted with seventeen perpetrators. In some cases over 20 hours of interviews were held, involving numerous sessions covering pretrial, criminal trial, presentencing, incarceration, and post incarceration periods. In six cases only brief telephone conversations were held with perpetrators, but information from them was heavily supplemented with facts and opinions of other case participants. No attempt was made to carry out psychological profiling, but obvious characteristics were determined in a gross fashion by interviewers with expertise in computer technology, management, and law. The sample of perpetrators was chosen on the basis of geographic and interview schedule expediency, case notoriety, and technical novelty or frequency of the abuse method. In the future attempts will be made to choose perpetrators so that the growing sample will be more representative of the total file of cases.

Characteristics were collected and synthesized by interviewing perpetrators, and conclusions were based on computer technology management experience of the interviewers. Characteristics of white collar criminals were identified from criminology literature (Cressey, 1971; Smigel, 1970; Geis, 1968). Theories and information from this source include the trust position vulnerability, Robin Hood, and differential association theories; known characteristics of people in EDP occupations such as their ages, skills, occupation-related actions, technical challenge and game playing interests; and characteristics discovered in interviews, such as tendencies to collusion and business and occupational aggressiveness. The characteristics

identified are those that a manager of a computer system might recognize among people within the computer environment operating or affected by computer services.

There are ten characteristics of the typology and supporting data based on the sample of 17 perpetrators.

(1) Age--Perpetrators are young. Mean age is 29 years, median age is 25 years, and the range is 18 to 46 years.

(2) Skill Level--Skill level pertaining to the abuse is high, with professional and managerial skills predominant:

| Skill Level/Occupation | Number of Perpetrators |
|---|---|
| Low experience technician | 1 |
| Technician | 3 |
| Low experience professional | 1 |
| High experience professional | 5 |
| Manager | 7 |

(3) Relation Between Occupation and Abuse--In all cases except one, perpetrators performed their acts while engaged in their occupations. The exception is an individual who, while president of an electronic supply house, posed as a telephone company employee to order the delivery of telephone equipment. Eleven of the perpetrators violated their occupational positions of trust. Six performed their acts without violating occupational trust.

The perpetrators' occupations, associated with types and characteristics of the victims appear in Table 1.

TABLE 1

COMPUTER ABUSE PERPETRATORS' OCCUPATIONS AND TYPES OF VICTIMS

| Perpetrator Occupations | Victims | Number of Perpetrators |
|---|---|---|
| Retail consumer | large insurance company | 1 |
| Teller | large bank | 1 |
| Accountant and computer service company owner | small manufacturing company (one accountant) | 1 |
| Time-sharing user | large service, small service, large private system | 3 |
| Business programmer | small banks | 2 |
| Systems programmer | state agency | 1 |
| Data input supervisor | large insurance company | 1 |
| Computer operations and and systems managers | small bank, large insurance companies | 3 |
| Firm presidents | small electronic supply and software house | 2 |
| Business manager | large manufacturer | 1 |
| Sales manager | large time-sharing service | 1 |

A significant range of types of perpetrators and victims is included with consumers, non-EDP employees, EDP employees, managers and staff, and large and small victims in various industries.

(4) Abuse Modi Operandi--The modi operandi were almost equally divided between unauthorized data manipulation during authorized computer use and unauthorized computer use. In eleven cases computers were primarily objects of acts; in five of the cases they provided the environment for the act; and in one case a computer was the instrument of the act. Eight cases involved batch-operated computer systems, five involved time-sharing systems, and four involved transaction systems.

Table 2 presents a range of perpetrators' technical acts.

Types of losses were: information or property fraud or theft in five cases, financial fraud or theft in ten cases, and unauthorized use of services in two cases. In the last two cases, perpetrators were able to use time-sharing services without paying for them and also took proprietary data, but no loss was sustained by victims of the data theft.

(5) Collusion--Collusion occurred in seven cases. Four of the cases involved only two people; the others involved five, seven and twenty-two people. Collusion was found necessary by the perpetrators either because they did not possess all of the skills, time, or resources necessary for the act, or they needed assistance in converting the act to financial gain. Several of the other perpetrators said they considered obtaining assistance from others but rejected the idea because they felt they should not entice others into wrongdoing.

TABLE 2

PERPETRATORS' TECHNICAL METHODS OF COMPUTER ABUSE

| Number of Cases | Methods |
|---|---|
| 2 | Manipulation of data by unauthorized computer program changes. |
| 1 | Unauthorized use of an existing program to manipulate data. |
| 3 | Compromise or penetration of a time-sharing computer system by legitimate access from an on-line terminal performed by discovering and exploiting a weakness or error in the system controls that protect users or the system. |
| 2 | Impersonating an authorized terminal user of a time-sharing computer service by using confidential identification codes to obtain and use proprietary programs and data. |
| 1 | Use of a computer as an instrument or tool to plan or control a noncomputer related act. |
| 2 | Taking by manual means and/or selling copies of proprietary computer programs without the owner's permission or knowledge. |
| 4 | Inputing incorrect data and/or using incorrect output by authorized and correct means but for unauthorized purposes. |

(6) Personal Gain--For a group of eight of the cases, a total financial gain of $4 million was discovered, with an average gain of $500,000 per case. The range for the 15 cases is $1400 to $1.5 million. Another type of gain was business or employment advantage over competitors through sabotage or espionage (intelligence gathering).

(7) Differential Association--Thirteen perpetrators demonstrated the differential association syndrome: The white collar criminal in his act deviates from accepted practices of his associates only in small ways.

(8) Robin Hood Syndrome--Twelve perpetrators exhibited the Robin Hood syndrome: They differentiate strongly between harming people, which is highly immoral within their standards, and harming organizations, which they can easily rationalize.

(9) Game Playing--Fifteen perpetrators indicated that they considered their acts games pitting their skills against the computer and the victim organization. The games represented challenges to them, and made their lives exciting and filled with danger. Fourteen perpetrators accepted the challenge with considerable aggressive behavior, identified by one perpetrator as the desire to participate in physically dangerous activities such as entering a bull ring or driving a race car.

(10) Dispositions--The dispositions of perpetrators as of this writing follows:

| Disposition | Number of Perpetrators |
|---|---|
| Felony conviction | 9 |
| Felony charged | 1 |
| Lawsuit judgment | 1 |
| Charges dropped | 1 |
| No sanctions proposed | 4 |
| Hired by victim | 1 |

Only one perpetrator, a nineteen-year-old programmer, had a prior conviction--for a misdemeanor of marijuana possession.

(11) Personal Characteristics--Generally the perpetrators were accepted as reliable, honest, bright, highly motivated in their work and most desirable people for a manager to hire. They do not appear special as a class and could not be classed as professional criminals who take pride in their wrongdoing. The greatest fear they reported occurring during their acts was unanticipated detection and exposure of their acts to their families, friends, and coworkers. This was feared more than incarceration. In fact, after sentencing, several said imprisonment was the best solution to the original problem that drove them to their acts. After they were caught, their greatest concern was to minimize the criminality aspects of their cases.

This initial study of perpetrators is enough to suggest the value of a thorough sociological and psychological study as a basis for identifying populations of potential perpetrators in automated crime.

## Computer System Vulnerabilities that Facilitate Abuse

Vulnerabilities to computer abuse must be understood for effective threat and risk analysis and computer security (Martin, 1974; Patrick, 1975). Many vulnerabilities seem obvious, but the security planner can never be sure he has thought of them all or even the important ones. Two analyses, based on the principal vulnerability found or surmised in each of the 375 recorded cases of computer abuse were made to assist in this activity. The first was based on a breakdown of common functional weaknesses, such as inadequate input/output controls; the second was based on a breakdown of the most common functional and physical locations of vulnerabilities. Tables 3(a) and 3(b) summarize these vulnerabilities and locations.

## Functional Vulnerabilities

Eight primary functional vulnerabilities emerged from the analysis. They are listed below in order of frequency of occurrence. Each vulnerability is general enough to maintain an acceptable level of confidence in assignment of cases to types of vulnerabilities. This approach was adopted because the amount of information about some cases is limited. Examples from the file that demonstrate the range of acts facilitated by each vulnerability appear in the appendix.

(1) Poor Controls Over Manual Handling of Input/Output Data

This vulnerability was associated with 147 cases. The greatest vulnerability occurs wherever assets are most exposed. Over the past 17 years--the period of reported cases-- assets have been most tangible and subject to human acts before entry into computers and after output from computers. Data assets are more

accessible outside computers than when they are within them, and programs must be executed to achieve unauthorized access. Controls that are often absent or weak include separation of data handling and conversion tasks, dual control of tasks, document counts, batch total checking, audit trails, protective storage, access restrictions, and labeling.

(2) Weak or Nonexistent Physical Access Controls--This vulnerability to access to computing facilities accounted for 46 cases. Where physical access is the primary vulnerability, nonemployees have gained access to computer facilities, and employees have gained access at unauthorized times and in areas in which they were unauthorized. Perpetrators' motivations have included political, competitive, and financial gain. Financial gain occurred mostly through unauthorized selling of computer services, holding computer centers for extortion purposes, burglary, and larceny. In a number of cases employee disgruntlement has been the motivating factor. In some of these cases disgruntlement stemmed from frustration with various aspects of automated society. Controls that were found to be weak or nonexistent include door access, intrusion alarms, low visibility of assets, identification and establishment of secure perimeters, badge systems, guard and automated monitoring functions (closed circuit television), inspection of transported equipment and supplies, and staff sensitivity to intrusion. A number of the intrusions occurred during nonworking hours when safeguards and staff who might notice intrusions were not present.

Four cases from the case file in which abuse was facilitated by physical access vulnerability involved attacks on computers with firearms; one involved a dispute over national politics; another case was perpetrated by a computer operator frustrated with his job, and the remaining two are presumed to have involved citizens frustrated in dealing with government bureaucracy and computer-based services.

(3) Computer and Terminal Operations Procedures--This vulnerability accounted for 43 cases. Losses resulting from operational procedures weaknesses have resulted from sabotage, espionage, sale of services and data extracted from computer systems, unauthorized use of facilities for personal advantage, and direct financial gain associated with negotiable instruments in operational EDP areas. The controls whose weakness or absence facilitates these kinds of acts include separation of operational staff tasks, dual control over sensitive functions, staff accountability, accounting of resources and services, threat monitoring, close supervision of operating staff, sensitivity briefings of staff, documentation of operational procedures, backup capabilities and resources, and recovery and contingency plans. The most common abuse problem has been the unauthorized use or sale of services and data. The next most common problem is sabotage perpetrated by disgruntled EDP operations staff.

(4) Weaknesses in Business Ethics--Abuse facilitated by this vulnerability accounted for 41 cases. A weakness or breakdown in business ethics can result in computer abuse perpetrated in the name of a

TABLE 3

VULNERABILITIES TO COMPUTER ABUSE

(Incidence in Reported Cases)

(a) Vulnerable Functions

| Function | Number of Cases | Percent of Cases |
|---|---|---|
| Manual handling of input/output data | 147 | 41% |
| Physical access to EDP facilities | 46 | 13 |
| Operations procedures | 43 | 12 |
| Business practices | 41 | 11 |
| Computer programs usage | 33 | 9 |
| Operating systems access and integrity | 24 | 6 |
| Time-sharing service usage | 19 | 5 |
| Magnetic tape storage | 9 | 3 |
| Totals | 362* | 100% |

(b) Vulnerable Locations

| Functional Locations | Number of Cases | Percent of Cases | Total Number of Cases | Total Percent of Cases |
|---|---|---|---|---|
| Data and report preparation | 120 | 33% | | |
| Terminal areas | 14 | 4 | 134 | 37% |
| Computer operations | 95 | 26 | | |
| Terminal areas | 10 | 3 | 105 | 29 |
| Non-EDP | 44 | 13 | 44 | 13 |
| Computer systems | 7 | 2 | | |
| Terminal systems | 33 | 9 | 40 | 11 |
| Programming | 27 | 7 | 27 | 7 |
| Magnetic tape storage | 12 | 3 | 12 | 3 |
| | | | 362* | 100% |

*13 of 375 cases were not amenable to analysis

business or government organization. The principle act is more related to a company's practices or management decisions rather than to identifiable unauthorized acts of individuals using computers. These practices and decisions result in deception, intimidation, unauthorized use of services or products, financial fraud, espionage, and sabotage in competitive situations. Controls include review of business practices by company boards of directors or other top level management, certified public accountant audits, and effective practices of regulatory and law enforcement agencies.

(5) Weaknesses in the Control of Computer Programs--This vulnerability facilitated 33 cases. Programs are assets subject to abuse. They can also be used as tools in the perpetration of abuse, and are subject to unauthorized changes to perpetrate abusive acts. The latter abuses are the most common. Controls found lacking include labeling programs to identify ownership, formal development methods (including testing and quality assurance), separation of programming responsibilities in large program developments, dual control over sensitive parts of programs, accountability of programmers for the programs they produce, the safe storage of programs and documentation, audit comparisons of operational programs with master copies, formal update and maintenance procedures, and establishment of ethical concepts of program ownership.

(6) Operating System Access and Integrity Weaknesses--This vulnerability facilitated 24 cases. All of these compromises of computer operating systems that are recorded involve the use of time-sharing services.

Compromises are accomplished through discoveries of weaknesses in design or taking advantage of bugs or shortcuts introduced by programmers in the implementation of operating systems. The acts involve intentional searches for weaknesses in operating systems, or the unauthorized exploitation of weaknesses discovered accidentally. Most of the acts have been perpetrated in university-run time-sharing services by students committing vandalism or malicious mischief, or attempting to obtain computer time without charge. Controls that would eliminate weaknesses in operating systems include methods for proving the integrity and security of the design of operating systems, imposing sufficient implementation methods and discipline, proving the integrity of implemented systems relative to complete and consistent specifications, and adopting rigorous maintenance procedures.

(7) Poor Controls Over Access Through Impersonation to Time-Sharing Services--This vulnerability facilitated 19 cases. Unauthorized access through impersonation to time-sharing services can most easily be gained by obtaining secret passwords which are keys for the most common method of protecting users of time-sharing services. Perpetrators learn passwords that are exposed accidentally through carelessness or administrative failures, or obtain them by conning people into revealing their passwords or by guessing obvious combinations of characters and digits. It is suspected that this type of abuse is so common that few victims bother to report cases in recordable form. Control failures include poor administration of

passwords, failure to change passwords periodically, failure of users to protect their passwords, poor choices of passwords, absence of threat monitoring or password-use analysis in time-sharing systems, and failure to suppress or obliterate the printing of passwords.

(8) Weaknesses in Magnetic Tape Control--This vulnerability accounts for nine cases. Theft of magnetic tapes, their destruction, and data erasure from them are acts attributed to weaknesses in control of magnetic tapes. Many other cases, identified as operational procedure problems, involved the manipulation of data on tapes and copying. (No cases are known in which magnetic disk packs have been subject to abusive acts.) Controls found lacking include limited access to tape libraries, safe storage of magnetic tapes, the labeling of tape reels, location and reel number accounting, control of degausser equipment, and backup capabilities.

Functional Locations of Vulnerabilities

The functional locations of vulnerabilities were analyzed for the 375 cases. Data and report preparation areas and computer operation facilities--the physical locations with the highest concentration of manual functions--were the most vulnerable locations.

Nine primary functional locations of vulnerabilities emerged from the analysis.

(1) Data and Report Preparation Facilities--These were the locations of 120 cases. Areas included key-to-tape/disk/card data conversion, computer job setup, output control and distribution, data collection, and data transportation. Input and output areas associated with on-line,

remote terminals are not included here.

(2) Computer Operations--These were the locations of 95 cases. All functional locations concerned with operating computers in the immediate area or rooms housing central computer systems are included in this category. Detached areas containing peripheral equipment cable-connected to computers and computer hardware maintenance areas or offices are also included. On-line remote terminals (connected by telephone circuits to computers) are not included here.

(3) Areas Without EDP Functions--Forty-four cases occurred in non-EDP locations. Many cases involved business decisions in which the primary abusive act occurred in non-EDP areas such as management, marketing, sales, and business offices.

(4) On-Line Terminal Systems--These were the locations of 33 cases. The vulnerable functional areas are within on-line computer software operating systems where acts occur by execution of programmed instructions such as are generated by terminal commands.

(5) Programming Offices--These were the locations of 27 cases. This includes office areas where programmers produce and store program listings and documentation.

(6) Data Preparation and Output Report Handling Areas for On-Line Terminals--Fourteen cases occurred in these locations. This category includes the same functions identified in (1), data preparation but is associated with on-line terminals rather than computers.

(7) Magnetic Tape Storage Facilities--These were the locations of 12 cases. Areas included in the category are tape libraries and any

storage place for tapes containing usable data. This does not include temporary or short-term storage of tapes in tape-drive mounting areas. The latter are included in categories (2), computer operations, and (1), data preparation.

(8) On-line Terminal Operations Areas--These were the locations of ten cases. This category is the equivalent of (2), computer operations, but is in on-line terminal areas.

(9) Central Processors--These were the locations of seven cases. These functional areas are within computer systems where acts occur in the computer software operating system (not induced from terminals).

Safeguards Against Computer Abuse

A computer-dependent organization intent on optimizing resource expenditure for computer security can profitably use the results of this study against known and reported types of computer abuse. In general, priorities for safeguards should be established in the following order:

(1) The most important priority, by far, is safeguarding input/output data from disclosure (taking), modification, and denial of use during manual handling in data preparation and conversion and in report Preparation and distribution.

(2) Secondly, access to sensitive EDP areas should be strictly limited. Particular attention should be given to access by non-EDP employees and nonoperational employees (such as programmers) into any operational areas and to the access of operational employees and vendors' employees into operational areas not directly connected with their work. The dangers are primarily vandalism and sabotage.

(3) Computer and on-line terminal operational safeguards are almost as important as access control. The dangers also derive principally

from vandalism and sabotage by disgruntled employees in positions of trust.

(4) Business ethics are next in importance to access and operations safeguards. Lack of ethics is a vulnerability found at the highest levels of management and among EDP managers and staff performing or supporting unethical acts for higher management. Accepted ethical standards are needed throughout the computer field.

(5) The next level of concern should be directed at the control of application and operating system programs, including safeguards against unauthorized modification and use, and proprietary aspects.

(6) The specialized and growing problem of preventing access to time-sharing systems by unauthorized users is of next importance.

(7) Finally, the special problem of protecting magnetic tapes in tape storage areas from vandalism and theft must be addressed.

Physical EDP areas of importance for safeguarding appear to be primarily those where manual, operational functions are performed. They are followed by computer systems, then programming offices, and finally magnetic tape libraries. An interesting conjecture is based on the apparent concentration of abuse in the areas of heaviest manual functions. As technical advances eliminate and reduce the size of manual activities, the incidence of abuse could diminish, independent of the degree of security efforts.

# APPENDIX

## Range of Acts Perpetrated in Each Vulnerability:

## Examples from Case File

RANGE OF ACTS PERPETRATED IN EACH VULNERABILITY:
EXAMPLES FROM CASE FILE

1. Poor Controls over Manual Handling of Input/Output Data

Case 75327* -- A keypunch operator in Stockholm, Sweden manipulated payroll data to produce 86 false payroll vouchers payable through the Swedish postal system. She cashed the vouchers at small, remote post offices that had either not received the computer listings of valid vouchers, or did not bother to check the listings before cashing the vouchers. She escaped to South America.

Case 75321 -- A data control clerk in a bank computer center embezzled $7,200. He diverted and stole checks being processed from a correspondent bank. For each check he then wrote a check for the identifical amount on his own checking account and then deposited it in a second checking account, also his own. When his own check turned up for processing, he destroyed it and substituted the stolen check. Thus, the check he wrote against his own account was never charged against that account.

Case 75316 -- A check proofing operator mutilated her own checks. This caused them to be rejected by the computer system and returned to her to be placed in a correctly encoded envelope for further processing. However, the operator failed to do this and resubmitted the checks. She did this repeatedly, so that the checks were never debited from her account balance. The loss was recovered and the proof operator was not prosecuted.

Case 75312 -- An EDP employee embezzled $190,500 by inflating payroll totals in order to make use of blank checks produced at the beginning and end of the payroll printer runs. He filled in the blank checks and forged the endorsements. He was caught and convicted and made partial restitution.

Case 74324 -- A man was convicted of a welfare fraud of $73,525. He convinced his former girlfriend, a clerk in a state department of public aid office, to cooperate with him by issuing emergency aid checks to welfare recipients, who then shared the gain with the perpetrators. Over a 6-month period, 173 unauthorized checks were distributed. The emergency aid disbursement process through on-line computer terminals had fewer controls than in normal welfare disbursement. The crime was discovered by an auditor.

---

*The first two digits of case numbers identify year of occurrence. The third indicates the type of loss (1=vandalism; 2=information or property fraud or theft; 3=financial fraud or theft; 4=unauthorized use or sale of services). The last digit or two digits is a sequence number.

Case 74323 -- A newspaper article alleges that five U.S. Federal Energy Administration payroll office employees altered personnel files to give them extra sick leave and annual leave. The employees were suspended, according to the news article, but recalled to work because they were the only people who knew how to run the payroll system.

Case 7524 -- Three oil company employees are alleged to have conspired to manipulate computer stored data and oil tank gauges to indicate a full delivery had been made to a refinery from tankers when only part of the load went into the tanks. The rest of the oil is alleged to have been delivered to two smaller companies. The acts were discovered when an inventory check revealed a discrepancy between the amount of oil in the tanks and the amount supposed to be in the tanks according to computer-stored records.

Case 7543 -- A police chief was suspected of altering his own driving record through an on-line computer terminal of a regional law enforcement computer network.

Case 72316 -- Several EDP employees threatened the president of their company that they would vandalize and change invoices being processed through the computer so that the company would lose money if the president did not double their salaries.

2. Weak or Nonexistent Physical Access Controls

Case 72113 -- In a hospital where a new on-line computer system had been installed, an unknown person gained access to a computer terminal area on several occasions and entered incorrect pharmaceutical orders for patients being treated by a doctor who was opposed to the new computer system.

Case 7414 -- A computer operator in one of two competing computer service companies broke into the rival company's computer facilities at 5:00 a.m. on a Sunday morning by waiting until the guard left and jimmying the front door. He then poured ten gallons of gasoline over the computer, peripheral equipment, and supplies. He powered up the computer and lit a match causing a massive explosion and fire that destroyed a large computer system. The operator, his employer and his employer's wife were convicted of arson and conspiracy. The computer operations manager is under indictment.

Case 7447 -- An unknown person gained access to a computer terminal room by asking the janitor to open the door for him. He picked the locks of the telephones and terminals to gain unauthorized use of time-sharing services.

Case 72212 -- An EDP employee or a vendor's maintenance engineer did $490,000 worth of damage to computer memory stacks by attacking them with a pointed instrument, probably a screwdriver.

Case 7219 -- An unknown person poured acid over telephone wires where they enter a building containing data processing equipment.

Case 7522 -- Twelve persons, including a computer manufacturer's employee, thought to be engaged in international espionage, were caught while taking computer components, maintenance manuals, magnetic tapes and circuit diagrams from computing facilities in Frankfurt and Karlsruhe, Germany. Financial losses were estimated to be $110,000.

Case 73111 -- An anti-Israeli demonstration was aimed at a bank, a symbol of Zionism, in Paris. Rioters blew out windows of a key-punch room and attacked the data processing facilities with Molotov cocktails, causing major damage in the data preparation areas.

3. Weaknesses in Computer and Terminal Operations Procedures

Case 6914 -- A keyboard operator in an on-line luggage control system at Orly Airport in France shattered a CRT screen with her high-heeled shoe in a fit of resentment.

Case 74313 -- In a large bank fraud in Germany, computer operators prevented bookkeeping entries by activating system interrupts from the computer console. Invoices were prepared by the system without recording the transactions.

Case 70410 -- A programmer analyst used his employer's computer under nonchargeable software development usage in conjunction with his personal outside consulting business.

Case 7348 -- A senior analyst sold computer time at a rate lower than that offered by his employer and charged the time to program testing.

Case 6711 -- A disgruntled computer operator dropped pieces of metal into an IBM 2740 terminal causing electrical shorts, fires, and considerable downtime. The operator was discharged and successfully prosecuted.

Case 72411 -- An EDP employee developed his own computer service business in a neighboring city using his employer's computer system. The perpetrator was discharged.

Case 72410 -- A computer operator in a university computing service center used the computer to prepare political campaign literature for a student election. The perpetrator was discharged.

Case 7217 -- An EDP employee sabotaged a computer, causing a week of downtime for a loss of $50,000. His purpose was to embarrass his new supervisor. The perpetrator was discharged and a civil suit was filed against him.

Case 7429 -- A night computer operator colluded with a head shipping clerk to manipulate data in an inventory system by erasing and substituting invoice numbers in an accounts receivable application; $20,000 worth of merchandise was stolen. The perpetrators were arrested and charged with grand theft.

Case 7427 -- A computer printer operator was paid to make an extra carbon copy of competitive bidding reports for industrial espionage purposes. The operator was discharged.

Case 7438 -- A computer operator printed copies of unemployment checks and deleted the copied record from the file. An auditor discovered the $10,000 fraud in a computer audit run. The employee was convicted and given a suspended sentence and 5 years' probation.

Case 7415 -- A computer operator working alone at night carried a hand gun because the computer center was in a high crime area. One night, out of frustration with the computer, he shot it with his gun.

Case 6941 -- A computer operator in a Norwegian service bureau extracted medical records of individuals with particular types of ailments and used them for marketing purposes.

4. Weaknesses in Business Ethics

Case 7527 -- A credit bureau sent advertising notices to the subjects of their credit information, offering to sell the credit files to them to prevent the files from being put into a larger computer-based credit system.

Case 7515 -- Two computer and peripheral equipment manufacturers engaged in charges and countercharges of unfair competition and industrial espionage and sabotage including wiretapping and destruction of products and production facilities. Civil suits have been filed.

Case 7523 -- A customer charged a computer equipment vendor with fraudulently representing the capacity and capability of a computer system and charged that the full system was never delivered and did not have adequate software.

Case 7539 -- One company made a loan to another company based on certain collateral. The pledging of the collateral was hidden by the company receiving the loan so that it could be reused for new loans. Computer listings containing fake data describing the collateral were used.

Case 73325 -- An ex-convict established a phony investment bank. He sent out fake confidential computer printouts to potential shareholders to lend credibility to his offer.

Case 73411 -- A customer installed a program packaged product without a license to do so. He was discovered and the program product was removed from the system.

Case 7445 -- A county commissioner privately contracted for business in which he used the county's computer system. The charge was conflict of interest, a second-degree misdemeanor.

Case 7446 -- A computer dating service was sued because referrals for dates were so few and inappropriate. The new owner of the dating bureau said that no computer was used at that time although use of a computer was advertised.

Case 73216 -- A convicted criminal filed an appeal against the U.S. Army claiming he was denied a fair trial by admission of computer-produced statistical summaries from which inferences of guilt were suggested. The appeal was denied.

Case 73316 -- A company advertised that computer-selected sweepstakes winners were to receive $250.00 vacation certificates by paying only $15.00. The certificates were for land promotion presentations at various resorts but did not include transportation. All certificates had the same computer-printed serial number.

Case 7249 -- According to a newspaper report, the U.S. Senate Watergate Committee was investigating secret ownership of a computer service firm by a well known national political figure. The firm caused McGovern for President political mailings generated from computer mailing lists to be ineffective because they arrived at voters' addresses the day after the national election.

Case 7237 -- Stockholders swindled by their company filed suit against the computer manufacturer that supplied their company with computing equipment, claiming the computer manufacturer failed to inform stockholders of the vulnerability of the computer products to fraud, and failed to provide sufficient security in its products. The suit was dropped before trial.

5. Weaknesses in the Control of Computer Programs

Case 75315 -- The manager of a bank computer center made unauthorized changes to the demand deposit accounting program to credit service charges to his and a friend's accounts rather than to the proper bank income account.

Case 75314 -- A programmer changed a dividends payment program to reduce dividends of eight stockholders and issue a check to a fictitious person in the total amount of the reductions. The loss was $56,000.

Case 7544 -- A part-time data processing instructor wrote and executed a program to print 50 copies of political campaign material urging defeat of a public schools override issue. The material was printed on a terminal located in his home.

Case 72219 -- The president of a French software company posed as a professor of computer science on a tour in the United States where he collected many free programs offered from more than 200 computer centers. He returned to France and sold copies of the programs he had collected. He was caught and fined 5,000 francs for the sale of one program. No action was taken concerning all the other programs he was selling.

Case 74210 -- A programmer was fired for unsatisfactory performance. He returned to the programming area at night and attempted to steal flow charts and record layouts for the program he had been working on. He was caught by a janitor but no action was taken against him.

Case 6542 -- A systems programmer replaced a computer operating system supervisory module with a new one that allowed him access to the area of storage used for the resident operating system.

Case 6521 -- Accounting clerks programmed and used a program called "fudge." It was run at the end of each month to change account balances until all column totals balanced correctly.

Case 7439 -- A programming manager in a savings and loan association changed updates to the savings program to ignore withdrawals from his account. He was convicted after he was caught by auditors when he made a keypunch error in an account number.

Case 72216 -- A computer specialist in the government taxation commission in a foreign country sold copies of program logic documentation describing the controls and checking on deduction claims in income tax forms.

Case 73213 -- A programmer in a small accounting firm took all copies of programs and documentation and moved a great distance away to set up his own business.

Case 73212 -- A 19-year-old girl convinced her boyfriend to steal copies of computer programs from his employer, a service bureau. She then attempted to sell them to customers of the service bureau. She was convicted and received a one-year suspended sentence.

Case 71319 -- A programmer created a sales commission account in a mail order company under the salesman name of Zwana to be the last account in the file. He changed the sales commission program to collect rounded down fractions of pennies into this last account. It was discovered after 3 years when the marketing organization chose the first and last accounts in the file for a public relations activity.

Case 72212 -- The owner of a software leasing company convinced programmers to take copies of programs from their employers and sell them to the software leasing company which then marketed the software.

6. Weaknesses in Operating System Access and Integrity

Case 74213 -- European news media reported that a 15-year-old London school boy compromised a commercial time-sharing system by obtaining and using operating system program listings to discover privileged user access codes, and was able to take over the time-sharing system.

Case 6942 -- Students obtained access to operating system accounting files and suppressed charges to their own accounts and obtained high priority services.

Case 6611 -- Students maliciously caused disruption of a time-sharing service when they tested the operating system and found a failure in the exception handling of filled physical disk storage.

Case 7317 -- Students using a time-sharing service discovered their accounting passwords had gained status to allow them to run restricted programs. The cause of the weakness was a bug in the operating system.

Case 7329 -- A programmer compromised an operating system and discovered cryptographic keys used to protect computer files.

Case 7441 -- A graduate student compromised a time-sharing system to convert his terminal to the functional equivalent of the computer console. He performed this act to convince management of the computer facility of the vulnerability of the time-sharing system.

Case 7343 -- A student wrote a program masquerading an an operating system. When a user attempted to log in, the masquerading program obtained his account number and then declared the system unavailable. The student used the account numbers discovered in this fashion for his own purposes to obtain computer time without charge.

7. Poor Controls over Access Through Impersonation to Time-Sharing Services

Case 7525 -- A time-sharing user discovered he was being underbid by small amounts in contract negotiations where the data was stored in a time-sharing service computer. He concluded that a recently terminated employee retained knowledge of his password. He had the password changed and the problem disappeared.

Case 74316 -- A man was convicted in France of counterfeiting bank cash dispenser credit cards. He impersonated a bank official to obtain the personal identification numbers associated with the cards by calling the card number holders requesting them to report their numbers so that new numbers could be assigned.

Case 6543 -- Unauthorized use of time-sharing service was discovered when a computer terminal repair password was being used by unauthorized persons.

Case 6842 -- High school students found a time-sharing user's passwords on discarded terminal printouts. The students used the passwords to obtain unauthorized services.

Case 7344 -- An unauthorized user of a commercial time-sharing service was found to have used 8 hours of computer time by continuing to use a a password assigned him only for demonstration purposes. The password had not been purged as scheduled.

Case 72210 -- A former employee of a credit-reporting company obtained credit reports by using identification numbers of legitimate subscribers that he had obtained in his previous employment.

8. Weaknesses in Magnetic Tape Control

Case 7528 -- An EDP employee stole a magnetic tape and used it to have address labels printed for use in organizing activities.

Case 74212 -- A mailing house employee was caught in attempts to sell magnetic tapes containing mailing lists to a competitor of the mailing house.

Case 7511 -- An EDP employee sabotaged his company be erasing magnetic tapes with a degausser.

Case 6212 -- An EDP employee in a bank destroyed all dividend accounts for shareholders of a large company by destroying the magnetic tapes containing the data with a sharp instrument.

Case 7216 -- A tape librarian in an insurance company was fired but given a 30-day notice. During that time she replaced most of the magnetic tapes in the tape library with scratched tapes.

## REFERENCES

Cressey, D. Other People's Money. Wadsworth, 1971

Geis, G. (Editor). White Collar Criminal, The Offender in Business and Professions. Atherton Press, 1968.

Smigel, E. and Ross, H. Crime Against Bureaucracy. Van Nostrand Reinhold, 1970.