COMPUTER CRIME AND SECURITY:
AN ANNOTATED BIBLIOGRAPHY OF THE PERIODICAL LITERATURE

David Graham
Ulrike Richardson

U.S. General Accounting Office
Office of Library Services
Technical Library Branch
September 1984

GAO Libraries Bibliography Series
OLS-84-03

TABLE OF CONTENTS

		Page
I.	The Computer Security Problem: An Overview.....	1
II.	Computer Criminals: Who They Are and How They Do It.....	12
III.	The Legal Response.....	19
IV.	Safeguarding the System.....	22

INTRODUCTION

It has been estimated that the loss in the United States from computer crime may be $1 billion annually, and the problem cannot be measured in dollar value alone. Confidential personal and business information, even our national defense secrets -- any data stored on computers -- are possible targets of some form of computer abuse, from simple unauthorized access to sabotage.

This bibliography of periodical articles from 1980 to 1984 explores a wide range of computer crime and security issues. Part I considers the extent of the problem and management's responsibility in meeting it. Part II spotlights computer criminals and the motivations for and variety of their crimes. Part III concerns the legislation (or lack thereof) which addresses computer crime. And Part IV reviews computer security controls which are presently available, including security hardware and software, and management controls such as insurance and the audit.

I. THE COMPUTER SECURITY PROBLEM: AN OVERVIEW

Ball, Leslie D. "Computer Crime Is a Growth Business." Across the Board, 19, No. 6 (June 1982), 42-49.

Ball's article is a good overview of computer crime, covering types of common crimes (theft of assets, electronic funds transfer, insurance fraud) as well as how these crimes are committed. Ball feels managers contribute to the incidence of computer crime by giving data processing staff too much responsibility over computers they themselves do not understand. Also, computer criminals get away with theft by blaming the computer and then erasing improper transactions. A discussion of current and proposed legislation dealing with the problem is also presented.

Bequai, August. "What Can be Done To Stem Rising Computer Crime?" Office, 98, No. 5 (November 1983), 10, 83.

Some estimates put U.S. losses from computer crime at $1 billion annually. In this simple overview of the problem, the author identifies five categories of computer-related crime. These are sabotage, theft of data, theft of property, theft of services, and financial fraud. He then cites a number of recent examples of computer crimes. The author makes several suggestions to help stem the growing problem: management must provide adequate security for its systems and be willing to prosecute culprits even in the face of public ridicule; criminal investigators must become better trained in handling computer crime; the courts must equip themselves to handle high technology cases. In addition, the author proposes a code of ethics for computer personnel.

Blakeney, Susan. "Computer Crime: A Worldwide Concern." Computerworld, 17, No. 52 (December 26, 1983), 57-60.

Computer experts from Australia, Brazil, France, Italy, Japan, Sweden, and West Germany were polled to determine the extent of and attitudes toward computer crime in their countries. Six of the countries seem to have a major problem with computer crime, though it may manifest itself in various ways, ranging from sabotage in Italy to Soviet espionage in Sweden. Most countries, however, agree that data processing personnel are the main culprits. The questions of controls and countermeasures are also addressed in some detail.

Campbell, Robert P. "Locking Up the Mainframe. (Part I)." Computerworld, 17, No. 41 (October 10, 1983), In Depth, 1-14.

Campbell, Robert P. "Locking Up the Mainframe. (Part II)." Computerworld, 17, No. 42 (October 17, 1983), In Depth, 1-13.

Part 1 of this article outlines the current state of the art of computer security technology and what we can expect in the future. The author's predictions can be viewed in the light of his contention that previous predictions have proven overly optimistic. Part 2 discusses the socioeconomic aspects of computer security, including legal issues. The author draws several conclusions. First, he concludes that much more of the annual data processing budget should be allocated for system security, but also that much more of the security burden should be placed on system vendors. Second, he believes there is a "chilling" likelihood that computer crime will soon extend to the breaching of home computers. Ironically, this may prove to be the best motivation for "more trustworthy architectures." Finally, he thinks that much more government

intervention is needed, considering the potential magnitude of computer security problems.

Coates, Joseph F. "The Future of Computer Data Security: News, Good News and Better News." Vital Speeches of the Day, 48, No. 9, 280-284.

The computer industry is not sufficiently aware of threats to its data, and neither industry nor government is planning for ways to address the impact of computers on society. Coates provides discussions of what he calls the "big" issues involved with the computer revolution. These are privacy, use of the computer as a political tool by extremist groups, antisocial uses of computers, and the vulnerability of the financial industry to disruption of computer systems by foreign powers. He then provides specific suggestions for improving data security, all of which are rather controversial, such as setting IQ ceilings for computer operators.

"Computer Security." New Scientist, 99, No. 1365 (July 7, 1983), 11-19.

Actually three articles covering a wide range of computer security issues: "Computer Thieves Steal £2.5 Billion a Year," "How To Review Your Security," and "Cryptography for Beginners."

"Computer Security: What Can Be Done?" Business Week, No. 2809 (September 26, 1983), 126-130.

A breezy introduction to computer crime and security in the big business environment, this article touches briefly on a wide range of issues, from management attitudes to password standards.

"DP Crime: Where There's a Will, There's a Way." Computerworld, 17, No. 52 (December 26, 1983), 53-54.

As computer security becomes more sophisticated, so do computer criminals. One expert recommends that one percent of the annual corporate budget go into computer security. Other recommendations include a computer security manager who reports directly to the management information services director, a written security policy statement, and regular but unannounced DP audits. The article also points up the growing role of technology in deterring computer crime and briefly discusses security software, dial-up/call-back security devices, and encryption devices.

Englade, Ken. "Can You Keep a Secret?" Savvy, 5, No. 1 (January 1984), 65-67.

This is a brief non-technical introduction to the computer security problem. Designed primarily to alert managers to the immensity of the problem and the need to take action, the article briefly discusses various types of computer crime and various means of combatting it. Includes a directory of security software manufacturers, computer security organizations, and security consultants.

Galloway, James R. "Crime, Abuse, and the Computer: the Problem and the Federal Experience." GAO Review, 19, No. 3 (Summer 1984), 16-17, 35.

The author, a senior evaluator at the U.S. General Accounting Office, examines techniques used by computer criminals and discusses crime in the government, where instances of crime are frequently detected by accident. He then focuses on the federal agencies with responsibility for policies and guidance on matters of information system security. He concludes by reviewing the status of computer crime legislation introduced into the 98th Congress.

Gassaway, Paul. "Theft of Computer Time." Office Administration and Automation, 44, No. 11 (November 1983), 41-43.

Employees' use of company computers for non-company activities is one of the more benign breaches of database security. Often, in fact, simple unauthorized computer use is not punishable by law. The author contends, however, that by running up costs, taking up data storage space, and slowing response time, this theft of computer time poses a major problem for managers. Among the security measures the author recommends are restricting physical access and monitoring transactions.

Gilchrist, Bruce. "Morality in the Computer Classroom." Datamation, 28, No. 12 (November 1982), 222-228.

While estimates of the extent of computer crime vary, the fact remains that with the increasing use of computers by millions of people, conditions for increasing crime are ripe. Gilchrist focuses on the educator's responsibility for teaching new users how to interact appropriately with computers. He feels computer abuse should be discussed during classes so that illegal activity is discouraged and students become aware of the need to defend systems against abuse, as well as recognize attempted crime. One problem that currently exists is the cavalier attitude of computer instructors toward their systems. This has led to encouragement of students trying to break into their organization's own computer system and the widespread distribution of passwords to unauthorized users.

Hammond, James H, Jr. "Guarding the Gate: Data Processing Security." Mortgage Banking, 43, No. 7 (April 1983), 27-35.

Writing from the auditor's perspective, the author outlines the best approach to a Data Processing Security Evaluation (DPSE) and discusses the most likely areas of weakness in system security. These include poor physical security of unauthorized access, inadequate disaster and backup plans, and poor personnel practices.

Henriques, Vico E. "Guilty, Not Guilty, or Not So Guilty?" Technology Review, 85, No. 3 (April 1982), 24-30.

Henriques, president of the Computer and Business Equipment Manufacturers Association, presents his organization's view that most of the press concerning computer crime is speculative and sensational. He criticizes the view that most computer crime goes unreported, fueling a "tip of the iceberg" myth. Instead, he quotes a Peat, Marwick and Partners study which states that crime occurs only in about two instances for every 10,000 installations. Henriques believes that very few data processing professionals are involved in crime. He also feels that as long as humans deal with computers, there will be some abuses. However, he feels that "computer crime is not now, never has been, and never will be out of control ... "

Kelly, Orr. "Pentagon Computers: How Vulnerable to Spies?" U.S. News and World Report, 95, No. 18 (October 31, 1983), 36-37.

Pentagon computers are so vulnerable to sabotage that "tiger teams" of government computer experts can almost always break into them in simulated tests. Since security must be built into a system rather than added on, the government is stuck with thousands of computers whose vulnerability cannot be

eliminated until the computers are replaced. The most likely saboteur is the "trusted employee" who is really a hostile agent. The article briefly describes the techniques which might be used to sabotage U.S. military computers. The vulnerability of civil agency computers is also mentioned.

Landwehr, Carl E. "Formal Models for Computer Security." ACM Computing Surveys, 13, No. 3 (September 1981), 247-278.

The need to ensure the security of military information is universally acknowledged. Landwehr begins his paper with a discussion of military classification and clearance procedures, and he examines how automation aggravates security problems. The remainder of this article focuses on models created to deal with the automation problem.

McKibbin, Wendy Lee. "Who Gets the Blame for Computer Crime?" Infosystems, 30, No. 7 (July 1983), 34-36.

The ultimate responsibility for the security of a computer system lies with the data processing manager, and he or she is liable to criminal prosecution if the system is breached. To prevent this, the data processing manager must have top management support and must learn to "think like the enemy." The article is best in its discussion of the likely suspects and motives for computer crime.

Moulton, Rolf T. "Network Security." Datamation, 29, No. 7 (July 1983), 121-124.

Computer networks, connected over some distance by diverse communications links, are particularly vulnerable to security breaches. The author discusses the liabilities of four categories of networks: intrabuilding, local area,

domestic, and international. He suggests five major issues management must consider in implementing a network security program: the data security policy, the risk and vulnerability assessment, access control and authorization, data encryption, and the security audit and audit report.

Parker, Donn B. "How Much Computer Abuse Is There?" Computer Security Journal, 2, No. 1 (Spring 1983), 85-89.

In this article Parker seems to be responding to criticism of one of his earlier works, Crime by Computer. In that first work he reported on cases of computer crime in terms of criminal activity per computer, which in 1975 was reported to be five cases per 10,000 computers. Here he disavows the validity of these numbers (of use only to actuaries) while maintaining that his major point remains the same: statistics on crime are not all-important -- safeguarding computers is.

"Protecting the Corporate Data Resource." Computerworld, 17, No. 48 (November 28, 1983).

This 30-page Computerworld special report includes articles on program piracy, data encryption, personnel security, and a glossary of the latest computer fraud jargon, among other features.

"A Question of Leadership." Datamation, 29, No. 2 (February 1983), 119-128.

Six computer security specialists air their frustrations and concerns in this non-technical panel discussion. The main concerns seem to be the need to educate computer users at all levels in the ethical use of computers, and the question of who is responsible for the users' education.

Seaman, John. "Beware of the Wireless 'Datanapper'." Computer Decisions, 15, No. 7 (July 1983), 54-58.

The author, citing a study by J. Michael Nye, a computer security consultant, dicusses the vulnerability of wireless data transmissions to interception. Microwave, satellite, and radio transmissions can all be intercepted with varying ease, using readily available equipment. While there is no foolproof way to stop thieves, data encryption seems to be the most effective countermeasure. At present, encryption is prohibitively expensive, but Nye expects the cost to drop.

Silverman, Martin E. "Selling Security to Senior Management, DP Personnel, and Users." Computer Security Journal, 2, No. 2 (Fall/Winter 1983), 7-17.

Convincing management, financial officers, and data processing personnel of the need for computer security is a business problem, not a technical problem, and must be approached using traditional business principles. A need for security must be established and a means provided to fulfill the need. The benefits must outweigh the costs. Short, non-technical awareness sessions are the best means of educating various groups in the need for security. The article is chatty and non-technical itself -- an excellent exercise in public relations.

Simkin, Mark G. "Is Computer Crime Important?" Journal of Systems Management, 33, No. 5 (May 1982), 34-38.

In an attempt to determine if computer crime is indeed an important concern, the author examines seven measures of the concept of "importance." These are growth, average losses, likelihood of occurence, catastrophic consequences, expert opinion, practitioner opinion, and public opinion. Only growth and average losses indicate that computer crime is something to be concerned with -- the other measures tend to indicate that the problem is not as severe as some believe.

"The Spreading Danger of Computer Crime." Business Week, No. 2684 (April 20, 1981), 86-92.

Computer fraud is occurring 20 times more frequently than 10 years ago with reported losses of at least $100 million a year. This is due to the spread of low-cost personal computers and increases in the number of people who have access to computers through remote terminals. Examples of sophisticated computer fraud, including the Wells Fargo case, the Dalton School case, Union Dime, and others are discussed. Corporate executives have failed to set up anti-fraud devices largely because they are unaware of the computer's complexity and rely too heavily on data processing staff, who resist controls that might slow data processing. Encryption software may help solve fraud problems, and sales of these devices are exploding. Access control software may stop internal computer frauds. Limiting access of programmers to their software once it is operating can be effective in limiting fraud committed by data processing personnel in performance of their jobs. Finally, audit software allows non-EDP auditors to obtain audit reports.

Statland, Norman. "What You Should Know About Data Security." Price Waterhouse Review, 26, No. 3 (1982), 2-10.

The author contends that computer crime is growing at least as fast as the use of computers -- at a 15 percent compound annual rate. In a question-and-answer format, he discusses what a company can do to prevent or minimize losses. These measures include recognizing data security risks, performing a security review, and determining what hardware and organizational controls are needed.

Vohs, Dennis. "The Financial Executive's Role in Computer Security." Financial Executive, 49, No. 4 (April 1981), 30-32.

This article provides an overview of the growth of computer crime and types of crime currently being committed, including data theft and sabotage. The "timebomb" planted in programs can destroy whole data banks and can be set to "explode" if a programmer loses his job. Such incidents can be very difficult to prevent since apparently unrelated events trigger the explosion. To prevent such occurrences, financial executives must take an active part in protecting hardware, controlling access to computers, and protecting software. Uniform software packages, which are created and maintained by independent professionals, may help prevent software sabotage by disgruntled programmers.

Ward, Gerald M. and Donald A. McGovern. "Security Problems Proliferate Along With Personal Computers." Management Review, 72, No. 7 (July 1983), 29-31.

Microcomputers pose significant threats to data security. They may be used as programmable terminals and provide unauthorized access to a mainframe computer. The informal environment of micros and unsophisticated software means that management often has little control over system access and program changes. Much of the available microcomputer software does not leave an audit trail, its size makes it easy to steal, and its physical nature makes it easy to destroy. The author stresses that management must have the same controls over micro systems as over mainframe systems, and provides a checklist to help management address security issues.

II. COMPUTER CRIMINALS: WHO THEY ARE AND HOW THEY DO IT

Alexander, Charles. "Crackdown on Computer Capers." Time, 119, No. 6 (February 8, 1982), 60-61.

Notorious computer capers, computer safeguard devices, and software piracy are some of the issues Alexander discusses in this article. While none of the topics is given extensive analysis, the article is helpful to those seeking current background material on computer crime.

Becker, Jay. "Who Are the Computer Criminals?" New Scientist, 85, No. 1998 (13 March 1980), 818-821.

The author, who is the director of the National Center for Computer Crime Data in Los Angeles, claims computer criminals are not as bright as many criminologists maintain. This article debunks the myth of the computer criminal as genius and presents evidence that the environment rather than personality can predict and prevent computer crime. The following perceptions of computers held by computer criminals are described as: 1) computer as play-pen, 2) computer as the land of opportunity, 3) computer as cookie jar, 4) computer as war zone, 5) computer as soapbox, 6) computer as fairyland, and 7) computer as toolbox.

"Beware: Hackers at Play." Newsweek, 102, No. 10 (September 5, 1983), 42-48.

Computer hacking (using home computers to break into large databases) has been called a teenage "rite of passage" and a "nondestructive form of social deviancy." This article explores the motivations and successes of hackers and the anxiety they have created in the computer world.

Bigelow, Robert P. "Computer Crime Is a People Problem." Infosystems, 27, No. 7 (July 1980), 80.

The author asserts computer crime is largely due to a lack of precautions concerning users and is not due to weaknesses inherent in the computer system itself. He traces some well-known cases of computer crime and describes methods used by criminals to gain access to systems.

Bloom, Robert. "Catching the Computer Crook." Infosystems, 27, No. 7 (July 1980), 30-35.

The FBI's profile of computer criminals spotlights an individual from 18 to 30 years old, outwardly loyal to the company, with no previous legal difficulties, and very bright. This article describes renowned computer criminals and their crimes and briefly explores the responsibility of the auditing profession in detecting such crime. Legislation, including the Federal Computer Systems Protection Act of 1979, is discussed, as is the response to such legislation by opponents who feel such revision of the law is unnecessary.

Bologna, Jack. "Motivated Climate Prevents White-Collar Crime." Journal of Systems Management, 31, No. 7 (October 1980), 36-38.

Bologna focuses on the state-of-mind of employees with access to a firm's assets and recommends that motivational climate in a data processing installation be assessed in an attempt to reduce white-collar crime. Past occurrences indicate that work-related frustration may lead to sabotage, large-scale fraud, or embezzlement. He recommends an annual motivational climate study, such as the University of Michigan's Survey of Organizations, to help defuse job frustration.

Colvin, Bill D. "Training Computer Crime Investigators." EDPACS, 9, No. 9 (March 1982), 6-11.

The author, an FBI staff member, discusses areas of vulnerability in computer installations and claims that law enforcement officers can be trained to investigate 93 percent of all computer crimes, while recognizing the need for outside consultation on the remaining seven percent. He classifies computer crime into six "crime schemes" ranging from the simplest, input/output alteration (level one) to communications (level six). Skill levels needed to commit these crimes and level of training needed by law enforcement personnel to discover them are then presented.

"Computer Security." Dun's Business Month, 120, No. 6 (December 1982), 94-96.

The article focuses on four key elements common to computer crimes. The first of these is the elevation of computer criminals to near cult status for their ability to "beat computers." Second, computer criminals are discovered by accident or not at all; those who are discovered are seldom prosecuted. Third, computer criminals are thought to be extraordinarily bright. Finally, computer criminals, even when caught, are seldom punished. From the data processing manager's perspective, the most important security principle may still be one of the simplest: limit access as far as possible.

"Filching Figures." Time, 121, No. 3 (January 17, 1983), 41.

A case involving the attempt of a former Federal Reserve Board employee to obtain money supply figures in advance of their scheduled public release is discussed. The article also reveals how the crime was discovered.

Grant, Peter and Robert Riche. "The Eagle's Own Plume." Proceedings -- U.S. Naval Institute, 109, No. 7 (July 1983), 29-34.

The authors describe convincing scenarios in which military computers are penetrated by saboteurs, with dire results. Two subversion techniques, the "Trap Door" and the "Trojan Horse," are discussed in some detail. The case is made for pursuing computer security research. The authors also recommend the use of penetration techniques as an offensive weapon.

Guncheon, Kelly F. "Tracking Computer Fraud: Blue Cross Plans Gird to Battle Illegal Claims." Hospitals, 56, No. 19 (October 1, 1982), 104-112.

Because of the proliferation of electronic claims processing, hospital employees responsible for billing medical services are in a better position to defraud hospitals. Paper trails have virtually disappeared, and computer operators often blame the system for their errors or transgressions. To combat improper activity, 20 Blue Cross and Blue Shield plans have organized their own antifraud investigation teams to deal with Medicare claims, private-sector fraud, and fraud prevention. This article provides information on their investigative techniques and procedures.

Henkel, Tom. "Radio Waves from Your System Giving Away Your Secrets?" Computerworld, 17, No. 19 (May 9, 1983), 1, 10.

Many parts of a computer system give off radio waves, called radio frequency interference (RFI), which theoretically can be monitored and thus provide criminals with computer data. In this brief but intriguing article, two positions on the security implications of RFI are discussed: the first, that with the proper equipment, these emanations can be successfully monitored and hence represent a substantial security risk; the second, that monitoring RFI is

extremely complicated and promises so little return that the problem is negligible.

Kolata, Gina. "Students Discover Threat: The Discovery of Simple But Powerful Ways To Break Into Computer Systems Poses a Problem: Who Should Be Told of the Threat and How?" Science, 215, No. 4537 (March 5, 1982), 1216.

The question raised in this article is how information relating to a threat to large numbers of computer systems should be disseminated without increasing the potential for additional abuse. The Stanford Research Institute (SRI) was told about a way to trick a system into believing the user is another user logged into another terminal, as a result of a discovery by University of California students. SRI told computer and trade manufacturing associations of the threat, as well as the National Security Association. The NSA, however, while sharing views with SRI, maintains it would not have initiated discussions about the problem.

Kolata, Gina. "When Criminals Turn to Computers, Is Anything Safe?" Smithsonian, 13, No. 5 (August 1982), 117-126.

Teenage "whiz kid" involvement with computer crime as well as adult techniques for infiltrating computers are discussed in this article. The motivation of teenagers involved in disrupting or stealing from computers can be attributed in part to the need to impress peers as well as the development of a kind of addiction to programming, often called "hacking." The article also mentions adult crime, including a fascinating discussion of Department of Defense "tiger teams" set up to try to infiltrate DOD computers. These teams

were eventually phased out because they were invariably successful at getting any information from any computer.

Perry, Tekla S. and Paul Wallich. "Can Computer Crime Be Stopped?" IEEE Spectrum, 21, No. 5 (May 1984), 34-35.

Largely anecdotal and very readable, this article describes numerous techniques for breaching the security of computer systems. A brief discussion of existing security technology is not particularly reassuring.

Simkin, Mark G. "Computer Crime: Lessons and Directions." CPA Journal, 51, No. 12 (December 1981), 10-14.

Characteristics of common computer abuse are discussed by the author and examples of crimes occurring in recent years are given. Many crimes have common traits: they are performed with unsophisticated procedures, many of them happen through lack of controls rather than failure of controls, and few are committed by programmers. The author believes that likely targets of future crimes include banks, non-bank financial institutions, and small data processors. Computer crime is important to auditors because of increased auditor liability and the provisions of the Foreign Corrupt Practices Act of 1977.

Tompkins, Fred. "Computer Crime Catalog: Techniques and Targets of Computer Abuse." Bulletin of the American Society for Information Science, 8, No. 3 (February 1982), 24-26.

This article provides an excellent introduction to commonly used techniques for computer tampering. These include "data diddling," "logic

bombs," "salami," and "Trojan horses." Explanations of these techniques are given, and serve as illustrations of how easy computer abuse is to commit.

"Who Cooked the Computer?" Newsweek, 99, (March 1, 1982), 61.

This brief article discusses a case evolving at the advertising agency of J. Walter Thompson in which "data diddling," or the entering of faulty data, occurred. This appears to have been done either to increase a sales commission or impress management with sales performance. As a result of the crime, net earnings for four years were adjusted downward by $12 million, and the company's stock fell 21 percent.

Bequai, August. "Federal Computer Crime Legislation Is Needed." DM, Data Management, 19, No. 5 (May 1981), 22-24.

The author traces the history of the proposed Federal Computer Systems Protection Act. He discusses its provisions and the position of opponents to the legislation. Critics of the legislation claim such a bill would unleash floods of new government regulations and would be detrimental to states' rights. Bequai also discusses the assertion that computer crime is non-existent and originates in management folklore.

Brownstein, Ronald. "Computer Communications Vulnerable as Privacy Laws Lag Behind Technology." National Journal, 16, No. 2 (January 14, 1984), 52-57.

The laws governing eavesdropping on computer-to-computer communications are fuzzy or non-existent. Criminal elements and law enforcement and other federal agencies alike use this situation to their advantage. Pointing up a generally lackadaisical attitude in Congress, the author discusses the legal environment of computer privacy, especially as concerns electronic mail, wire-tapping, and computer matching.

Glynn, Elizabeth A. "Computer Abuse: The Emerging Crime and the Need for Legislation." Fordham Urban Law Journal, 12, No. 1 (1983-1984), 73-101.*

Existing statutes have been used with only limited success in prosecuting computer criminals. Glynn examines in detail the state of computer crime legislation at the federal and state levels and calls for development of new legislation to cut computer abuse.

* Available in the GAO Technical Library on LRS fiche 83-17018

Johnson, Bob. "DPers on Weg Ruling: Personal Use of CPU Same as DP Abuse." Computerworld, 16, No. 19 (May 10, 1982), 1, 4.

This article discusses a New York criminal court ruling that the use of corporate computers for personal business is not illegal. A survey of DP executives conducted by Computerworld, however, revealed that they do consider personal use of a corporate computer to be abuse and would terminate employees caught tampering with computers. One key feature of the court ruling was that the firm involved did not publish documents prohibiting personal use of computers. Johnson points out that a company must make employees aware of what can and cannot be done with company DP equipment.

Nellis, Joseph L. "Computer Law Lags Behind Technology." DM, Data Management, 20, No. 8 (August 1982), 14-15.

Nellis addresses the need for uniform federal laws dealing with computer crime and cites cases where theft or fraud occurred and convictions were not obtained because of legal loopholes. At the time this article was prepared, only 14 states had addressed computer crime, and these laws vary considerably. No specific legislation on computer crime has been enacted. This has led to difficulty obtaining prosecutions.

Ognibene, Peter J. "High-Tech Miscreants Beware: Congress Is Moving Against Computer Crime." National Journal, 16, No. 33/34 (August 18, 1984), 1573-1577.

On July 16, 1984 the President signed the Small Business Computer Crime Prevention Act. Two related bills (HR 5616 and S 2270) seem likely to pass Congress soon in some form. This article discusses the details of the bills and the growing Congressional interest in cracking down on computer crime.

"White-Collar Crime: A Survey of Law." American Criminal Law Review, 18, No. 2 (Fall 1980), 165-384.

While this entire issue is devoted to white-collar crime, the most pertinent information to this bibliography is found on pages 370-386. This section focuses on the definition of computer crime, categories of computer crime, and provisions of title 18 of the United States Code applicable to computer crime. Pertinent cases also are cited.

"Access Control Hardware." EDPACS, 9, No. 8 (February 1982), 9-11.

This article describes new developments in access control devices, including fingerprint control, signature verification control, hand geometry control, and eye blood vessel control. Vendors offering these types of systems are listed, as are key features in each system.

Bernhard, Robert. "Breaching System Security." IEEE Spectrum, 19, No. 6 (June 1982), 24-31.

There is considerable debate concerning the magnitude and seriousness of computer crime and the amount of control needed to safeguard data processing systems. The first half of this article explores this debate in some detail, presenting the views of prominent data processing managers. The second half of the article describes systems designed to detect tampering, including operating systems (OS), and the kernel approach, developed by Honeywell. Also included is a transcript of a lecture given by William H. Murray, manager of Data Security Support Programs of IBM, on some typical means of penetrating system controls, including eavesdropping and use of a Trojan horse.

Blanding, Steven F. "Computer Fraud Auditing -- A Case History." EDPACS, 9, Nos. 2 & 3 (August/September 1981), 1-23.

Blanding relates a case of computer fraud he dealt with while an EDP audit supervisor for the Commonwealth of Virginia. The article includes descriptions of the fraud, which, as in many cases of fraud, did not include any brilliant techniques. It also includes an overview of the systems in operation at the time of the fraud and techniques used by fraud investigators.

Cerullo, Michael J. "Safeguard Your Minicomputer System." Financial Executive, 51, No. 7 (July 1983), 30-41.

The author proposes a comprehensive management approach to the security of a medium-size minicomputer system, covering accidental damage as well as unauthorized access. Two areas of emphasis distinguish this article from most others: the author recommends a series of strong personnel controls, including adequate compensation and opportunities for advancement, and stresses that only cost-justifiable controls be implemented.

Cohn, Arnold M. "Total Information System Security." Journal of Systems Management, 33, No. 4 (April 1982), 14-17.

This article asserts that most major information thefts are possible not because of computer programming fraud, but instead because of poor security in business procedures. He points out three necessary levels of systems and data security: 1) the prevention of unauthorized persons from using the system, 2) the capability of correcting erroneous data and identification of unauthorized users to management, 3) the ability to re-create the system if it is somehow destroyed. Security measures for both batch and online systems are then outlined.

Comer, Mike. "Contingency Planning -- and the Audit." Accountancy, 94, No. 1075 (March 1983), 58-61.

The author contends that because computers concentrate data in a single system, they are particularly risk-ridden. In planning system security, management must undertake a risk evaluation and a risk management study which classes risks in the following categories: risk acceptance, risk avoidance, risk transfer, or risk reduction. Includes an enlightening discussion of computer insurance.

"Computer Security." Electronics, 57, No. 5 (March 8, 1984), 121-140.

A series of four technical articles: "Operating Systems Key Security with Basic Software Mechanisms," "On-Chip Hardware Supports Computer Security Features," "Call-Back Schemes Ward Off Unwanted Access by Telephone," and "Security-Minded System Design Can Protect Data Bases."

Davidson, Thomas L. and Clinton E. White Jr. "How To Improve Network Security." Infosystems, 30, No. 6 (June 1983), 110-112.

The authors discuss the security liabilities of computer networks and recommend the usual safeguards, including security software and data encryption. The article is distinguished by its discussion of data encryption in the network environment, where conventional encryption key distribution methods are vulnerable to fraud. The authors propose a modified key distribution system which improves user identification.

Dietz, Lawrence D. "Computer Security: Not Just for Mainframes." Mini-Microsystems, 15, No. 6 (June 1982), 251-255.

System security is becoming increasingly important as system vendors face liability for losses caused by the lack of safeguards in a computer if it is used to defraud an organization. The Foreign Corrupt Practices Act has caused vendors to attempt to improve security since it requires businesses to safeguard their data from the possibility of computer crime. The typical security budget for data processing installations is predicted to jump from $5,000 in 1981 to $30,000 in 1983, and these figures represent only add-on security provisions. Dietz then provides a list of definitions of computer crime tactics

(salami, spoofing, superzap) and file protection packages available to defend against these attacks.

Gillard, Collen and Jim Smith. "Computer Crime: A Growing Threat." Byte, 8, No. 10 (October 1983), 398-424.

This article is best in its description of the tools of computer security, particularly the SAU, a dial-up/call-back unit which verifies the location of an access request. The article as a whole is a good overview of the computer crime problem.

Hardenburg, Kurt L. "Controlling Systems Programming Activities." EDPACS, 7, No. 7 (January 1980), 1-20.

Hardenburg discusses methods of monitoring the systems programmers in an organization to ensure computer security. He contends programmers have too much freedom in many DP installations, and he presents a three-phase system software control procedure to alleviate the problem.

Howe, Charles L. "Coping with Computer Criminals." Datamation, 28, No. 1 (January 1982), 119-128.

Naivete on the part of MIS managers is a key problem in computer security. Data processing professionals are often too reliant on hardware and software and too trusting when it comes to personnel. To solve this problem, the following steps should be taken: 1) a policy statement covering computer usage should be issued, 2) potential employees should be checked before they are hired, 3) an information security department should be formed, and 4) management should receive some sensitivity training to help it spot problems that may lead employees to computer crime.

Inglesby, Tom. "Do I Need To Limit Access Anymore?" Infosystems, 30, No. 2 (February 1983), 74-76.

This is a brief, non-technical review of access control problems and solutions. Two recent developments are discussed in some detail. One is a radio token system which is worn on the belt and signals detectors to allow access to terminals or terminal rooms. As an added element of security, a card key is needed to activate the token. The second development is an identification system which reads the unique pattern of veins on the back of the eyeball. Other intriguing developments, mentioned only in passing, include identification by palm print, hand geometry, fingerprints, voice patterns, and signatures.

Kelley, Joseph T. "Computer Security: The Hidden Risk." Governmental Finance, 10, No. 3 (September 1981), 25-28.

Risks to computer systems generally fall into one of three categories: loss of data integrity, loss of data confidentiality, and loss of data processing availability. These categories can be used to classify damage to the data processing system and to help management perform a risk analysis to weigh impact of risks and cost of protection.

Kesney, Ed. "Shielded DP Rooms Combat Industrial Espionage." DM, Data Management, 19, No. 7 (July 1981), 22-23.

Radio Frequency (RF) shielded computer rooms protect computer facilities from persons attempting to scramble data or steal it. This article discusses costs and benefits of this means of protecting data processing facilities.

Lasden, Martin. "Computer Crime." Computer Decisions, 13, No. 6 (June 1981), 104-112, 116-124.

This is a very comprehensive article covering many aspects of computer crime in a round-table discussion format. Discussions include ways of preventing fraud, new systems being designed to restrict access, legislation concerning computer crime, and the position of vendors on computer crime.

Ochs, Laurance J. "Is Your Computer Fraud Insurance Adequate?" ABA Banking Journal, 75, No. 10 (October 1983), 112-113.

The author analyzes five major computer fraud insurance policies and discovers holes in each. Most notable is that none of the policies adequately defines what is covered.

Peterson, Ivars. "Keeping Secrets Secret." Science News, 120, No. 16 (October 17, 1981), 252-254.

Since it is now possible to wiretap data transmission with inexpensive equipment available at many computer stores, access control to computers in communications networks is increasingly vital. However, there is growing debate concerning the effectiveness of the National Bureau of Standards' DES encryption standard. This article discusses private research into cryptography and the government's resistance to such research on the basis of potential danger to national security.

Ramsgard, William C. "Security at Sign-On Time." Journal of Systems Management, 33, No. 2 (February 1982), 32-33.

The sign-on procedure is discussed in detail in this brief article. Included are 14 tips on how to establish an effective procedure. Among them are the use of a unique human characteristic in the procedure, such as voice or

fingerprint, the publicizing of all controls, and the inclusion of a personal item in the password, such as a favorite food.

Rhodes, Wayne L. "Protecting the Data Cookie Jar." Infosystems, 28, No. 8 (August 1982), 36-40.

The trend toward distributed data processing and shared database systems is greatly contributing to the need for increased access controls. Human error may cause user problems because so many individuals share the system. This article discusses the need for software security packages, including Boole & Babbage's SECURE and Schrager, Klemens & Kruegar's ACF2.

Quarendon, Simon. "Data Encryption." The Accountant, 185, No. 5551 (July 16, 1981), 76-78.

Data encryption can be very effective in protecting data from unauthorized users. The author defines encryption and explores three methods of encryption currently available: Electronic Code Book (ECB), Cipher Feedback Mode (CFM), and Cipher Block Chain (CBC). Major applications of this technology are then discussed.

Sachs, Randi T. "What's New in Encryption?" Administrative Management, 43, No. 2 (February 1982), 36-39, 91.

Data encryption is a necessary form of data security if an organization is transmitting information that can be used by others to do it harm. The largest user of this method is the Defense Department, followed by financial institutions. This article discusses the need for data encryption as well as how these methods work, including a fairly detailed discussion of digital data encryption technology, such as DES. A list of vendors also is included.

St. Clair, Linda. "Security for Small Computer Systems." EDPACS, 11, No. 5 (November 1983), 1-10.

Small computer systems have substantially different security requirements than mainframe systems. The small system itself and the environment in which it operates make for distinct assets and liabilities from a security perspective. The author contends that personnel training and supervision are the keys to security, as the information stored in the small computer system is of little value to outsiders. Security software, passwords, and disaster planning and recovery are also discussed.

Schwartz, Michael B. "Safeguarding EFTs." Datamation, 29, No. 2 (February 1983), 148-160.

Electronic Funds Transfers (EFTs), if unguarded, are particularly vulnerable to fraud. In technical language, this article discusses the vulnerability of EFTs and how the use of FIMAS, a recent message authentification standard, can protect EFTs through data encryption.

Schweitzer, James A. "Computer Security: Make Your Passwords More Effective." EDPACS, 10, No. 8 (February 1983), 6-11.

Many breaches of computer security could have been avoided with adequate password protection. Passwords are often constructed too simply, are not kept secret, and often are not changed on a regular basis. In this article the author proposes improvements in password form, use, and administration, and discusses improved access techniques such as "handshaking," encrypted passwords, and "smart cards."

Snyders, Jan. "Security Software Doubles Your Protection." Computer Decisions, 15, No. 9 (September 1983), 46, 50-56.

Security software is an important component of database security. Employing passwords and access codes, such software can limit access to data files and allow management to monitor terminal useage. Some software even provides information about which employees are online at any given time. The author discusses various industries' applications of security software. Includes a buyer's guide.

Srinivasan, Cadambi A. and Paul E. Dascher. "Computer Security and Integrity: Problems and Prospects." Infosystems, 28, No. 5 (Part 1) (May 1981), 116-123.

Management should recognize the need for formal computer security programs, including a computer security charter and a firm policy to include security countermeasures and continuing audits. The authors list a variety of prevention and detection safeguards useful for preventing and detecting violations of the computer.

Vichas, Robert P. "Locking Out Computer Crime." Management World, 11, No. 7 (July 1982), 14-15, 25.

Citing statistics relating to computer crime, the author states that for most companies, the odds are high that theft or abuse will occur, and odds are low that the theft will be discovered. Odds are also low that the thief will be caught, punished, and required to make restitution. Vichas provides a three-part checklist for computer security, including data security, computer equipment, and systems operations elements. The importance of an adequate audit trail also is discussed.

Wallach, Gloria T. "Controls Prevent Computer Negligence and Fraud." Journal of Systems Management, 34, No. 5 (May 1983), 30-32.

A brief, practical introduction to computer security, this article addresses security measures in the I/O Control and Data Entry departments and the Systems and Programming department, as well as physical security of a data processing facility and additional computer operational controls. In her conclusion the author points up the importance of high administrative standards and fair personnel policies. "Management," she writes, "sets the moral climate of a company."

Whalen, John D. "A False Sense of Security." Infosystems, 30, No. 8 (August 1983), 100-103.

No security software automatically protects data; rather, a security software package is just one component of an overall database security system. The author offers two sets of criteria for selecting the proper security software. The technical criteria include compatibility, operational acceptability, ease of implementation, and expandability. The functional criteria include accountability, auditability, integrity, and usability. The author recommends the use of an evaluation team to select the proper software and outlines a series of tests for prospective software packages.