COMPUTER AND DATA SECURITY:
A COMPREHENSIVE ANNOTATED BIBLIOGRAPHY.

John Arthur Scherf

September 1973

This research was supported in part by the Advanced Research Projects Agency of the Department of Defense under ARPA Order No. 2095 which was monitored by ONR under Contract No. N00014-70-A-0362-006, and in part by the Information System Security Project of the M.I.T. Sloan School of Management, and in part by the I.B.M. Data Security Project.

PROJECT MAC

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Cambridge Massachusetts 02139

ACKNOWLEDGEMENTS*

I would like to express my sincere thanks to Professor Stuart E. Madnick of the Sloan School of Management. His guidance, support, and helpful insight provided a valuable contribution to this work.

It is not possible to properly acknowledge the valuable support and encouragement of my wife, Susan, who served as typist, editor, and grammarian. Her assistance made this work more readable and significantly increased its timeliness.

I am greatly indebted to my father, Arthur C. Scherf, who has given me profitable lifelong advice and the needed financial support which made this work possible. I also owe special thanks to Don Hewitt for providing me with computer programming support.

This report was composed and edited using MIT's IBM System/370 Model 165 time-sharing computing system, with the aid of the NSCRIPT manuscript processing system.

*The work reported herein was supported in part by the Information System Security Project of the M.I.T. Sloan School of Management, in part by the I.B.M. Data Security Project, and in part by Project MAC, an M.I.T. research program sponsored by the Advanced Research Projects Agency of the Department of Defense.

COMPUTER AND DATA SECURITY:
A COMPREHENSIVE ANNOTATED BIBLIOGRAPHY.*

ABSTRACT

Articles discussing computer and data security topics are scattered over a very large number of sources which publish articles on security on an irregular basis. This makes it quite difficult for the security consultant, the internal auditor, the computer user, the data processing manager, the business executive, or anyone else to find out what has actually been done in this field without doing extensive, time-consuming, literature research. To ease this problem there currently exist approximately seven computer security bibliographies containing from 50 to 250 entries. Although they are all less than three years old, only one has annotations over a few sentences in length, and only two use any sort of classification or index scheme. The one bibliography with paragraph length annotations is primarily concerned with very technical aspects of hardware and software access control. Most of the other bibliographies are also concerned with only certain subsets of security problems. This paper is apparently the first attempt to produce a bibliography covering all aspects of computer and data security, and having annotations that more than superficially describe each article's content.

This bibliography contains 1,022 entries. About half these entries are extensively annotated, another quarter being superficially annotated, and the rest being unannotated. All extensively annotated entries are rated as to their current usefulness and uniqueness. A subject index of 160 items is provided for referencing purposes. The introduction to this bibliography briefly discusses: privacy, security, and integrity; threats of data misuse; physical, procedural, and hardware/software security; development and scope of the bibliography; the subject index; outstanding articles and books; computer security firms; and the future. A list of 34 firms selling computer security services or equipment is presented following the bibliography.

*This report reproduces a thesis of the same title submitted to the Alfred P. Sloan School of Management, Massachusetts Institute of Technology, in partial fulfillment of the requirements for the degree of Master of Science, September 1973.

TABLE OF CONTENTS

I. INTRODUCTION

Before discussing the development and content of this bibliography, a brief introduction will be given on "computer and data security" for the benefit of those unfamiliar with the subject. Two other excellent introductions to computer security can be found in Browne (bibliography reference number 1370) and Hoffman (4560). These introductions are quite different from the following discussion and can serve as excellent complementary readings.

PRIVACY, SECURITY, AND INTEGRITY.

It is quite important that one be fully aware of the difference in the meanings of the words privacy, security, and integrity. One of the better definitions of privacy is given by Alan F. Westin in his classic book entitled PRIVACY AND FREEDOM (9940).

> "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others... The individual's desire for privacy is never absolute, since participation in society is an equally powerful desire. Thus each individual is continually engaged in a personal adjustment process... in the face of pressures from the curiosity of others and from the process of surveillance that every society sets in order to enforce social norms."

The privacy question largely involves ethical and moral questions of how much and under what circumstances information may legitimately be stored on an individual.

The introduction to Annette Harrison's bibliography (4280) is an excellent summary of many current "privacy protection" problems.

IBM (2220) defines data security as "the protection of data from accidental or intentional disclosure to unauthorized persons and from unauthorized modification." This definition is applicable whether or not computers are used to process the data. Although data security considerations need not always be concerned with computers, computer security considerations are always concerned with data. For without data the computer is a useless tool. Almost all commonly used definitions of computer security incorporate some form of data security definition. The following computer security definition was constructed from several other popular definitions.

> Computer (and data) security is a problem of comprehensive control involving physical, procedural, and hardware/software protective measures which are used to insure that data privacy decisions are enforced, and to protect against accidental or intentional destruction of the computer and its data.

Good integrity means that the computer hardware and operating system are performing according to design objectives; that data files contain accurate and complete data; that personnel are honest and obey security procedures; and that computer programs perform legitimately and without error. Integrity is primarily concerned with fraud and error problems while security is primarily concerned with the protection of privacy decisions. Because integrity and security considerations are frequently identical, almost all authors include integrity considerations in their use of the word "security". This bibliography attempts to provide a comprehensive list of articles on security (and integrity). However, only the most recent and useful articles and books on privacy are included.

THREATS OF DATA MISUSE.

Seven bad things can happen to data. It can be: accidentally disclosed to unauthorized persons; intentionally disclosed to unauthorized persons; accidentally and unknowingly modified; intentionally and secretly modified; accidentally destroyed; intentionally and illegitimately destroyed; and temporarily denied access by its rightful users. Data safeguards should exist if the data is valuable. However, these safeguards are unlikely to exist if the disclosure, modification, or destruction of the data is not harmful to the data caretaker. Intentional data threats will exist if the data is valuable, either in terms of physical or mental well-being, to the person who discloses, destroys, or alters it. Data threats can also be viewed as being either internal or external to the computer system. One way of distinguishing between internal and external threats is to classify all threats as internal if and only if they could realistically be controlled by the computer hardware or operating system. Some computer manufacturers are now devoting a considerable amount of money to designing computers less susceptible to internal threats. External threats require procedural and physical safeguards and are largely the responsibility of the computer user.

There are several important differences between data stored in magnetic form within a computer or on removable files, and data stored in manila envelopes. The most important of these differences is that no physical access is required to destroy, secretly modify, or steal the computerized data. Modifications to the computerized data will produce no detectable erasures. Extremely large amounts of computerized data can be destroyed, modified, or stolen in a very small amount of time. Obtaining evidence for legal prosecution of those who misuse computerized data is often more difficult unless special safeguards are implemented. For these reasons one would think that most organizations would protect their computerized data with as much or greater effort than they used to protect that same data in pre-computer days. Unfortunately, this is not often the case.

There are several other reasons why computerized information is rapidly requiring more and better methods of protection. All types of organizations are becoming increasingly dependent on computer data processing for their continued operations. Not only are more organizations using computers for financial accounting, but computers are being increasingly relied upon for inventory control, sales forecasting, order entry, etc.. There has been a significant increase in the use of remote-access, time-shared computers which are vulnerable to a whole range of new threats. In addition, a larger segment of the population has become familiar with computer technology and the ways in which it may be used for criminal means.

PHYSICAL, PROCEDURAL, AND HARDWARE/SOFTWARE SECURITY.

To get a better idea of the differences among these three methods of providing security, quickly scan the items within the "specific safeguard" section of the subject index. Although this classification of 54 specific safeguards may be somewhat arbitrary, it should quickly become apparent that adequate computer and data security cannot be obtained if any one of these three methods of providing security is ignored. Physical security is required for preventing common types of sabotage; procedural security is needed to detect and prevent most clever types of data input and program fraud, and for providing adequate backup; and hardware/software security is essential in time-shared computers for preventing unauthorized access to sensitive computer-stored data. For local-access batch-processing computer systems very good procedural and physical safeguards can solve most security problems. Basic operating system safeguards for errorless computer operation and a secure log of console commands are nearly adequate hardware/software protective measures. However for remote-access, time-shared computers, sophisticated hardware/software privacy safeguards are crucial.

DEVELOPMENT AND SCOPE OF THE BIBLIOGRAPHY.

Most of the entries in this bibliography were found by conducting an extensive literature search at the Harvard and MIT business libraries and at the MIT engineering library. Reference sources such as THE BUSINESS PERIODICALS INDEX, FUNK AND SCOTT INDEX OF CORPORATIONS AND INDUSTRIES, READER'S GUIDE TO PERIODICAL LITERATURE, IEEE TRANSACTIONS ON COMPUTERS, COMPUTER AND CONTROL ABSTRACTS, DATA PROCESSING DIGEST, ACM COMPUTING REVIEWS, and COMPUTER ABSTRACTS were used. Bibliographies at the end of some articles led to additional entries being found. COMPUTERWORLD newspaper (2170) was responsible for a very large number of security articles.

While performing this literature search the following computer security bibliographies were found: 0770, 1370, 2080, 5530, 7630, 9400, and 9920. This bibliography contains most, but not all, of the entries in these other bibliographies. One reason for this is that most of these bibliographies were found near the end of the literature search and the addition of a few more entries was not considered important. Another reason for not using these bibliographies as sources was the possible violation of copyright laws. Three of these bibliographies (0770, 5530, 7630) still have a value not made obsolete by this bibliography.

Articles dealing solely with personal privacy issues are not included in this bibliography. Articles dealing with both privacy and security issues, or having major computer security implications, are included. An exception was made to include a few classic articles and books on privacy. Those who are primarily interested in privacy issues should consult the following bibliographies: 0310, 4270, 4280, 4560, and 9600.

Time did not permit careful reading of all entries in this bibliography. Approximately half of the entries were carefully read and annotated. Another quarter were briefly scanned and annotated, or annotated from another author's extensive comments. Only the carefully read entries were rated as to their current usefulness and uniqueness.

EXPLANATION OF THE SUBJECT INDEX.

The subject index was first developed after this author had read approximately 50 different articles on computer and data security. As additional entries were read the index was modified by adding to and subtracting from various parts of it. Whenever significant changes were made, an attempt was made to go back and reindex the relevant previously read entries. However, it is possible that the initially read entries, near the beginning of this bibliography, are not as well indexed as the more recently read entries.

This bibliography is stored in a computer to make later updating relatively easy. The primary purpose of the subject index is to make possible computer searching of entries by their subject content. Although manual use of the subject index is somewhat cumbersome, the index's value was considered sufficient to justify its being left in this hard copy publication.

To keep the subject index from becoming too large and unmanageable, the classification of computer security subjects was done at a fairly low level of detail. An attempt was made to offer two levels of detail by using "general" and "specific" categories for the threats and safeguards. All articles were indexed by at least one of the general threat or general safeguard indices. Additional subject indices for specific safeguards, specific threats, computer environment, and miscellaneous subjects were used only if the article had more than superficially discussed that specific subject. Determining when the discussion on a particular subject was no longer superficial and worthy of being indexed requires a somewhat arbitrary decision to be made. Therefore, one should not put too much faith in the accuracy and uniformity of the entries' indices.

The specific safeguard indices can be used as a high level checklist of currently available safeguards. All the safeguards discussed in over 400 articles easily fit into this safeguard classification scheme. However, the grouping of these 54 specific safeguard indices into the three general areas of physical, procudural, and hardware/software safeguards was somewhat arbitrary because several of these indices can easily fit into more than one general area. For more detailed checklists on physical and procedural safeguards see Krauss (5490) or Van Tassel (9400). A comprehensive checklist for hardware and software safeguards apparently does not yet exist.

The specific threat indices in the subject index are useful for referencing bibliography entries but serve rather poorly as a checklist of threats. Most currently available threat checklists are really checklists on methods of security system penetration. It is important to distinguish between "threats" such as programmer fraud and stealing proprietary software, which are the potential and actual actions of people, and "methods of penetration" such as software trapdoors, wiretapping, and password discovery. Although a complete list of methods of penetration would be quite useful as a security checklist, it would be far too lengthy to be useful as a subject index for this bibliography. For this reason only a general high level classification of specific threats was used for indexing purposes.

The list of computer and data environment indices covers four different dimensions: type of information, use of information, type of computer system, and user environment. These dimensions were selected because they were found to have considerable value in referencing the entries. However, they were selected somewhat arbitrarily, and it is possible that other dimensions could have been used with equal success. The miscellaneous indices were used because several useful security subjects could not be fit into a framework which only included specific safeguards, specific threats, and computer environment classifications.

The rating of all carefully read entries as to their current usefulness and uniqueness is not an absolute indicator of their value. All the entries may be valuable to the novice, but only a few may interest the expert security consultant. The ratings only attempt to separate the generally useful entries from the less generally useful ones within a particular computer security subject. The more advanced, more unique, and more detailed articles were generally given higher ratings. It should also be noted that these ratings were determined solely by this author. Their accuracy and uniformity are subject to error.

OUTSTANDING ARTICLES AND BOOKS.

Approximately 70 of the 600 rated entries were rated as "good" and another 40 rated as "excellent". The following paragraph lists thirty different security subjects, with each subject being followed by one or more numbers that indicate which of these 110 "good" or "excellent" articles are primarily concerned with that subject. This will enable easy location of a few good articles on the thirty different subjects without having to use the more cumbersome subject index. However, the following paragraph is not nearly as accurate or as comprehensive as the subject index.

General discussions of threats and/or safeguards (1370, 4280, 5540, 9400, 0170, 0660, 0670, 0950, 2220, 4560, 5160, 5980, 6480); actual examples of computer crimes and disasters (5400, 5900, 8570, 9080, 9100); computer fraud (0160, 1600); programmer operating system penetration (0300); employee threats (5640); physical security (4350, 5490); data structure safeguards (1680); hardware/software access control (0770, 2230, 3950, 6550, 6560, 7020, 7100, 0850, 1030, 1710, 2240, 2430, 3550, 6010, 6110, 6810, 7050, 9120, 9580, 9840); operating system integrity (0330, 0920, 1030); cryptography (1720, 3790, 5320, 6390, 8550, 8850, 9260); existing equipment and system descriptions (7020, 0850, 1710, 2240, 9840); insuring statistical confidentiality (4230, 4590); management responsibilities (4740); assigning security responsibilities (3530, 0650);

auditing control (1980, 5530, 0650, 2610, 6590, 8690, 9190); independent internal control group (8690, 9400); operations control (7840); backup (2090); emergency, contingency and recovery plans (2090, 1080); insurance (1220); computer room environment control (6830); equipment vulnerability to radiation and magnets (0670, 6130, 9200); wiretapping (5450); voting systems (3160, 8300, 8570); security cost effectiveness (8410, 9280, 9850); implementing a security program (1360, 8770, 8970); system certification (1070, 9850); obtaining services from security consulting companies (2010, 5250, 6150); checklists (1070, 5490, 5530, 9400); security frameworks (9280); legal matters (0550, 3850, 3520, 3540); government regulation (8180, 9560, 9940, 9950, 5960, 8790); privacy issues (1690, 4270, 4280, 7490, 9560, 9940, 1250, 1710, 1890, 4520, 6400, 8790); and computer security research surveys (1690, 7490, 8410, 9950, 1250, 6030, 8300).

COMPUTER SECURITY FIRMS.

Following the annotated bibliography is a list of 34 companies selling computer security services and/or equipment. The list is probably not very comprehensive, but no references to other security firms could be found. Harold Witzer (9920) included with his annotated bibliography a list of 66 companies that sell locks, surveillance systems, alarms, and guard services. However, none of those 66 companies appear to have any expertise in dealing with computer related security problems.

The brief comments on these 34 listed companies were obtained from the same source used to locate the company name and address. No direct company contacts were made to obtain additional information. Before choosing one of these 34 firms to perform a security survey, it is recommended that articles by Mandell (6150) and Johnson (5250) be read. Mandell warns of hiring security consultants that also sell security equipment. Some have been known to greatly exaggerate threats in order to sell their equipment.

THE FUTURE.

Considerable research work still needs to be done before all major problems related to computer and data security are solved. However, many organizations could greatly lessen their existing vulnerability to security threats if they just used some of the many currently available cost-effective safeguards. Now that the recent wave of bombing scares has subsided, perhaps many organizations will take a more rational, less physical security oriented approach to security, and devote more attention to threats of unauthorized information disclosure, errors, and fraud. Employees are rapidly becoming the biggest security problem (see entry 5640).

Most of the security problems surrounding physical safeguards have already been delineated and several large physical safeguard checklists currently exist (see Krauss 5490). Although numerous procedural safeguards exist, research still needs to be done to develop coherent methods of integrating different subsets of these procedural safeguards into cost-effective security programs. The Canadian Institute of Chartered Accountants (1980) is taking a major step in this direction. Kuong (5530), Krauss (5490), and Van Tassel (9400) have developed extensive checklists of procedural safeguards, but their methods of implementing these safeguards appear to be somewhat arbitrary.

Researchers are just beginning to develop good frameworks for considering hardware/software safeguard trade-offs. Graham (3950) has developed an excellent framework for comparing and evaluating different access-control systems. AFIPS (1070) has started a comprehensive program with a long-range goal of developing computer system certification procedures. Manuals with checklists and procedures to follow will cover topics such as operational audits, performance reviews, acceptance tests, system reliability, and data collection. If AFIPS succeeds in its goal of system certification, it will have solved one of the major remaining problems of computer and data security. Until just recently, computer equipment manufacturers have been accustomed to designing only very minimal hardware/software safeguards into their equipment. However their attitudes are rapidly changing. IBM plans to spend $40,000,000 over the next five years to develop hardware and software means of controlling access to sensitive computerized data. It appears that very secure and economical hardware/software access control systems will become a reality in the near future. The major problem lies not in developing a secure access control system, but in developing an economically acceptable one.

Another major remaining problem to be solved in the near future is the development of a coherent method for integrating not only procedural safeguards but also physical and hardware/software safeguards into a cost-effective security program. In order to develop security programs with significantly improved performance and lower cost, it will be necessary to quantify, measure, and establish numerical values for various types of threats and safeguards. Collection and analysis of relevant statistics on threats and the affect of safeguards on these threats will be a necessary first step.

In the area of legal controls much has been proposed but Congress has taken little action. Two important books by Alan F. Westin (9940, 9950) have done much to put the privacy problem into proper focus. Just recently a federal government advisory committee has recommended a new code for fair information practice, backed up by strong laws (8180).

Perhaps "Watergate" will provide the necessary catalyst for Congress to pass these needed laws on personal information privacy, Even though attainment of 100% secure systems appears unlikely, the future looks very bright for new improvements in computer and data security measures.

II. SUBJECT INDEX TO THE ANNOTATED BIBLIOGRAPHY

A. PUBLICATION FACTS.

- aa Book.
- ab Magazine or journal article.
- ac Newspaper article.
- ad Report or paper (university, business or government).
- ae Presentation at a workshop, conference, symposium, or meeting.
- af Unpublished or miscellaneous material (such as sales brochures, bulletins, reference indexes, etc.).
- ag AFIPS Conference Proceedings.
- ah Communications of the ACM.
- ai Computerworld.
- aj RAND Corporation reports.
- ak IBM publications.
- al MIT publications.

B. ACTUAL EXAMPLES OF COMPUTER SECURITY CRIMES AND DISASTERS.

- ba Theft.
- bb Fraud.
- bc Destruction.
- bd Hardware and software error.
- be Human error.
- bf Degradation of service.
- bg Theft, fraud, destruction, and errors.

C. GENERAL SAFEGUARD CATEGORIES.

- ca Computer hardware and software safeguards (research literature).
- cb Computer hardware and software safeguards (practical literature).
- cc Management control and operating procedure safeguards.
- cd Physical and architectural safeguards.

D. GENERAL THREAT CATEGORIES.

- da Theft (Disclosure of sensitive or valuable data to those without ligitimate, authorized needs-to-know).
- db Fraud (Secret alteration of valuable data or performing illegal acts where data alteration isn't needed).
- dc Destruction (Partial or complete destruction of data and/or equipment by intent or accident).
- dd Hardware & software error (includes programmer errors).
- de Human error.
- df Degradation of service.
- dg Theft, fraud, destruction, and errors.

E. SPECIFIC SAFEGUARDS.

Computer hardware and software safeguards.

ea Identification and authentication of remote users.

eb Data structure and data management techniques.

ec Hardware access control (practical solutions).

ed Software access control (practical solutions).

ee Access control (theoretical-experimental solutions).

ef Access control below file level.

eg Residue control.

eh File integrity (programs and data).

ei Operating/security system integrity and protection.

ej Processing restrictions.

ek Computer audit programs.

el System monitoring and logging of significant events.

em Checkpoint/restart procedures.

en Exception handling.

eo Hardware & operating system error controls (diagnostic routines, parity checks, graceful degradation, etc.).

ep Data transmission security.

eq Cryptography, data scrambling, and data compression.

er Desensitizing information by introducing errors, data separation, etc..

es Insuring statistical confidentiality.

Procedural Safeguards.

fa Organization of the firm and EDP related groups.

fb Management responsibilities.

fc Assigning security responsibilities.

fd Information classification and/or value determination.

fe Authorization of individuals to access specific data.

ff Auditing.

fg Independent internal control group.

fh Acquisition and validation of input information.

fi Validation of programs.

fj Program and data updating procedures.

fk Retention of information (obsolescence).

fl Control of sensitive printouts through destruction.

fm Operations control.

fn Schedules for all production jobs.

fo Documentation standards and procedures.

fp Library control of tapes, cards, disks; and good housekeeping procedures.

fq Separation and rotation of duties.

fr Personnel advancement opportunities and grievance procedures.

fs Personnel policy on security-related behavior (establishing, enforcing, and discipling).

ft Personnel integrity investigations.

fu Personnel security education and training.

fv Backup (files, documentation, personnel, and sites).

fw Emergency, contingency, and disaster recovery plans.

fx Aperiodic testing and updating of security system.

fy Insurance.

fz Legal contracts.

f1 Trade secrets and copyrights.

Physical and architectural safeguards.
ga Computer room architecture.
gb Computer room environment control.
gc Equipment & storage media durability or reliability; & accessory protective devices (plastic covers, safes).
gd Backup power supplies.
ge Fire alarms and extinguishers.
gf Physical access controls (alarms, guards, locks, etc.).
gg General discussion of safeguards.
gh Existing system and equipment descriptions.

H. SPECIFIC THREATS.

Threats internal to computer system.
ha General discussion of internal data access threats.
hb Espionage.
hc Copying & selling proprietary software or databases.
hd Illegally reading private information of others.
he Combining authorized data to produce unauthorized information.
hf Accidental disclosure of restricted information.
hg Malicious destruction of others' data.
hi Accidential destruction of others' or one's own data.
hj Embezzlement.
hk Data input fraud.
hl Operator fraud.
hm Programmer fraud.
hn Program user fraud.
ho Fraudulently altering others' data to lessen one's non-financial liabilities.
hp Data input errors.
hq Operator errors.
hr Programmer errors.
hs Program user errors.
ht Operating system error.
hu Hardware errors.
hv Hardware or software implementation delays.
hw Negligence.

Human threat.
ia Operator.
ib User of "canned" programs.
ic High-level language programmer.
id Assembly language programmer.
ie Maintenance personnel.
if Manager.
ig Authorized file user.
ih Authorized computer system user.
ii Unauthorized computer system user.

Threats external to computer system.

ja General discussion of external threats.

jb Labor strikes.

jc Physical theft of tapes, cards, etc.,

jd Radiation.

je Wiretapping.

jf Bombs, magnets, and other means of sabotage.

jg Fire, water, dust, static electricity, earthquake, tornato, etc..

jh Air conditioning, and power failures.

K. COMPUTER AND DATA ENVIRONMENT.

Type of Information.

ka Personal information stored on others.

kb One's private information stored exclusively for one's own use.

kc Information stored for renting and royalty.

Use of information.

kd Accounting and financial.

ke Manufacturing.

kf Marketing and sales (mailing lists).

kg Research and development.

Type of computer system.

la Batch processing (multiprogramming).

lb Time sharing (multiprogramming, remote real-time-interactive access).

User environment.

ma EDP Service bureaus (facilities management, "canned" program services, or selling only computer time).

mb Organizations owning and selling access rights to large "personal information" databanks.

mc Banks, credit agencies, insurance companies, and other financial institutions.

md Federal government.

me Local government.

mf Legal and law enforcement.

mg Medical.

mh Military.

mi Transportation.

mj Educational.

mk Voting systems.

N. MISCELLANEOUS.

na Recovery from computer errors, crimes, and disasters.

nb Security expense versus requirements, and security cost effectiveness.

nc Reliability, flexibility, efficiency, and non-monetary costs of security.

nd Obtaining services from security consulting companies.
ne Computer security apathy.
nf Implementing a security program.
ng Areas currently being researched, or needing future research.
nh Security frameworks.
ni Security checklists.
nj Private legal matters, and management's legal responsibilities.
nk Manufacturers' responsibility in providing safeguards.
nl Government regulation.
nm Privacy issues.
nn General survey articles.
no Computer security research surveys.
np Other bibliographies and references.
nq Classified articles.

X. ESTIMATE OF ARTICLE'S CURRENT USEFULNESS & UNIQUENESS.
x1 Poor.
x2 Fair.
x3 Good.
x4 Excellent.

III. CLASSIFICATION OF BIBLIOGRAPHY ENTRIES BY SUBJECT

A. PUBLICATION FACTS.

```
****
*aa* Book.
****
*0300*0390*0420*0990*1010*1340*1350*1980*2210*2610*3040*3170
*3450*3510*3610*3760*3990*4170*4350*4360*4370*4380*4420*5060
*5070*5180*5190*5320*5480*5490*5530*5540*6210*6240*6360*6480
*6580*7000*7420*7450*7710*7960*8530*9400*9600*9850*9855
```

```
****
*ab* Magazine or journal article.
****
*0020*0050*0060*0070*0080*0150*0160*0170*0180*0190*0220*0250
*0260*0270*0310*0340*0350*0370*0380*0400*0410*0430*0480*0500
*0520*0530*0540*0550*0640*0650*0660*0670*0700*0720*0730*0790
*0800*0820*0830*0840*0860*0880*0890*0940*0960*0970*0980*1000
*1020*1030*1040*1050*1310*1320*1330*1360*1400*1410*1420*1450
*1530*1550*1570*1590*1600*1660*1670*1680*1710*1740*1750*1780
*1790*1800*1820*1830*1860*1870*1880*1900*1930*1940*1990*2000
*2010*2030*2040*2050*2070*2090*2100*2110*2120*2130*2140*2160
*2200*2230*2260*2300*2340*2350*2360*2380*2390*2410*2420*2450
*2460*2510*2520*2560*2590*2600*2660*2670*2680*2700*2720*2730
*2740*2750*2760*2810*2820*2830*2840*2850*2900*2920*2940*2990
*3020*3100*3140*3160*3200*3260*3280*3290*3320*3330*3340*3360
*3400*3420*3430*3440*3460*3490*3530*3540*3570*3590*3600*3620
*3630*3660*3670*3710*3720*3730*3740*3780*3790*3840*3850*3880
*3890*3910*3920*3930*3960*3970*3980*4030*4040*4060*4090*4100
*4120*4130*4150*4160*4250*4260*4290*4300*4310*4330*4340*4390
*4410*4430*4440*4450*4460*4470*4480*4500*4520*4530*4540*4560
*4590*4600*4630*4650*4660*4670*4680*4690*4710*4720*4730*4750
*4760*4790*4800*4870*4880*4950*4960*4970*4990*5010*5030*5040
*5050*5110*5150*5160*5200*5210*5220*5230*5240*5270*5280*5300
*5330*5360*5390*5400*5410*5420*5430*5440*5450*5470*5510*5520
*5550*5610*5630*5650*5660*5740*5750*5760*5770*5800*5810*5820
*5830*5860*5870*5880*5890*5900*5910*6070*6080*6090*6100*6160
*6200*6230*6250*6270*6290*6340*6370*6380*6400*6410*6450*6460
*6470*6510*6520*6570*6590*6600*6610*6630*6640*6760*6770*6790
*6820*6830*6840*6850*6860*6870*6880*6890*6900*6910*6920*6970
*7010*7070*7130*7140*7180*7190*7220*7250*7260*7300*7310*7350
*7360*7370*7380*7400*7430*7440*7460*7510*7520*7530*7540*7550
*7560*7600*7610*7620*7640*7660*7680*7690*7700*7760*7770*7790
*7810*7820*7830*7840*7850*7880*7890*7910*7920*7950*7970*7980
*7990*8000*8010*8070*8090*8100*8110*8120*8130*8150*8170*8200
*8210*8240*8250*8270*8280*8290*8330*8340*8350*8370*8400*8420
*8470*8480*8490*8500*8560*8650*8690*8700*8710*8740*8750*8760
*8770*8800*8810*8820*8830*8870*8880*8890*8910*8970*8990*9000
*9060*9070*9130*9150*9160*9170*9180*9190*9200*9210*9300*9320
```

```
*9330*9380*9410*9430*9440*9450*9460*9470*9480*9500*9530*9620
*9630*9640*9650*9660*9670*9680*9690*9700*9710*9760*9765*9770
*9775*9785*9790*9795*9805*9810*9815*9820*9825*9830*9835*9845
*9860*9870*9875*9880*9885*9890*9895*9900*9905*9910*9925*9930
*9935*9950*9955*9960*9965*9970*9980*9985*9990

****
*ac* Newspaper article.
****
*0030*0090*0110*0120*0140*0210*0230*0320*0330*0460*0470*0610
*0680*0710*0760*0810*0870*0910*1070*1080*1090*1100*1110*1120
*1130*1140*1150*1160*1170*1180*1190*1200*1210*1220*1230*1240
*1250*1260*1270*1280*1290*1300*1440*1490*1500*1520*1540*1560
*1580*1610*1620*1630*1640*1650*1810*1960*1970*2020*2060*2150
*2170*2180*2190*2250*2290*2310*2400*2440*2530*2550*2620*2650
*2710*2770*2780*2870*2880*2890*2910*2950*3050*3110*3130*3180
*3190*3220*3230*3370*3410*3470*3480*3770*4140*4180*4190*4200
*4210*4220*4320*4550*4810*4820*4830*4840*4850*4890*4900*4940
*4980*5090*5100*5120*5170*5250*5290*5310*5370*5460*5640*5670
*5680*5690*5700*5710*5720*5730*5790*5840*5930*5940*5950*5960
*5970*5980*5990*6000*6010*6020*6030*6040*6050*6130*6150*6180
*6190*6260*6280*6330*6420*6430*6620*6650*6660*6670*6680*6690
*6700*6710*6720*6730*6750*6930*6940*6960*6990*7060*7080*7120
*7160*7330*7340*7390*7410*7470*7480*7500*7650*7730*7860*7870
*7900*8040*8050*8140*8180*8300*8320*8430*8460*8510*8570*8580
*8590*8600*8610*8620*8630*8640*8720*8730*8780*8790*8860*8940
*8950*8980*9040*9080*9090*9100*9110*9120*9290*9310*9350*9360
*9490*9510*9540*9550*9610*9740*9750*9915*9940*9945*9975

****
*ad* Report or paper (university, business or government).
****
*0100*0130*0290*0360*0490*0560*0570*0580*0590*0600*0620*0750
*0770*0780*0850*0930*1060*1460*1470*1730*1760*1910*2080*2330
*2370*2490*2540*2640*2690*2960*2970*3010*3030*3070*3080*3090
*3120*3150*3210*3240*3300*3310*3350*3390*3500*3550*3640*3690
*3750*3800*3860*3940*4020*4050*4070*4110*4270*4280*4400*4490
*4510*4570*4640*4700*4780*4860*4910*4920*4930*5000*5020*5340
*5350*5500*5580*5600*5780*6170*6220*6300*6320*6350*6500*6540
*6550*6560*6780*6950*7020*7030*7040*7050*7100*7110*7170*7200
*7240*7290*7490*7580*7590*7670*7750*8060*8080*8190*8220*8260
*8270*8310*8380*8410*8440*8450*8520*8660*8670*8900*8920*8960
*9020*9030*9050*9140*9230*9240*9250*9270*9280*9370*9560*9570
*9580*9590*9720*9730*9800*9805*9845*9920

****
*ae* Presentation at a workshop, conference, symposium, or
****   meeting.
*0010*0040*0200*0280*0440*0450*0510*0630*0690*0740*0900*0920
*0950*1380*1390*1430*1510*1680*1690*1700*1720*1770*1850*1890
*1920*2240*2270*2280*2320*2430*2470*2480*2500*2630*2790*2930
*3000*3060*3270*3380*3520*3650*3680*3700*3810*3820*3830*3870
```

```
*3900*3950*4000*4010*4230*4240*4580*4610*4620*4770*5130*5140
*5260*5380*5560*5570*5590*5620*5850*5920*6060*6110*6140*6310
*6390*6440*6490*6530*6550*6740*6800*6810*6980*7090*7150*7210
*7230*7270*7280*7290*7320*7780*7930*7940*8020*8030*8160*8200
*8220*8230*8550*8680*8850*8930*9010*9220*9260*9280*9390*9420
*9520*9570*9580*9780*9800*9840*9865

****
*af* Unpublished or miscellaneous material (such as sales
****   brochures, bulletins, reference indexes, etc.).
*0240*1370*1480*1840*1950*2570*2580*2800*2860*2980*3250*3560
*3580*4080*4740*5080*6120*7570*7630*7720*7740*7800*8360*8390
*8540*8840

****
*ag* AFIPS Conference Proceedings.
****
*0440*0450*0570*0630*0920*0950*1690*1700*1720*1890*2240*2280
*2430*2470*3060*3520*3650*3810*3830*3950*4230*4580*5260*5560
*5850*6310*6390*6440*6550*6810*6980*7270*7290*7780*8020*8550
*8850*9260*9280*9390*9420*9520*9570*9580*9800*9840

****
*ah* Communications of the ACM.
****
*0520*0550*0720*2230*2680*2750*3620*3960*4120*4250*4300*4800
*5610*5660*6370*6640*8200*8500*9210*9380*9500

****
*ai* Computerworld.
****
*0030*0110*0120*0140*0210*0230*0320*0330*0460*0470*0760*0810
*0870*0910*1070*1080*1090*1100*1110*1120*1130*1140*1150*1160
*1170*1180*1190*1200*1210*1220*1230*1240*1250*1260*1270*1280
*1290*1300*1440*1500*1520*1560*1610*1620*1630*1640*1650*1810
*1960*1970*2020*2170*2180*2190*2290*2310*2400*2440*2530*2550
*2620*2650*2710*2770*2780*2870*2880*2890*2910*2950*3110*3130
*3180*3190*3220*3410*3470*3480*3770*4180*4190*4200*4210*4220
*4320*4550*4810*4820*4830*4840*4850*4890*5090*5120*5170*5250
*5290*5640*5670*5680*5690*5700*5710*5720*5730*5790*5840*5930
*5940*5950*5960*5970*5980*5990*6000*6010*6020*6030*6040*6050
*6130*6180*6190*6420*6430*6620*6650*6660*6670*6680*6690*6700
*6710*6720*6730*6750*6930*6940*6960*7080*7120*7160*7330*7340
*7390*7410*7470*7500*7650*7730*7860*7900*8040*8050*8140*8300
*8320*8430*8460*8570*8580*8590*8600*8610*8620*8630*8640*8780
*8790*8860*8940*8950*8980*9040*9080*9090*9100*9110*9120*9290
*9310*9350*9360*9490*9510*9540*9550*9610*9740*9750*9915*9940
*9945*9975

****
*aj* RAND Corporation reports.
****
```

*0360*0560*0570*0580*0590*0600*4270*4280*4400*7290*8190*9250
*9270*9280*9560*9570*9580*9590

****
ak IBM publications.
****
*1840*2220*2330*2370*2540*3070*3120*3240*3550*3800*3860*4070
*4910*4920*4930*5500*6950*7020*7030*7040*7050*7170*7890*8350
*8660*8670*8680*9230*9240*9845*9910

****
al MIT publications.
****
*0720*1910*2430*2680*2960*3310*3960*6780*7000*7100*8190*9370

B. ACTUAL EXAMPLES OF COMPUTER SECURITY CRIMES AND DISASTERS

****
ba Theft.
****
*0010*0070*0160*0600*1110*1240*1540*1670*1710*3190*3200*3370
*3720*3730*3740*3840*3890*3930*4040*4190*4210*4670*4830*5090
*5450*5750*5970*6690*6700*6710*6790*6840*6880*7140*7160*7380
*7540*7550*7610*8140*8590*8600*8610*9150*9390*9975

****
bb Fraud.
****
*0010*0070*0080*0090*0140*0150*0160*0320*0910*1040*1100*1150
*1310*1520*1550*1600*1620*1670*2020*2060*2110*2130*2140*2150
*2180*2310*2770*2870*2880*3020*3190*3370*3490*3720*3730*3740
*3770*3780*4660*4810*5010*5160*5290*5310*5400*5720*5750*5930
*6040*6260*6340*6360*6420*6430*6710*6840*6960*6990*7060*7140
*7180*7450*7460*7910*8210*8570*8610*8620*8720*8780*9080*9100
*9160*9390*9550

****
bc Destruction.
****
*0110*0180*0330*0740*0750*0760*0810*1040*1160*1290*1530*1580
*1930*1960*2060*2180*2740*2820*2890*3360*3660*3970*4060*4220
*4360*4690*4820*4840*4900*5580*5670*5730*5830*5900*5940*5990
*6150*6160*6500*6610*6660*6670*6680*6820*6840*6850*6880*7250
*7390*7750*7900*8240*8250*8320*8370*8520*8640*8940*8950*9290
*9310*9350*9410*9490*9770*9915*9945

****
bd Hardware and software error.
****
*0120*0230*1130*1150*1160*1270*1300*1580*3020*3230*3540*3890
*4060*6000*6750*7120*8570*8860*9360*9660*9965

```
****
*be* Human error.
****
*0120*0230*1090*1100*1580*2060*2740*2870*3130*3220*3230*4060
*4860*5150*5650*6790*7120*8460*8720*8860*9360*9540*9660*9940

****
*bf* Degradation of service.
****
*2890*6430*7080*8610*9510*9610*9930

****
*bg* Theft, fraud, destruction, and errors.
****
*0170*0190*0480*0660*0670*1790*2090*2170*3170*3510*4170*4380
*4980*7150*7730*8360*9400*9930
```

C. GENERAL SAFEGUARD CATEGORIES.

```
****
*ca* Computer hardware and software safeguards (research
****   literature).
*0300*0770*0780*1460*1700*1840*2000*2230*2380*2400*2680*2930
*3090*3310*3550*3950*4560*4570*4580*5780*5850*6810*7090*7100
*7780*8190*8470*8930*9240*9250*9370*9720*9730*9800

****
*cb* Computer hardware and software safeguards (practical
****   literature).
*0030*0050*0060*0140*0200*0290*0300*0340*0370*0440*0450*0490
*0510*0520*0530*0570*0580*0600*0610*0630*0640*0650*0660*0670
*0680*0690*0720*0800*0850*0900*0920*0940*0970*1030*1070*1190
*1200*1210*1260*1350*1360*1370*1390*1400*1410*1420*1470*1510
*1550*1670*1680*1690*1710*1720*1770*1790*1850*1860*1880*1890
*1910*1990*2100*2160*2190*2210*2220*2240*2270*2280*2320*2330
*2340*2370*2390*2420*2430*2440*2470*2480*2490*2500*2560*2570
*2580*2590*2620*2630*2640*2660*2670*2690*2750*2780*2790*2800
*2810*2830*2960*3000*3010*3030*3060*3070*3080*3120*3140*3150
*3160*3170*3180*3210*3240*3300*3320*3380*3450*3470*3480*3550
*3560*3590*3610*3620*3650*3670*3680*3690*3700*3710*3760*3790
*3800*3810*3820*3830*3860*3870*3890*3900*3940*3960*4000*4020
*4050*4070*4100*4160*4190*4230*4250*4300*4330*4340*4400*4440
*4490*4510*4530*4540*4550*4590*4620*4640*4730*4740*4770*4780
*4790*4800*4810*4830*4860*4880*4890*4910*4920*4930*4940*5000
*5130*5200*5260*5340*5350*5380*5450*5470*5500*5510*5520*5530
*5540*5560*5570*5590*5600*5610*5620*5680*5690*5700*5710*5730
*5920*5950*5970*5980*6010*6030*6100*6110*6130*6140*6170*6180
*6190*6220*6240*6310*6320*6350*6380*6390*6400*6430*6440*6450
*6520*6530*6540*6550*6560*6570*6620*6640*6690*6720*6740*6780
*6800*6870*6930*6940*6950*6970*6980*7000*7020*7030*7040*7050
*7110*7150*7160*7170*7180*7190*7200*7210*7220*7230*7240*7270
```

```
*7280*7290*7300*7320*7330*7390*7400*7440*7490*7670*7690*7790
*7820*7870*7880*7930*7940*8020*8030*8050*8070*8090*8160*8200
*8260*8270*8280*8290*8300*8310*8340*8380*8390*8410*8420*8440
*8490*8500*8530*8540*8550*8560*8590*8600*8660*8670*8680*8770
*8850*8880*8890*8900*8920*8930*8960*8990*9020*9030*9050*9070
*9080*9100*9120*9130*9140*9150*9170*9200*9210*9220*9230*9250
*9260*9270*9280*9300*9380*9420*9430*9440*9450*9500*9520*9560
*9580*9590*9660*9710*9750*9790*9805*9810*9845*9855*9890*9910
*9970

****
*cc* Management control and operating procedure safeguards.
****
*0010*0020*0040*0050*0090*0100*0130*0160*0170*0180*0190*0200
*0220*0240*0250*0260*0270*0280*0340*0350*0360*0390*0400*0410
*0420*0460*0470*0530*0550*0560*0570*0590*0600*0610*0640*0650
*0660*0670*0680*0700*0710*0740*0750*0760*0770*0780*0790*0800
*0820*0830*0840*0860*0890*0930*0950*0960*0970*0980*0990*1000
*1020*1050*1060*1070*1080*1090*1100*1140*1180*1200*1220*1230
*1250*1260*1280*1320*1330*1340*1350*1360*1370*1380*1400*1410
*1420*1440*1450*1480*1490*1500*1550*1580*1600*1630*1650*1670
*1680*1690*1710*1730*1740*1750*1760*1770*1790*1810*1820*1850
*1870*1890*1900*1920*1930*1950*1970*1980*1990*2020*2030*2070
*2080*2090*2100*2120*2130*2140*2160*2170*2180*2190*2210*2220
*2250*2260*2290*2300*2320*2330*2340*2350*2360*2410*2460*2480
*2490*2500*2510*2520*2540*2550*2560*2590*2600*2610*2620*2630
*2640*2650*2660*2690*2700*2710*2720*2730*2740*2760*2780*2810
*2850*2860*2870*2900*2920*2940*2980*3000*3010*3020*3040*3100
*3130*3140*3160*3170*3200*3220*3230*3250*3260*3270*3280*3290
*3320*3390*3400*3410*3420*3440*3460*3490*3500*3510*3520*3530
*3540*3570*3580*3590*3600*3630*3640*3650*3670*3720*3730*3740
*3750*3760*3770*3780*3820*3850*3880*3910*3920*3930*3970*3980
*3990*4000*4010*4030*4040*4050*4060*4070*4080*4090*4100*4110
*4130*4140*4150*4160*4170*4180*4190*4210*4230*4240*4250*4260
*4290*4310*4330*4360*4370*4380*4390*4400*4410*4430*4440*4450
*4460*4470*4480*4500*4520*4530*4540*4550*4600*4610*4620*4630
*4650*4660*4680*4700*4710*4720*4730*4740*4750*4760*4810*4830
*4860*4870*4900*4960*4980*4990*5010*5020*5040*5050*5060*5070
*5090*5110*5120*5130*5150*5160*5180*5190*5210*5220*5230*5240
*5250*5270*5280*5290*5300*5310*5330*5340*5360*5370*5390*5400
*5410*5420*5430*5440*5460*5480*5490*5530*5540*5550*5630*5640
*5650*5660*5720*5740*5750*5760*5770*5790*5800*5810*5820*5840
*5860*5870*5880*5890*5910*5930*5950*5960*5970*5980*5990*6000
*6030*6040*6050*6060*6070*6080*6090*6150*6160*6200*6210*6230
*6240*6250*6260*6270*6280*6290*6300*6360*6370*6380*6400*6410
*6420*6430*6460*6470*6480*6490*6510*6520*6550*6560*6580*6590
*6600*6610*6620*6630*6650*6700*6710*6730*6750*6760*6770*6790
*6840*6850*6860*6890*6900*6910*6920*6960*6970*7060*7070*7120
*7130*7140*7150*7180*7190*7210*7220*7230*7240*7250*7260*7270
*7290*7310*7320*7350*7370*7400*7420*7430*7450*7460*7470*7480
*7490*7500*7510*7520*7530*7550*7560*7630*7640*7660*7680*7700
*7710*7720*7740*7750*7760*7770*7800*7810*7830*7840*7850*7880
```

```
*7890*7920*7930*7940*7950*7960*7970*7980*7990*8000*8010*8020
*8060*8070*8100*8110*8120*8130*8150*8170*8180*8210*8230*8270
*8280*8300*8310*8320*8350*8360*8390*8410*8430*8440*8460*8480
*8490*8510*8570*8580*8590*8600*8620*8630*8650*8690*8700*8710
*8720*8730*8740*8760*8770*8780*8790*8800*8810*8820*8830*8840
*8860*8870*8880*8890*8900*8910*8940*8970*8980*8990*9010*9040
*9050*9060*9070*9080*9090*9100*9110*9120*9130*9140*9160*9170
*9180*9190*9210*9250*9280*9320*9330*9360*9400*9410*9440*9460
*9470*9480*9530*9560*9580*9590*9610*9620*9630*9640*9650*9660
*9670*9680*9690*9700*9765*9770*9775*9780*9785*9790*9795*9805
*9810*9815*9820*9825*9830*9840*9845*9850*9855*9865*9870*9875
*9880*9885*9895*9910*9920*9925*9930*9950*9955*9960*9980*9985
*9990
```

```
****
*cd* Physical and architectural safeguards.
****
*0100*0130*0170*0180*0190*0500*0530*0540*0610*0620*0660*0670
*0730*0740*0750*0800*0870*0880*0970*1070*1080*1130*1170*1190
*1260*1270*1290*1300*1350*1360*1430*1440*1450*1530*1550*1570
*1590*1640*1670*1730*1780*1790*1830*1920*1930*1960*1970*2030
*2040*2050*2070*2080*2100*2120*2170*2180*2190*2210*2250*2320
*2330*2350*2360*2490*2600*2610*2620*2690*2740*2760*2840*2890
*2970*2990*3140*3170*3180*3310*3330*3340*3350*3360*3400*3420
*3450*3660*3720*3730*3740*3760*3970*4040*4060*4070*4170*4350
*4360*4380*4410*4420*4460*4470*4540*4600*4690*4700*4710*4730
*4740*4760*4820*4840*4850*4950*4980*5030*5080*5100*5130*5140
*5150*5170*5220*5230*5250*5490*5530*5540*5670*5730*5750*5830
*5840*5900*5940*5980*6020*6030*6070*6090*6120*6140*6150*6160
*6330*6400*6520*6580*6600*6620*6660*6670*6680*6820*6830*6880
*6970*7010*7080*7100*7150*7160*7210*7220*7230*7240*7250*7260
*7320*7340*7350*7360*7370*7410*7570*7580*7590*7600*7620*7630
*7650*7660*7750*7760*7840*7850*7860*7910*8060*8220*8230*8240
*8250*8270*8320*8330*8360*8370*8390*8400*8410*8420*8430*8450
*8520*8590*8600*8640*8750*8760*8770*8880*8940*8950*9000*9170
*9290*9310*9350*9400*9490*9510*9590*9700*9740*9760*9770*9780
*9790*9810*9835*9855*9860*9900*9905*9915*9920*9930*9935*9945
*9960*9990
```

D. GENERAL THREAT CATEGORIES.

```
****
*da* Theft (Disclosure of sensitive or valuable data to
****   those without ligitimate, authorized needs-to-know).
*0030*0130*0160*0270*0360*0370*0380*0450*0560*0570*0630*0640
*0700*0710*0790*0850*0930*0940*0950*0960*1040*1050*1060*1190
*1240*1250*1380*1470*1490*1540*1560*1570*1620*1640*1660*1670
*1680*1690*1700*1710*1720*1760*1800*1810*1820*1840*1860*1880
*1890*1920*2160*2180*2220*2240*2300*2340*2350*2380*2400*2410
*2460*2550*2570*2580*2590*2630*2690*2730*2830*2850*2900*2910
*2920*2990*3010*3040*3050*3060*3140*3150*3190*3200*3250*3260
```

```
*3370*3400*3410*3420*3440*3450*3470*3560*3610*3630*3640*3650
*3670*3700*3710*3760*3790*3800*3810*3840*3850*3860*3870*3890
*3900*3920*3930*3990*4000*4010*4040*4110*4140*4150*4180*4190
*4210*4240*4370*4400*4420*4430*4440*4450*4460*4470*4480*4520
*4530*4550*4570*4580*4590*4620*4630*4670*4680*4700*4710*4720
*4730*4750*4770*4780*4800*4830*4890*4940*4950*4960*5020*5070
*5090*5190*5230*5250*5330*5340*5350*5370*5380*5450*5460*5500
*5510*5550*5660*5680*5690*5700*5710*5750*5760*5810*5850*5920
*5950*5960*5970*5980*6050*6070*6090*6140*6150*6160*6220*6280
*6350*6370*6380*6390*6440*6450*6480*6490*6500*6510*6530*6570
*6590*6620*6690*6700*6710*6720*6790*6840*6880*6930*6940*6980
*7090*7140*7160*7170*7280*7290*7380*7470*7490*7500*7510*7540
*7550*7560*7570*7610*7620*7640*7760*7780*7910*7920*7960*8110
*8140*8170*8180*8260*8290*8310*8330*8340*8370*8400*8430*8510
*8550*8560*8600*8610*8730*8740*8790*8810*8820*8830*8850*8880
*8890*8900*8960*8980*8990*9150*9170*9210*9240*9260*9270*9280
*9300*9380*9390*9420*9430*9440*9450*9500*9560*9600*9690*9720
*9730*9800*9825*9840*9845*9850*9855*9870*9875*9885*9950*9975

****
*db* Fraud (Secret alteration of valuable data or perform-
****   ing illegal acts where data alteration isn't needed).
*0030*0080*0090*0130*0140*0150*0160*0240*0270*0380*0450*0530
*0640*0650*0910*0920*1040*1150*1190*1310*1380*1520*1600*1620
*1640*1670*1710*1750*1820*1860*1920*1980*2020*2060*2110*2130
*2140*2150*2160*2180*2220*2310*2340*2450*2630*2650*2730*2770
*2870*2880*3020*3050*3160*3190*3220*3370*3400*3450*3490*3670
*3750*3770*3780*3910*3980*3990*4030*4160*4320*4370*4430*4460
*4480*4520*4550*4570*4580*4660*4720*4730*4810*4950*5010*5070
*5190*5260*5290*5310*5350*5380*5400*5660*5680*5720*5740*5750
*5850*5920*5960*5980*6040*6050*6070*6090*6150*6160*6260*6340
*6360*6420*6430*6550*6560*6590*6710*6840*6960*6980*6990*7060
*7140*7170*7180*7290*7450*7460*7560*7640*7910*8170*8210*8280
*8300*8490*8570*8610*8620*8630*8740*8780*8790*8890*8900*9080
*9100*9110*9160*9280*9390*9440*9500*9550*9570*9660*9720*9730
*9750*9800

****
*dc* Destruction (Partial or complete destruction of data
****   and/or equipment by intent or accident).
*0110*0130*0220*0270*0330*0430*0490*0500*0530*0620*0730*0760
*0790*0810*0820*1040*1080*1120*1160*1170*1190*1290*1430*1530
*1570*1580*1630*1640*1650*1670*1730*1780*1830*1920*1930*1960
*2050*2060*2160*2180*2250*2290*2520*2690*2700*2760*2820*2890
*2970*2990*3040*3050*3330*3340*3350*3360*3430*3660*3670*3860
*3970*3990*4060*4130*4220*4360*4370*4420*4460*4490*4500*4570
*4580*4690*4730*4820*4840*4850*4900*4950*4990*5030*5040*5050
*5140*5170*5200*5250*5260*5380*5500*5630*5670*5730*5830*5900
*5920*5940*5980*5990*6020*6060*6070*6090*6120*6130*6150*6160
*6330*6580*6610*6660*6670*6680*6820*6840*6850*6880*6980*7140
*7170*7250*7260*7390*7410*7570*7580*7590*7600*7650*7750*7760
*7900*7910*8040*8050*8060*8080*8220*8240*8250*8320*8370*8400
```

```
*8430*8520*8940*8950*9010*9200*9220*9280*9290*9310*9350*9460
*9490*9500*9720*9730*9750*9760*9770*9780*9835*9900*9915*9935
*9945

****
*dd* Hardware & software error (includes programmer errors).
****
*0040*0120*0230*0630*0820*0840*0870*0880*0920*1120*1150*1160
*1270*1300*1510*1580*1820*1870*1980*2420*2520*2530*2590*2720
*2760*2810*2840*2980*3020*3110*3180*3230*3680*3860*4030*4060
*4120*4310*4490*5030*5200*5260*5570*5810*6000*6120*6550*6560
*6570*6590*6750*6760*6830*6860*7120*7300*7310*7370*7400*7600
*7640*8120*8300*8570*8860*9220*9330*9360*9560*9570*9660*9855
*9860*9880*9905*9965

****
*de* Human error.
****
*0040*0120*0230*0450*0630*0820*0840*0950*1090*1120*1500*1580
*1750*1890*1980*2060*2520*2590*2760*2810*2870*2980*3110*3130
*3220*3230*3680*3980*4030*4060*4440*4450*4860*4890*5200*5330
*5650*5740*5810*6050*6590*6600*6730*6760*6790*6860*7120*7300
*7400*7460*7640*7960*7990*8110*8120*8300*8460*8740*8860*9330
*9360*9540*9560*9660*9855*9880*9940

****
*df* Degradation of service.
****
*1900*2040*2890*3520*3530*3540*5150*5800*5910*6310*6430*6500
*6600*6630*7010*7080*7370*7530*7740*7950*7990*8130*8610*8690
*8750*8970*9000*9180*9510*9610*9740*9820*9830*9860*9930*9980
*9985

****
*dg* Theft, fraud, destruction, and errors.
****
*0050*0170*0180*0190*0300*0340*0390*0420*0550*0660*0670*0970
*0990*1010*1030*1070*1140*1180*1210*1220*1230*1260*1340*1360
*1410*1420*1550*1770*1790*1900*1970*1990*2030*2070*2090*2120
*2190*2210*2440*2560*2600*2620*2740*3170*3480*3510*3520*3530
*3540*3720*3730*3740*3820*3940*3950*3960*4020*4070*4080*4100
*4170*4250*4330*4340*4380*4410*4540*4600*4610*4640*4740*4760
*4880*4910*4920*4930*4980*5000*5060*5120*5150*5160*5180*5210
*5220*5240*5440*5480*5490*5530*5540*5580*5590*5640*5780*5790
*5800*5840*6030*6080*6100*6170*6180*6240*6270*6310*6320*6400
*6410*6520*6630*6740*6810*6970*7000*7110*7130*7150*7210*7220
*7230*7240*7320*7350*7420*7480*7520*7530*7670*7680*7690*7730
*7840*7850*8020*8130*8190*8200*8270*8350*8360*8380*8390*8410
*8580*8590*8690*8700*8720*8770*8840*8970*9040*9050*9070*9120
*9140*9190*9370*9400*9480*9580*9620*9640*9680*9790*9810*9820
*9830*9865*9910*9930*9960*9970*9980*9985*9990
```

E. SPECIFIC SAFEGUARDS.

```
****
*ea* Identification and authentication of remote users.
****
*0300*0670*0900*1460*1670*1690*1710*1720*1860*2220*2320*2560
*2930*3480*3690*4770*4780*4800*5380*5920*6030*7020*7050*7100
*7210*7220*7230*7240*7490*8070*9270*9400*9500*9720*9730*9750
*9800

****
*eb* Data structure and data management techniques.
****
*1680*1700*2430*2790*3210*3860*3870*4640*4790*5260*6500*6980
*8930*9030*9370

****
*ec* Hardware access control (practical solutions).
****
*0290*0300*0670*0720*0850*1030*1510*1720*2560*3070*3690*3960
*4300*4910*4920*4930*5600*5610*6550*6560*7210*7220*7230*7240
*7270*8200*8500*9890

****
*ed* Software access control (practical solutions).
****
*0030*0290*0300*0370*0440*0450*0630*0640*0670*0720*0850*0900
*1030*1210*1510*1690*1710*1720*1880*1910*2180*2220*2230*2240
*2270*2370*2430*2560*3060*3090*3120*3310*3550*3620*3690*3700
*3810*3860*3940*3960*4510*4770*4910*4920*4930*5080*5260*5560
*5580*5600*5610*5620*5680*5710*6030*6110*6170*6310*6540*6740
*6780*6800*7000*7020*7030*7040*7050*7100*7110*7170*7200*7210
*7220*7230*7240*7270*7280*7360*7490*7670*8030*8160*8310*8380
*8500*8920*9020*9030*9050*9190*9230

****
*ee* Access control (theoretical-experimental solutions).
****
*0300*0440*1030*1390*1680*1700*2680*3550*3950*4560*4570*4580
*4640*4780*4790*4800*5590*5780*6810*7090*7100*8190*8200*9370
*9800

****
*ef* Access control below file level.
****
*0300*0900*1030*1880*2230*2240*2560*3090*3550*3700*4510*4560
*4570*4580*4640*4770*4780*4800*6170*7020*7030*7040*7050*7100
*7670*8200*8920

****
*eg* Residue control.
****
```

```
*9930

****
*eh* File integrity (programs and data).
****
*0040*0300*0850*0950*1680*1690*1880*1890*1980*2320*2630*4640
*5260*6080*7300*8190*8770*9190*9560

****
*ei* Operating/security system integrity and protection.
****
*0290*0300*0660*0670*0920*1030*1510*2220*2270*2800*3080*3160
*3550*3940*3950*3960*4770*4910*4920*4930*5560*5570*5600*5610
*6110*6550*6560*6810*7000*7020*7050*7110*7210*7220*7230*7240
*7270*7280*7290*7670*8160*8200*9020*9800

****
*ej* Processing restrictions.
****
*0300*0450*0850*1710*2220*2560*3550*3690*3950*4910*4920*4930
*7110*7210*7220*7230*7240*7290*9050*9190*9400*9440

****
*ek* Computer audit programs.
****
*0060*3320*5470*7440*7820*9710

****
*el* System monitoring and logging of significant events.
****
*0160*0180*0300*0440*0510*0520*0660*0670*0850*1030*1470*1600
*1670*1710*1980*2220*2270*2730*2900*3090*3160*3620*3680*3690
*3830*3950*4380*4560*4770*4780*4800*5350*5970*6170*6310*6320
*6590*6740*6800*7000*7020*7050*7110*7210*7220*7230*7240*7270
*7280*7290*7670*9020*9050*9120*9190*9270*9400*9520*9560*9800
*9930

****
*em* Checkpoint/restart procedures.
****
*1030*5200*6570*7880*9050*9220*9330*9865*9910

****
*en* Exception handling.
****
*0090*0650*1030*1600*2220*4380*7020*7050*7110*7270*9660

****
*eo* Hardware & operating system error controls (diagnostic
****   routines, parity checks, graceful degradation, etc.).
*1350*2420*6550*6560*6570
```

```
****
*ep* Data transmission security.
****
*0010*0300*0580*0690*2420*2470*2570*2580*3470*3690*3890*5000
*5450*5690*6140*6180*6220*6240*6430*6530*6570*6720*7210*7220
*7230*7240*7330*7780*7790*8290*8330*8340*8470*8670*8680*8960
*9260*9270.sp

****
*eq* Cryptography, data scrambling, and data compression.
****
*0300*0580*0670*0950*0970*1710*1720*1840*2220*2380*2390*2400
*2570*2580*2830*2960*3240*3300*3470*3560*3610*3690*3710*3790
*3800*3890*5320*5450*5510*5520*5680*5700*6390*6440*6450*6940
*6950*7290*7790*8090*8260*8470*8530*8540*8550*8560*8660*8850
*9240*9260*9270*9280*9300*9380*9400*9420*9430*9450

****
*er* Desensitizing information by introducing errors, data
****   separation, etc..
*1680*2560*4230*5690*7780*9260

****
*es* Insuring statistical confidentiality.
****
*3250*3260*4230*4590*6930*7780*8810*8820

****
*fa* Organization of the firm and EDP related groups.
****
*5390*5540*6590*7840*7850*7970*8000*9040

****
*fb* Management responsibilities.
****
*0280*0530*0550*0660*1210*1740*2220*3530*3880*4010*4080*4380
*4740*5120*5250*5540*5640*6300*6840*6900*7840*7850*7990*9110
*9930

****
*fc* Assigning security responsibilities.
****
*0860*1140*2220*2940*3530*3600*4090*5280*5410*5870*6250*6590
*6650*6890*7190*8580*9410*9530*9660*9670*9785

****
*fd* Information classification and/or value determination.
****
*0020*0300*0660*1890*2090*3030*3920*4230*5750*6090*6480*6730
*7020*7050*9280*9440*9855
```

```
****
*fe* Authorization of individuals to access specific data.
****
*1060*1980*2220*2320*2560*3550*3590*3630*4140*4530*5020*5370
*6050*6210*7090*7100*7470*7670*7960*9855*9910

****
*ff* Auditing.
****
*0060*0090*0160*0180*0340*0390*0400*0410*0420*0550*0650*0660
*0860*0890*0970*0980*0990*1000*1090*1140*1320*1330*1340*1600
*1820*1980*2090*2130*2140*2180*2320*2560*2610*2730*2860*2940
*3100*3160*3320*3460*3490*3530*3570*3600*3690*3910*3980*4090
*4260*4290*4330*4340*4430*4480*4550*4600*4610*4650*4720*4730
*5060*5070*5110*5160*5180*5210*5270*5280*5300*5350*5360*5390
*5410*5420*5430*5470*5540*5740*5770*5800*5820*5860*5880*5890
*6080*6250*6290*6400*6460*6470*6590*6650*6760*6770*6890*6910
*6920*7070*7130*7180*7190*7420*7440*7450*7460*7480*7520*7640
*7700*7710*7810*7820*7840*7850*7980*8010*8480*8580*8690*8700
*8720*8800*8910*9040*9050*9060*9080*9100*9120*9190*9320*9400
*9470*9480*9530*9620*9630*9640*9660*9680*9710*9765*9785*9815
*9895*9910*9955

****
*fg* Independent internal control group.
****
*0160*0190*0860*1600*1980*2090*3530*4760*5150*5160*6760*8400
*8690*9040*9400*9660

****
*fh* Acquisition and validation of input information.
****
*0950*1060*1250*1310*1890*1980*3130*3440*4530*4960*5650*6400
*6480*6510*7300*7840*7850*7960*8690*8780*9190*9540*9660*9855
*9885

****
*fi* Validation of programs.
****
*0300*1030*1150*1870*1980*2090*2560*2650*3160*3670*4030*4310
*4330*4340*4380*4860*5010*5160*6590*7180*7290*7300*7310*9040
*9050*9865

****
*fj* Program and data updating procedures.
****
*0950*1060*1250*2090*2870*3130*6280*6480*6590*7960*9660

****
*fk* Retention of information (obsolescence).
****
*1060*1350*2090*2690*3160*3530*6410*6480*7770*7960*8400*8690
```

```
*9400

****
*fl* Control of sensitive printouts through destruction.
****
*0650*2690*4210*4470*5020*6400*8690*9190*9440

****
*fm* Operations control.
****
*1020*2260*3280*3880*4390*4870*5180*5870*5910*6230*7070*7430
*7740*7830*7890*7950*8150*8490*8650*9330*9660*9775*9925

****
*fn* Schedules for all production jobs.
****
*0040*0190*1600*1980*3530*6230*9050

****
*fo* Documentation standards and procedures.
****
*1870*7840*7850*8690*9400

****
*fp* Library control of tapes, cards, disks; and good
****   housekeeping procedures.
*0180*0270*1630*1790*1980*2090*2610*2720*2980*3530*4330*4340
*5440*6590*6790*7710*7760*8430*8690*9400*9660*9855*9865

****
*fq* Separation and rotation of duties.
****
*0160*0970*1350*1670*1980*2090*2610*4660*7040*7840*7850*8210
*8690*9400*9660

****
*fr* Personnel advancement opportunities and grievance
****   procedures.
*1350*5640*6150*6160*6430

****
*fs* Personnel policy on security-related behavior (estab-
****   lishing, enforcing, and discipling).
*0160*0180*0640*1890*1920*2210*3530*3630*4450*5640*6090*6550
*6560*6840*6960*7210*7220*7230*7240*7260*7550*7750*8630*8870
*9110*9855*9875

****
*ft* Personnel integrity investigations.
****
*2090*4210*4810*5640*5840*5980*6030*6840*8170*8740*9400*9440
*9875
```

```
****
*fu* Personnel security education and training.
****
*0590*1890*2740*3530*7260*7800*8690*9060*9400*9470

****
*fv* Backup (files, documentation, personnel, and sites).
****
*0180*0190*0300*0470*0630*0660*0760*0970*1110*1290*1350*1650
*1670*1790*1980*2090*2430*2610*2760*4610*5140*5150*5220*5630
*5730*5800*6060*6400*6410*6850*7360*7660*7710*7760*7840*7850
*7930*7940*8640*8770*9010*9220*9400*9410*9660*9835

****
*fw* Emergency, contingency, and disaster recovery plans.
****
*0220*1080*1120*3530*4130*4360*4900*5140*5990*6610*6850*8060
*8770*9010*9410*9700*9930

****
*fx* Aperiodic testing and updating of security system.
****
*0300*0660*0800*1980*3160*3530*5150*5210*5420*5540*6300*6590
*7400*7680*7700*8590*9140*9400*9590*9660*9865

****
*fy* Insurance.
****
*0260*0350*0660*0790*1220*1230*1360*1790*1900*2090*2180*2290
*2520*2700*3270*3510*4170*4380*4500*4990*5040*5050*5220*5240
*6270*6630*6860*7460*8840*9400*9460*9795*9825*9985

****
*fz* Legal contracts.
****
*0470*0550*0820*0830*0840*1180*1230*1580*1900*2460*3290*3500
*3520*3540*5790*7310*7530*8130*8400*9090*9400*9820*9830*9930
*9980

****
*f1* Trade secrets and copyrights.
****
*0550*0700*0830*1050*1790*2850*2920*3750*3850*5090*5460*5660
*5760*5970*7550*8730*9825*9865*9950

****
*ga* Computer room architecture.
****
*0180*0540*0660*1040*1290*1530*1590*1670*1920*2050*2180*2210
*3360*4420*4820*4850*5100*5140*5840*6020*6330*6820*7410*7600
*7750*7910*8220*9700*9770*9835*9900*9930
```

```
****
*gb* Computer room environment control.
****
*6830*9905

****
*gc* Equipment & storage media durability or reliability; &
****   accessory protective devices (plastic covers, safes).
*1300*2430*2690*2720*3180*3660*4490*4990*5030*5440*5730*5990
*6120*6130*6830*7340*7390*8050*8430*8640*9200*9915

****
*gd* Backup power supplies.
****
*0180*0870*0880*1130*1270*1300*2040*2840*4360*5030*7010*7750
*8060*8750*9000*9510*9740

****
*ge* Fire alarms and extinguishers.
****
*0430*1170*1780*1790*1830*2970*3330*3340*3350*3430*4730*5100
*5170*5440*6330*7580*7590*7660*7750*7860*8060*8400*8450*9835
*9900*9930*9935

****
*gf* Physical access controls (alarms, guards, locks, etc.).
****
*0180*1040*1190*1570*1590*1640*1790*1930*2990*3360*3420*4170
*4420*4690*4730*4850*4950*5030*5140*5150*5500*5840*6070*6820
*6880*7210*7220*7230*7240*7410*7570*7620*7650*7660*7910*7930
*7940*8330*8370*8400*8420*8450*9500*9700*9835*9930

****
*gg* General discussion of safeguards.
****
*0290*0300*0660*0670*0680*0850*1360*1380*1400*1440*1670*1730
*1790*2030*2120*2160*2210*2590*2740*2950*3000*3140*3150*3170
*3650*3690*3820*3900*4070*4170*4380*4400*5480*6210*6400*6520
*6620*7210*7220*7230*7240*8360*8410*9130*9400

****
*gh* Existing system and equipment descriptions.
****
*0030*0060*0300*0370*0450*0510*0520*0630*0690*0850*0920*1210
*1710*1790*1910*2100*2230*2240*2280*2370*2400*2560*2570*2580
*2990*3010*3030*3070*3120*3320*3690*3790*3800*3810*3830*3870
*3950*3960*4510*4530*4770*4780*4800*4910*4920*4930*4950*5520
*5560*5580*5680*5700*5850*5920*6010*6170*6550*6560*6740*6780
*6800*6950*7000*7020*7030*7040*7050*7110*7200*7670*8030*8310
*8380*8410*8420*8660*8920*9020*9030*9230*9300*9520*9560*9710
*9800*9835
```

H. SPECIFIC THREATS.

****
ha General discussion of internal data access threats.
****
*0170*0300*1010*1030*1240*1550*1680*2230*2560*3170*3720*3730
*3740*4000*4170*4640*4780*6350*7150*9270*9390*9400*9970

****
hb Espionage.
****
*0130*3040*3420*3450*3760*3890*3990*4370*4380*4420*4670*4680
*4700*4710*4750*5450*5850*6840*7160*7290*7560*8330*8380*9170
*9800

****
hc Copying & selling proprietary software or databases.
****
*0170*0480*0550*0670*1050*1540*2180*2400*2460*2920*3670*3700
*4610*4830*5090*5230*5460*5970*6690*6700*6880*7380*7540*7550
*8730*8770*9390*9550*9865*9875

****
hd Illegally reading private information of others.
****
*0020*0170*0300*0480*0570*0640*0660*0710*0850*0940*0950*0970
*1060*1250*1490*1670*1680*1690*1710*1720*1760*1790*1890*2160
*2310*2350*2400*2590*2630*2670*2690*2910*3050*3150*3190*3440
*3590*3630*3650*3840*3900*3920*4140*4380*4400*4520*4620*4890
*5810*6480*6490*6550*6560*6800*6870*7160*7210*7220*7230*7240
*7270*7290*7330*7470*7490*7920*7960*8020*8110*8610*8790*8990
*9560*9850*9855*9975

****
he Combining authorized data to produce unauthorized
**** information.
*0950*0960*1280*1470*1690*3250*3260*4230*4590*4960*7490*9800

****
hf Accidental disclosure of restricted information.
****
*0300*0840*1220*1680

****
hg Malicious destruction of others' data.
****
*0170*0300*0330*0480*0670*0810*1220*2090*3050*6840*8040*9780

****
hi Accidential destruction of others' or one's own data.
****
*0170*0300*0840*1030*1290*2670*3660*9800

```
****
*hj* Embezzlement.
****
*0010*0080*0090*0150*0160*0170*0240*0380*1600*1670*1980*2020
*2090*2110*2150*2450*3490*3780*4720*4810*5010*5070*5160*5190
*5290*5310*6260*6840*7450*7460*8210*8610*9080*9100*9160*9390

****
*hk* Data input fraud.
****
*0160*0170*1100*1600*1750*2110*2870*3980*4660*5290*5400*5720
*5740*6710*7910*8700*8780*9080*9400

****
*hl* Operator fraud.
****
*0910*1600*4660*5010*5290*6420*9400*9570

****
*hm* Programmer fraud.
****
*0090*0160*0170*0190*0910*1030*1600*2110*3770*4810*5010*5290
*5970*6040*8720*9080*9400*9570*9865

****
*hn* Program user fraud.
****
*1600*2900*8600*9570

****
*ho* Fraudulently altering others' data to lessen one's
****   non-financial liabilities.
*0140*0450*7910

****
*hp* Data input errors.
****
*0450*1100*1520*1750*2720*2870*3130*3220*3980*4860*5650*5740
*6760*7400*8700*9540*9660*9940

****
*hq* Operator errors.
****
*0190*0970*5150*9400*9660

****
*hr* Programmer errors.
****
*0190*0300*0550*0630*0970*1090*1580*2530*4030*4310*4860*5650
*6000*6750*6760*7310*9400*9660*9865
```

```
****
*hs* Program user errors.
****
*0550

****
*ht* Operating system error.
****
*0300*0920*1510*1580*2430*3860*4120*7210*7220*7230*7240*9520

****
*hu* Hardware errors.
****
*0300*0660*1580*2430*3180*3860*4120*6550*6560*6830*7210*7220
*7230*7240*9520*9570

****
*hv* Hardware or software implementation delays.
****
*1100*1150*1580*6600*7370*7990*8860

****
*hw* Negligence.
****
*3410*7210*7220*7230*7240*8880

****
*ia* Operator.
****
*0480*1710*2890*3160*5640*6030*6420*6700*6880*6960

****
*ib* User of "canned" Programs.
****
*none

****
*ic* High-level language programmer.
****
*5640*8610*9390

****
*id* Assembly language programmer.
****
*3160*5640*6010*6550*6560*7180*9570

****
*ie* Maintenance personnel.
****
*5640*6430*6550*6560*6880*9570
```

```
****
*if* Manager.
****
*0090*1310*1600*2110*2150*2310*5160*5720*5930*6260*6420*6840
*7910*8780*9080*9390

****
*ig* Authorized file user.
****
*8020*9390

****
*ih* Authorized computer system user.
****
*0140*1890*5970*8020*8610*9570*9750*9800

****
*ii* Unauthorized computer system user.
****
*0480*0570*0660*0910*1040*1240*1490*1540*1710*2110*3190*4830
*5080*5090*5400*6690*7330*7380*7910*8400*8600*9270*9570

****
*ja* General discussion of external threats.
****
*0540*0670*2190*3170*4170*7150*9400

****
*jb* Labor strikes.
****
*5640*6430*6580

****
*jc* Physical theft of tapes, cards, etc..
****
*0480*1110*3200*3930*4420*4470*4730*6620*9400*9875

****
*jd* Radiation.
****
*0670*1290*2690*3660*4380*6140*6150*6160*7160*7210*7220*7230
*7240*7290

****
*je* Wiretapping.
****
*0480*0660*0670*1660*1670*1710*1790*2560*3470*4380*5450*6140
*6720*7160*7290*7330*7610*9270

****
*jf* Bombs, magnets, and other means of sabotage.
****
```

```
*0110*0170*0190*0330*0670*1040*1160*1670*1790*1930*1960*2290
*2820*2890*3050*3360*3970*4060*4220*4360*4380*4420*4690*4840
*4850*6130*6150*6160*6330*6580*6610*6660*6720*6820*6880*7250
*7340*7900*8040*8060*8320*8370*8400*8430*8520*8940*8950*9200
*9290*9310*9350*9400*9490*9780*9835*9915*9945

****
*jg* Fire, water, dust, static electricity, earthquake,
****   tornato, etc..
*0170*0180*0430*0490*0500*0620*0730*0740*0750*1040*1080*1170
*1430*1530*1790*1830*2820*3180*3330*3350*3430*3660*4360*4380
*4420*4490*4730*4820*4900*5730*5830*5900*5940*5990*6670*6680
*6830*7390*7410*7750*8080*8400*8430*8640*9400*9770*9780

****
*jh* Air conditioning, and power failures.
****
*0670*0870*0880*1130*1270*1300*5940*7010*7080*8400*8750*9510
*9740*9860*9905
```

K. COMPUTER AND DATA ENVIRONMENT.

```
****
*ka* Personal information stored on others.
****
*0080*0450*0560*0570*0680*0820*0840*0930*0950*1100*1250*1310
*1690*1760*1890*2410*2550*2590*2870*3050*3110*3130*3150*3440
*3590*3630*3640*3650*3700*3920*4010*4140*4150*4180*4190*4210
*4230*4380*4400*4440*4450*4520*4530*4620*4630*4890*4940*4960
*5330*5370*5650*5810*5930*5950*5960*6050*6280*6480*6490*6510
*6800*6870*7470*7490*7500*7510*7920*7960*8020*8110*8180*8310
*8780*8790*8810*8820*8830*9280*9360*9560*9690*9840*9845*9850
*9855*9885

****
*kb* One's private information stored exclusively for
****   one's own use.
*0010*0020*0030*0080*0130*0160*0180*0190*0290*0330*0440*0530
*0650*0700*0940*1520*1580*1600*1710*1900*1980*2090*2560*2610
*3040*3490*3670*3890*3910*4610*5020*5090*5160*5220*5230*5450
*5550*5720*5800*6420*6590*6700*6710*6840*7180*7270*7460*7550
*8210*8330*8380*8520*8700*9050*9170*9400

****
*kc* Information stored for renting and royalty.
****
*4830*5760*5970

****
*kd* Accounting and financial.
****
```

```
*0010*0030*0090*0120*0140*0160*0170*0190*0240*0390*0420*0530
*0550*0650*0660*0820*0890*0990*1090*1140*1340*1520*1820*1980
*2090*2450*2530*3490*3530*3910*4160*4480*4810*5010*5060*5070
*5160*5180*5210*5220*5720*5800*6080*6400*6420*6590*6650*6710
*6840*6970*7420*7460*8210*8580*8610*8630*8690*8700*8720*9040
*9050*9080*9100*9110*9120*9160*9190*9390*9400*9610*9620*9630
*9640*9660*9680*9940

****
*ke* Manufacturing.
****
*1580*3680

****
*kf* Marketing and sales (mailing lists).
****
*1580*2310*5050*5930*6700*8600*9390

****
*kg* Research and development.
****
*0370*0940*6660*7360

****
*la* Batch processing (multiprogramming).
****
*0890*1100*1600*1820*2090*2240*2610*2760*5310*9400

****
*lb* Time sharing (multiprogramming, remote real-time-
****   interactive access).
*0300*0440*0450*0480*0570*0630*0640*0650*0660*0670*0680*0770
*0780*0850*0900*0920*0970*1010*1220*1240*1370*1540*1670*1710
*1720*1810*1860*1880*1910*2000*2160*2210*2230*2270*2280*2320
*2330*2400*2430*2560*2630*2640*2690*2730*2860*2900*2960*3000
*3120*3190*3470*3480*3550*3640*3650*3760*3810*3830*3840*3900
*4050*4100*4140*4380*4550*4560*4830*5200*5580*5850*6170*6180
*6240*6310*6350*6430*6570*6690*6740*6780*6800*7000*7020*7030
*7040*7050*7100*7200*7290*7330*7380*8020*8070*8200*8390*8600
*9130*9190*9220*9230*9270*9280*9400*9520*9560*9570*9800*9890
*9970

****
*ma* EDP Service bureaus (facilities management, "canned"
****   program services, or selling only computer time).
*0550*0820*0840*1180*1230*1240*1540*1710*1900*2100*2180*2460
*2610*2620*2640*3190*3290*3480*3520*3540*4830*5090*5790*5970
*7380*7530*8130*8140*8460*9400*9820*9830*9910

****
*mb* Organizations owning and selling access rights to
****   large "personal information" databanks.
```

```
*0300*0360*0460*0560*0570*0610*0840*0950*1230*1250*1560*1690
*1760*1810*1890*2550*2590*3150*3410*3440*3900*3920*4010*4110
*4230*4620*5330*5340*5950*5960*6050*6280*6480*7490*7960*8810
*8820*8830*9130*9560*9600*9840

****
*mc* Banks, credit agencies, insurance companies, and
****   other financial institutions.
*0140*0230*0390*0530*0540*0710*0810*1110*1120*1310*1520*1590
*1690*1830*2030*2110*2140*2150*2340*2770*2860*2900*2990*3050
*3110*3230*3530*3780*5220*5400*5720*5890*6000*6260*6360*6420
*6430*6630*6840*6880*6890*6970*7450*7460*7910*8210*8280*8460
*8620*8890*8900*9080*9100*9390*9700

****
*md* Federal government.
****
*0310*0680*0710*1280*1290*1690*1760*1800*1890*2590*3220*3230
*3930*4050*4530*4660*6930*7060*7490*7960*8610*8960*9390*9560
*9600*9845*9850

****
*me* Local government.
****
*1090*1100*1130*1160*2310*2870*3390*3930*4240*4810*5010*5670
*5930*6020*6750*6870*8610*8640*8860*9940

****
*mf* Legal and law enforcement.
****
*0450*1100*1410*1420*1610*1620*1690*1810*2550*3130*3630*3640
*3650*4140*4210*4320*5370*6960*7490*8020*8100*8310*8780*9170
*9210*9360*9540

****
*mg* Medical.
****
*0040*0600*1690*2320*2410*3590*3700*4190*4400*4620*6800*7490
*9600

****
*mh* Military.
****
*0020*0100*0130*0290*0330*0690*0730*0850*0910*1260*1470*1920
*3010*3030*3680*5850*6660*7110*7160*7270*8030*8380*8440*8520
*9140*9580*9800

****
*mi* Transportation.
****
*0730*1580*5030*6710*7540*7660*9610
```

```
****
*mj* Educational.
****
*0110*0370*0590*0930*0940*0960*1690*2290*3360*3770*3970*4220
*4690*4840*4850*6660*6820*7470*7490*8320*8940*8950*9290*9310
*9350*9915

****
*mk* Voting systems.
****
*1150*2650*2710*3160*6040*7180*8300*8570*8860
```

N. MISCELLANEOUS.

```
****
*na* Recovery from computer errors, crimes, and disasters.
****
*0100*0490*0500*0740*0750*1150*2430*3860*4820*5940*5990*7300
*7880*8080*8640

****
*nb* Security expense versus requirements, and security
****   cost effectiveness.
*0020*0130*0180*0190*0660*0850*1360*1700*1790*3170*3530*4070
*4350*4540*4600*4740*5130*5200*5250*6030*6270*6810*7020*7050
*7870*8410*8650*8770*8970*9260*9280*9795*9805*9930*9935

****
*nc* Reliability, flexibility, efficiency, and non-monetary
****   costs of security.
*0130*0300*1890*2230*3060*3170*3530*3550*3850*3880*3950*4570
*4580*6550*6560*7020*7050*9180*9280*9800

****
*nd* Obtaining services from security consulting companies.
****
*4050*4980*5250*6150*6160*7490*8370*8450*9835*9900

****
*ne* Computer security apathy.
****
*0190*0480*0590*0610*0810*1120*1500*1550*1650*1710*2780*3490
*3720*3730*3740*6730*8300*8720

****
*nf* Implementing a security program.
****
*0050*0130*0160*0650*1070*1360*1730*1890*1980*2030*2090*2560
*3170*3530*4070*4330*4340*4360*4380*4740*5120*5140*5220*5490
*5540*5980*6360*6400*6590*6790*7020*7030*7050*7180*7190*7840
*7850*8770*8970*9050*9280*9400*9930
```

```
****
*ng* Areas currently being researched, or needing future
****   research.
*0290*0300*0920*0950*1070*1200*1210*1610*1680*1690*1700*1720
*2000*2230*3030*3550*3690*3800*3850*4230*4520*4560*4770*4780
*4800*4880*4890*4940*5950*6390*6550*6560*6810*7000*7100*7140
*7490*7870*8190*8410*8890*8900*9120*9280*9805*9855

****
*nh* Security frameworks.
****
*0130*0660*0670*1060*1070*3690*3950*7210*7220*7230*7240*7290
*7320*8410*9280*9570

****
*ni* Security checklists.
****
*0010*0050*0160*0180*1070*1200*1320*1770*2940*3170*4160*4170
*4330*4740*4760*5270*5490*5530*6200*6400*6590*7210*7220*7230
*7240*7290*7460*7640*7680*7950*9050*9190*9400*9570*9990

****
*nj* Private legal matters, and management's legal
****   responsibilities.
*0230*0320*0550*0840*1180*1240*1580*2310*3130*3190*3490*3510
*3530*3540*4010*4080*4180*4220*4440*4450*5090*5930*5970*6000
*6280*6700*7120*7380*7530*8120*8460*8620*8780*8860*8980*9090
*9610*9820*9830*9865*9930*9950*9965

****
*nk* Manufacturers' responsibility in providing safeguards.
****
*0300*0360*0480*0550*0570*1580*1710*3520*3540*3790*4010*4440
*4450*4880*4890*4900*4940*5000*5670*5730*5940*6180*6190*6550
*6560*7180*7870

****
*nl* Government regulation.
****
*0560*0570*0680*0820*0830*0840*0950*1250*1810*2410*2530*3110
*3150*3440*3630*3690*3920*4010*4150*4440*4450*4520*4530*4560
*4630*5330*5460*5760*5950*5960*6050*6210*6240*6280*6370*6480
*6490*6510*7500*7960*8020*8180*8280*8510*8630*8780*8790*9110
*9400*9560*9600*9840*9845*9850*9855*9885*9950

****
*nm* Privacy issues.
****
*0040*0310*0360*0560*0570*0590*0600*0680*0710*0820*0840*0930
*0950*1060*1070*1250*1280*1310*1380*1560*1680*1690*1760*1800
*1810*1890*2170*2300*2320*2410*2550*2590*2910*3050*3110*3140
*3150*3390*3410*3440*3450*3590*3630*3640*3650*3700*3900*4010
```

*4110*4140*4150*4200*4210*4230*4240*4270*4280*4400*4520*4530
*4560*4630*4890*4940*4960*5330*5370*5950*5960*6050*6210*6240
*6280*6370*6380*6480*6490*6510*6870*7470*7490*7500*7510*7630
*7920*7960*8020*8110*8170*8180*8270*8310*8510*8780*8790*8810
*8820*8830*8990*9400*9210*9560*9600*9690*9840*9845*9850*9855
*9870*9880*9885

****
nn General survey articles.
****
*0170*0550*0670*0770*0780*1370*1380*1790*2610*0300*3170*3530
*3690*4360*4380*4560*5320*5490*5540*5980*6480*7100*7210*7220
*7230*7240*7290*8260*9250*9400*9590*9850

****
no Computer security research surveys.
****
*1250*1310*1690*1710*1970*1980*2910*4180*4880*4890*4940*6030
*6480*6510*7140*7490*7660*8060*8300*8410*8610*9020*9030*9855

****
np Other bibliographies and references.
****
*0310*0770*0780*1350*1370*1480*1940*1950*2010*2080*2170*2200
*2510*3580*4270*4280*4970*5530*7630*7720*9400*9600*9850*9920

****
nq Classified articles.
****
*3010*8380*9590

X. ESTIMATE OF ARTICLE'S CURRENT USEFULNESS AND UNIQUENESS.

****
x1 Poor.
****
*0180*0430*0440*0450*0580*0820*0970*1040*1140*1180*1260*1270
*1300*1310*1540*1550*1590*1670*1810*1900*1910*1930*1950*2030
*2060*2100*2120*2130*2140*2150*2200*2310*2370*2380*2550*2740
*2760*2830*2870*2920*2990*3120*3230*3340*3360*3400*3410*3480
*3490*3580*3720*3730*3740*3780*3830*3890*3910*3970*4060*4150
*4190*4410*4550*4660*4690*4830*4890*4940*4970*5030*5090*5220
*5240*5630*5650*5700*5710*5760*5840*5990*6040*6050*6060*6070
*6080*6180*6330*6420*6650*6720*6820*6880*6930*6970*7200*7360
*7380*7620*7710*7720*7910*8100*8110*8210*8240*8250*8280*8330
*8370*8510*8600*8620*8720*8760*8920*9040*9210*9230*9250*9440
*9450*9520*9670*9690*9700*9750*9940*9965

****
x2 Fair.
****

```
*0090*0130*0190*0470*0480*0530*0570*0630*0640*0760*0840*1050
*1100*1110*1120*1130*1150*1170*1200*1210*1230*1240*1290*1480
*1490*1580*1620*1700*1780*1790*1940*2000*2080*2110*2180*2280
*2510*2520*2560*2590*2650*2680*2890*2970*3030*3060*3130*3180
*3420*3440*3470*3590*3660*3690*3770*3810*3960*4080*4140*4210
*4330*4340*4360*4380*4440*4450*4530*4540*4570*4580*4600*4760
*4790*4820*4880*4950*4980*5120*5150*5370*5460*5560*5690*5720
*5730*5800*5810*5930*5940*5950*5970*6000*6210*6260*6430*6440
*6490*6510*6570*6630*6710*6840*7030*7040*7140*7160*7180*7210
*7220*7230*7240*7270*7290*7300*7330*7340*7460*7610*7660*7780
*7870*7990*8020*8120*8130*8200*8400*8470*8580*8590*8610*8630
*8640*8780*9110*9270*9380*9390*9410*9420*9460*9490*9540*9570
*9600*9660*9740*9770*9835*9885*9900*9920*9930*9980*9985

****
*x3* Good.
****
*0170*0310*0650*0660*0670*0770*0780*0850*0920*0950*1080*1220
*1250*1360*1600*1680*1710*1720*1890*2010*2240*2430*2610*3160
*3520*3540*3550*4350*4520*4560*4590*4740*5160*5250*5320*5400
*5450*5490*5640*5900*5960*5980*6010*6030*6110*6130*6150*6160
*6390*6400*6480*6590*6810*6830*7050*7840*7850*8300*8550*8560
*8570*8690*8770*8790*8850*8970*9080*9100*9120*9190*9200*9260
*9580*9800*9805

****
*x4* Excellent.
****
*0160*0550*1070*1370*1690*1980*2090*2170*2230*0300*3530*3790
*3850*3950*4230*4270*4280*5530*6550*6560*7020*7100*7490*7630
*8180*8410*9280*9400*9560*9850*9855
```

IV. ANNOTATED BIBLIOGRAPHY

*(0010)*68*ae*ba*bb*cc*ep*hj*kb*kd*ni
Aaron, William. "Embezzlement - Detection and Control." Speech before the NATIONAL RETAIL MERCHANTS ASSOCIATION EDP CONFERENCE, 1968.

Examples of computer misuse are given. Several security weak points in keeping financial records are described. Also, a checklist of security controls is presented.

*(0020)*70*ab*cc*fd*hd*kb*mh*nb
Abdian, A. G.; and Klienfelter, P. "Transfer of Security-Classified Information." JOURNAL OF CHEMICAL DOCUMENTATION, November 1970, pp. 224-226.

The safeguarding of security-classified information and the dissemination of this information are fundamentally conflicting requirements of the Defense Department Documentation Center. Complex and costly techniques must be used to achieve a satisfactory balance between these requirements. Areas of special difficulty or new interest are described. Also, the cost impacts of processing security-classified information are summarized with respect to several information processing functions.

*(0030)*70*ac*ai*cb*da*db*ed*gh*kb*kd
"Accounting System Uses 'Lock and Key' to Prevent Payment Default, Copying." COMPUTERWORLD, 20 May 1970.

The article discusses a software product that prevents default of payment and unauthorized copying of software packages.

*(0040)*68*ae*cc*dd*de*eh*fn*mg*nm
Acheson, E. D. (ed.). RECORD LINKAGE IN MEDICINE. E. and S. Livingston, London, 1968.

This is a publication of proceedings of a conference. Methods are described to insure that incorrect medical records are not accessed by the doctor. Some comments are also made on medical ethics.

*(0050)*67*ab*cb*cc*dg*nf*ni
Adams, D. L. "Planning Checklist for a Computer Installation." DATAMATION, June 1967, pp. 37-39.

*(0060)*72*ab*cb*ek*ff*gh
Adams, D. L.; and Mullarkey, J. F. "A Survey of Software." JOURNAL OF ACCOUNTANCY, September 1972, pp. 39-49.

*(0070)*69*ab*ba*bb
Adelson, Alan M. "Computer Bandits." TRUE, February 1969,

p.50.

*(0080)*65*ab*bb*db*hj*ka*kb
Adelson, Alan M. "Embezzlement by Computer." SECURITY WORLD, September 1965.

*(0090)*68*ac*bb*cc*db*en*ff*hj*hm*if*kd*x2
Adelson, Alan M. "Whir, Blink, Jackpot! - Crooked Operators Use Computers to Embezzle Money from Companies." THE WALL STREET JOURNAL, 5 April 1968, p. 1.

Several interesting examples of actual computer embezzlements are described. One manager in charge of back-office operations at Walston and Company, a New York brokerage firm, electronically siphoned $250,000 out of the company between 1951 and 1959. By the time the theft was finally uncovered, the man had become a vice president. Some very common safeguards are also suggested.

*(0100)*69*ad*cc*cd*mh*na
"ADP Installation Emergency Planning (Continuity of Operations)." AD-705 341, National Technical Information Service, Springfield, Virginia 22151, December 1969, 101 pp.

This is a task group report for the Department of Defense ADP Policy Committee.

*(0110)*70*ac*ai*bc*dc*jf*mj
"Aftermath of Sir George Williams University Computer Center Destruction in February, 1969." COMPUTERWORLD, April 1970, p. 1.

A computer center is destroyed by students over the racial prejudice of one professor. Students' intent was to use control of computer center as a bargaining strength. Lack of administration action angered the students.

*(0120)*71*ac*ai*bd*be*dd*de*kd
"Agency Collects Bills Previously Paid." COMPUTERWORLD, 3 March 1971.

*(0130)*67*ad*cc*cd*da*db*dc*hb*kb*mh*nb*nc*nf*nh*x2
"Air Force Systems Command Manual: System Security Engineering." AFSC Manual No. 207-1, Headquarters Air Force Systems Command, Andrews Air Force Base, Washington, D.C. 20331; or Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402, 28 December 1967, $.60.

The program formulated by this manual is intended to increase the effectivemess of the Aerospace Systems Security Program by focusing proper attention on the security of a system (computer, communications, missle, etc.) in time to permit its consideration during the basic definition/design effort. Although the manual doesn't specifically discuss "computer" systems, parts of it are pertinent to computer security. Of the manual's six chapters, chapter five is by far the most useful for computer systems. It presents a comprehensive and detailed model for analyzing threats such as theft, fraud, and sabotage. The model insures that all aspects of potential and actual threats are adequately investigated. It makes use of logical diagrams utilizing, AND, OR, INHIBIT, and EXCLUSIVE-OR logical gates.

*(0140)*70*ac*ai*bb*cb*db*ho*ih*kd*mc

"'Alert' Program Spots Credit Ring." COMPUTERWORLD, 9 December 1970, p. 1.

A bank's computer security system discovered that a New York haberdasher was involved with stolen credit cards.

*(0150)*60*ab*bb*db*hj

Allan, J. A. "Embezzlement by Electronics." ACCOUNTANTS MAGAZINE, April 1960, pp. 253-255.

*(0160)*71*ab*ba*bb*cc*da*db*el*ff*fg*fq*fs*hj*hk*hm*kb *kd*nf*ni*x4

Allen, Brandt R. "Computer Fraud." FINANCIAL EXECUTIVE, May 1971, p. 38.

First, the author reveals the magnitude of the fraud problem: 69,000 people were arrested for fraud in 1970; fraud and embezzlement losses exceed by a wide margin corporate robbery, burglary, and shoplifting losses; fraud losses exceed $1 billion annually; and 1.2% of all business failures (over 100 in 1969) were due to fraud. The number of fraud cases involving computers is sharply increasing. Four basic approaches to computer fraud are: manipulation of input data, developing improper computer programs, alteration of data files, and illegal transmission of teleprocessed information. Twelve interesting fraud examples are described to clarify these approaches. The author claims that the computer enhances opportunities for fraud and increases the problems of prevention. His reasons briefly are: new types of people, centralization of data, lack of human intervention, computer difficult to understand, changes made without a trace, and degraded audit trails. Surveys are cited which show the vast majority of embezzlements occur in the area of disbursement. Payroll accounts for less than 5% of the total. Recognizing certain danger signals from personnel behavior is also discussed. Finally, the following fraud prevention checklist is discussed: background checks, rotation of duties, production schedules, run control log, program change schedule, master file control, I/O checking by separate group, comparison of actual and planned performance, rigid password control, and an internal audit group.

*(0170)*72*ab*bg*cc*cd*dg*ha*hc*hd*hg*hi*hj*hk*hm*jf*jg *kd*nn*x3

Allen, Brandt R. "Computer Security - PART 1." DATA MANAGEMENT, January 1972, pp. 18-24.

The author states that the five major hazards to the computer complex are fire, water, theft, fraud, and sabotage. He then discusses each of these hazards in detail and presents a large number of accidents, crimes, and disasters that could occur in each hazard area. Of these hazards, fire is generally considered the most serious. Some valuable information is given on the vulnerability of magnetic tapes to fire and water. The discussion on fraud is almost identical to that found in an earlier article by Allen, entitled "Computer Fraud". Part 2 of this article, in the February issue, discusses precautions that management should employ to insure security of the computer and its data.

*(0180)*72*ab*bc*cc*cd*dg*el*ff*fp*fs*fv*ga*gd*gf*jg*kb *nb*ni*x1

Allen, Brandt R. "Computer Security - PART 2." DATA MANAGEMENT, February 1972, pp. 24-30.

The increasing use of on-line real-time computer systems, the tendency toward greater integration software and databases, and the increasing centralization of hardware are all making the security problem much more difficult. Common safeguards are briefly described for: physical security (flooding, riot, power, building location and architecture); software backup (data files, application programs, documentation, emergency drills); hardware backup (firms join to buy backup system); and operations (production schedules, run control log, program change control, master file control, I/O control, operations review, password control, internal audit group). Part 1 of this article can be found in the January issue of DATA MANAGEMENT.

*(0190)*68*ab*bg*cc*cd*dg*fg*fn*fv*hm*hq*hr*jf*kb*kd*nb *ne*x2

Allen, Brandt R. "Danger Ahead. Safeguard Your Computer." HARVARD BUSINESS REVIEW, November 1968, pp. 97-101.

Every company's management should ask itself what would happen if its computer center was completely destroyed, and is the same protection given to data in computer files as was given in pre-computer days. Examples are given of environmental disasters, mechanical failures, operator errors, program errors, theft, fraud, and sabotage. It is suggested that management compare the cost of complete and permanent computer disruption with the cost of complete protection. The author then gives some reasons for computer security apathy and recommends a few safeguards such as: controlled access to the computer room, scheduling of production jobs, file duplication, improved program design, and use of an internal security group.

*(0200)*71*ae*cb*cc
Allen, Brandt R. "New Developments in Computer Security." MDI SEMINAR REFERENCE MANUAL, 1971.

*(0210)*70*ac*ai
"All's Well That Ends Well." COMPUTERWORLD, 16 December 1970, p. 4.

*(0220)*67*ab*cc*dc*fw
Allsbrook, D. N. "Planning an Emergency Preparedness Program." BURROUGHS CLEARINGHOUSE, December 1967, p. 30.

*(0230)*70*ac*ai*bd*be*dd*de*mc*nj
"American Express Sued for $25,000." COMPUTERWORLD, 16 December 1970, p. 4.

*(0240)*71*af*cc*db*hj*kd
Amir, M. "Computer Embezzlement: Prevention and Control." COMPUTER BULLETIN, November 1971.

*(0250)*67*ab*cc
Anderson, Arthur F. "Company Security Practices." THE CONFERENCE BOARD RECORD, October 1967.

*(0260)*68*ab*cc*fy
Anderson, Arthur F. "Computer Insurance." THE ACCOUNTANT, 6 April 1968.

*(0270)*68*ab*cc*da*db*dc*fp
Anderson, Arthur F. "Records Protection in the Age of EDP." THE OFFICE, October 1968.

*(0280)*69*ae*cc*fb
Anderson, B. G. "The Systems Executive's Responsibility in Guarding the Data Resource." American Management Association Conference on Security and Catastrophe Prevention Management of the Computer Complex, November 1969.

*(0290)*72*ad*cb*ec*ed*ei*gg*kb*mh*ng
Anderson, James P. "Computer Security Technology Planning Study." AD-758 206, National Technical Information Service, Springfield, Virginia 22151, October 1972, 43

pp., $3.00.

This report presents the results of a planning study on computer security requirements for the U.S. Air Force. The study concludes that research and development is urgently needed to provide secure command/control and support systems for the Air Force.

*(0300)*72*aa*ca*cb*dg*fd*ea*ec*ed*ee*ef*eh*ei*ej*el*ep *eq*fi*fv*fx*gg*gh*ha*hd*hf*hg*hi*hr*ht*hu*lb*mb*nc*ng *nk*nn*x4

Anderson, James P. "Information Security in a Multi-User Computer Environment." ADVANCES IN COMPUTERS, Morris Robinoff ed., Academic Press Inc., 111 Fifth Avenue, New York, New York 10003, 1972, pp. 1-35.

This excellent article is primarily concerned with the threat to information posed by programmers who can gain access to a multi-user system and exploit known or suspected weaknesses in the operating system. The author essentially combined and summarized the contents of approximately 25 important articles on hardware and operating system security, as well as having added his own valuable ideas. Throughout this article, many different types or methods of illegal data access are mentioned, with feasible hardware and software countermeasures usually being proposed. Most of the article is quite technical and understanding it requires a fair knowledge of how computers process information.

Some of the more interesting comments in this article are presented below. The possibility of incomplete design is one of the major problems in information security in multi-user systems. Due to the very wide variability in the environment, equipment, stored information, and user populations, no single set of measures can be specified to insure multi-user system security. Several factors must be considered in categorizing data value. The issue of privacy relates to disclosure policy regardless of the kind of data or the environment it arises in. Because OS/360 uses locations within the user address space to store addresses of privileged operating systems routines, it is an easy system to exploit. The major source of security problems in contemporary operating systems is that systems designers are only remotely aware of potential malevolent penetration threats. The principle problems of file encryption are similar to those of password protected files. A pseudo-user program that periodically attempts to violate memory bounds and execute instructions reserved for the supervisor state is recommended. Wiretapping has not been a major problem. Information security is a problem of providing sufficient barriers and controls to force a prospective penetrator into attacks that carry a high risk of detection and/or have a very large work factor.

An outline of this article is given below. The Computer Security Problem (technical threats, backup data, types of multi-user systems); Techniques of System Access Control (password design considerations and distribution); Computer Characteristics Supporting Security (multiprogramming hardware, program isolation methods, privileged mode, I/O characteristics, virtual machines); Operating System Functions Related to Security (common services, output routing, sources of problems); Problems of File Protection (models for shared information and hierarchical access control); Techniques of File Protection (OS/360, encryption); Techniques for Security Assurance (pseudo-tester, audit trails, program validation); and Communications Problems (wiretapping, encryption equipment).

*(0310)*72*ab*md*nm*np**x3

Anderson, Ronald E.; and Fagerlund, Ed. "Privacy and the Computer: An Annotated Bibliography." COMPUTING REVIEWS, November 1972, pp. 551-559.

This is a 'selected' annotated bibliography of 102 articles. It is the most complete and up-to-date bibliography on privacy and computers. The articles are divided into three sections dealing with general privacy issues, government information systems, and U.S. congressional hearings. Only 10 of the 102 articles are concerned with computer security issues, and they can easily be found in other references. Eight other privacy bibliographies are mentioned at the beginning of this privacy bibliography. For the person primarily interested in privacy issues, Annette Harrison's two bibliographies covering the period prior to 1967 and 1967-1969, are excellent complementary references.

*(0320)*71*ac*ai*bb*nj

"Antitrust Suit Charges Rearrangement of Data." COMPUTERWORLD, 24 March 1971, p. 4.

*(0330)*69*ac*ai*bc*dc*hg*jf*kb*mh

"Anti-War Protestors Erase 1,000 Dow Tapes." COMPUTERWORLD, 3 December 1969, p. 1.

Damage done by war protestors at Dow Chemical's plant in Midland, Michigan is reported on.

*(0340)*65*ab*cb*cc*dg*ff

Arkin, A. "Computers and the Audit Test." JOURNAL OF ACCOUNTANCY, October 1965, p. 44.

*(0350)*66*ab*cc*fy

"Are Your EDP Operations Insured?" MANAGEMENT REVIEW, August 1966; or MODERN OFFICE PROCEDURES, May 1966.

Insurance is available to cover losses to any or all hardware, and source data. Business interruption and business continuation coverage is also available.

*(0360)*67*ad*aj*cc*da*mb*nk*nm
Armer, Paul. "Social Implications of the Computer Utility." P-3642, RAND Corporation, Santa Monica, California 90406, August 1967.

This article is mostly concerned with privacy issues. There is a conflict between the individual's right to privacy and society's right to know. The author discusses a group of rules, safeguards, penalties, and remedies to insure that individuals and organizations will be able to maintain an appropriate level of privacy.

*(0370)*70*ab*cb*da*ed*gh*kg*mj
Astin, A. W.; and Boruch, R. F. "A 'Link' File System for Assuring Confidentiality of Research Data in Longitudinal Studies." AMERICAN EDUCATIONAL RESEARCH JOURNAL, 1970, pp. 615-624.

*(0380)*71*ab*da*db*hj
Astor, Saul D. "An Investigator Talks of Embezzlement and Robbery." THE OFFICE, September 1971.

*(0390)*68*aa*cc*dg*ff*kd*mc
AUDITING BANK EDP SYSTEMS. Bank Administration Institute, 1968.

*(0400)*72*ab*cc*ff
"Auditing Computer Systems." MANAGEMENT ACCOUNTING, September 1972, p. 26.

*(0410)*67*ab*cc*ff
"Auditing Fast Response Systems." EDP ANALYZER, June 1967.

*(0420)*65*aa*cc*dg*ff*kd
AUDITING WITH THE COMPUTER. University of California Press, Berkeley, California, 1965.

*(0430)*70*ab*dc*ge*jg*x1
"Automatic Fire Protection System Protects Continental's EDP Units." INSURANCE, 1 March 1970, p. 36.

Automatic fire protection systems can be adapted easily and inexpensively for older buildings. Continental Airline installed a CO2 extinguishing system which can detect and extinguish a fire within seconds without risk to personnel or damage to records. The system is also architecturally concealed.

*(0440)*67*ae*ag*cb*ed*ee*el*kb*lb*x1
Babcock, J. D. "A Brief Description of Privacy Measures in the RUSH Time-Sharing System." AFIPS CONFERENCE PROCEEDINGS, Spring Joint Computer Conference, Vol. 30, 1967, pp. 301-302.

The RUSH (Remote Users of Shared Hardware) system includes some 80 modules of processors operating in a time-sharing mode on an IBM System/360, model 50. Since IBM was not planning to implement security techniques in their early OS/360 distributions, the author decided to build protection software for the RUSH monitor using the basic facilities of data management processors in OS/360. Some of the protection devices are: a LOGON statement that includes master and sub-account identifiers, and a password; optional password protection for reading and modifying files; a Remote Job Entry mode that prescans all control language statements and file calls, and only allows a user to access his own files; the full OS/360 memory protection features; and no acceptance of assembly language programs. However, this article is largely obsolete and presents only simple, very basic protection schemes.

*(0450)*71*ae*ag*cb*da*db*de*ed*ej*gh*ho*hp*ka*lb*mf*x1
Baca, R. L.; Chambers, M. G.; and Pringle, W. L. "Automated Court Systems." AFIPS CONFERENCE PROCEEDINGS, Fall Joint Computer Conference, Vol. 39, 1971, pp. 309-315.

This article is primarily concerned with describing the Harris County Subject-in-Process System which is a completely automated remote-access criminal record system. A short section at the end of the article briefly describes privacy and security safeguards of the system. Some of these are: input routines that check for unreasonable input data; password protection for files; requiring that privileged modifications to the data take place at specific terminals during only certain periods of the day; and periodically creating backup tapes for storage at a remote location.

*(0460)*70*ac*ai*cc*mb
"Backround Information Provided on Data Banks." COMPUTERWORLD, 30 December 1970, p. 10A.

*(0470)*ac*ai*cc*fv*fz*x2
"Backup Contracts Call for More Thought Than Good Handshake." COMPUTERWORLD, 25 August 1971, p. 4.

Informal arrangements between users to use each others hardware in emergencies can lead to major problems. Determining who is liable if the backup system doesn't perform properly is highly dependent on the circumstances in each situation. Formal contracts are suggested as well as periodic checking to insure that hardware changes at the computer center or backup site haven't made the backup site unuseable.

*(0480)*71*ab*bg*hc*hd*hg*ia*ii*jc*je*lb*ne*nk*x2
Bacot, Eugene. "Trapping Data Bank Busters." BUSINESS ADMINISTRATION (Great Britain), January 1971, pp. 16-19.

The article is primarily concerned with data thefts by electronic and physical access of files. The author attempts to persuade the reader that current British computer security is appallingly low. He describes many risks that the security-lax user will be exposed to. Approximately fifteen actual theft, fraud, and disaster examples are given. The article doesn't discuss anything particularily new or unusual, but it may reduce the security apathy of some readers. No specific safeguards are recommended.

*(0490)*61*ad*cb*dc*jg*na
Baker, H. R.; Bolster, R. N.; and Leach, P. B. "Surface Chemical Methods of Displacing Water and/or Oils, and Salvaging Flooded Equipment: Part 6 - Field Experience in Removing Seawater Salt Residues From Aircraft Cockpits and AVIONICS Equipment." Report 5680, Naval Research Laboratory, Washington, D. C., 1961.

Some of the information in this report would be of help in salvaging flooded computer equipment.

*(0500)*67*ab*cd*dc*jg*na
Baker, H. R.; Leach, P. B.; Singleterry, C. R.; and Zisman, W. A. "Cleaning by Surface Displacement of Water and Oils." INDUSTRIAL AND ENGINEERING CHEMISTRY, June 1967.

Summarizes methods for removing oily coatings or water from electronic equipment.

*(0510)*71*ae*cb*el*gh
Baker, P. S. "CCBS 10/50 Monitor Cataloguer." DIGITAL EQUIPMENT USERS SOCIETY FALL SYMPOSIUM, Digital Equipment Corporation, Maynard, Massachusetts, November 1971, pp. 5-9.

The cataloguer provides security for its users by maintaining control over demountable storage media. The cataloguer monitors: allocation of demountable peripheral storage devices, device status, and generation and maintenance of volume labels. Two mount commands are available to supplement existing control mechanisms and to relieve the user of having to be aware of device availability.

*(0520)*73*ab*ah*cb*el*gh
Balzer, R. M. "An Overview of the ISPL Computer System Design." COMMUNICATIONS OF THE ACM, February 1973.

*(0530)*71*ab*cb*cc*cd*db*dc*fb*kb*kd*mc*x2

"Banks May Face Trouble with DP Disasters." DATA MANAGEMENT, May 1971, pp. 46-47.

This article quotes Jerome Lobel, vice president of Dataguard Systems, as saying, "Exposure of many banks to EDP disasters is increasing so rapidly that nothing short of a miracle will save some banks from financial catastrophe." Lobel believes a large percentage of exposed cases are kept secret. A systems approach is recommended where a careful evaluation is made in each of these areas: computer hardware, software and operations; physical security; and control of personnel. It is also recommended that the bank's board of directors be made aware of computer security problems, that one person be in full charge of security, that recovery plans be developed, and that exposed frauds be reported to the police and not be kept secret.

*(0540)*70*ab*cd*ga*ja*mc

"Banks Spending for Computer Security in the Wild West." INFORMATION WEEK, 12 October 1970.

West coast banks are upgrading their computer security programs. Money is mostly being spent on physical safeguards.

*(0550)*68*ab*ah*cc*dg*fb*ff*fz*f1*hc*hr*hs*kd*ma*nj*nk
*nn*x4

Banzhaf, John F. III. "When Your Computer Needs a Lawyer." COMMUNICATIONS OF THE ACM, August 1968, pp. 543-549.

Liability for negligence, torts (such as slander of credit), and expressed or implied warranties are discussed. Their legal complications are explained so that owners, operators, users, and lessors of computers may be alerted to potential legal problems. The article focuses on troublespots in contracting for EDP services, in deciding whether or not to automate certain operations, in automating financial records, and in complying with legal regulations of record keeping. Patent, copyright, and trade secret protection are discussed along with the problem of storing copyrighted material in computer information systems. Although the law on some EDP matters, particularly patents, has changed significantly since this article was written, this article is still extremely relevant and valuable. The article points out many legal pitfalls and safeguards that should be known by those responsible for EDP operations or for developing new systems.

*(0560)*67*ad*aj*cc*da*ka*mb*nl*nm

Baran, Paul. "The Coming Computer Utility: Laissez-Faire, Licensing or Regulation?" P-3466, RAND Corporation, Santa Monica, California 90406, April 1967.

The computer utility is discussed with respect to its growth and the environment that will support the growth. Future applications, economic pressures, and dangers of the utility are also discussed. The protection of privacy problem is considered and several regulatory mechanisms are described. Some future policy choices are analyzed. The article is somewhat out-of-date with current technology and policy choices.

*(0570)*65*ad*ag*aj*cb*cc*da*hd*ii*lb*ka*mb*nk*nl*nm*x2
Baran, Paul. "Communications, Computers, and People." AFIPS CONFERENCE PROCEEDINGS, Fall Joint Computer Conference, Vol. 27, Sect. 2, 1965, pp. 45-49; or P-3235 RAND Corporation, Santa Monica, California 90406, November 1965.

Full electronic-switching telephone networks of the future will provide very flexible and cheap communications. This will make computer information utilities and their interconnection much more economically justifiable. Personal privacy might be greatly threatened because it would be possible to obtain someone's employment, health, scholastic, legal, tax, etc. records from a computer terminal connected to the nearest telephone. The author suggests that security problems be considered now, before illegal access of computerized information becomes commonplace. Software patch-ups at a later date may be more costly and less effective than an initial good security design. The author believes that laws will be ineffectual. They have had little affect on eavesdropping, and government regulations will needlessly invade the privacy of the business sector. He proposes an open list of several safeguards such as cryptography for data transmission and storage, and auditing of data accesses and file operating programs.

*(0580)*64*ad*aj*cb*ep*eq*x1
Baran, Paul. "On Distributed Communications: IX. Security, Secrecy, and Tamper-Free Considerations." RM-3765-PR, RAND Corporation, Santa Monica, California 90406, August 1964, 39 pp.

This report is the ninth of an eleven part series detailing a proposed digital data communications system based on a distributed network concept and to be used by the military. The report, although quite valuable in 1964, is largely out-of-date with current cryptography techniques. Much of the report discussed detailed implementation techniques based on now obsolete hardware. The few still relevant parts of this report can be better understood by reading more current articles.

*(0590)*68*ad*aj*cc*fu*mj*ne*nm

Baran, Paul. "On the Engineer's Responsibility in Protecting Privacy." Report, RAND Corporation, Santa Monica, California 90406, May 1968.

This report states that computer systems could be designed to provide better security, but aren't because most safeguards are expensive. Since there is no organization enforcing a code of ethics among engineers, the engineering school curriculums must be modified to include courses on privacy and social responsibilities.

*(0600)*67*ad*aj*ba*cb*cc*mg*nm

Baran, Paul. "Remarks on the Question of Privacy Raised by the Automation of Mental Health Records." P-3523, RAND Corporation, Santa Monica, California 90406, April 1967.

The problem of privacy of medical health records for both personal and statistical purposes is discussed. Major changes in the use of medical records over the next twenty years are predicted, and the resulting privacy problems are considered. Medical information systems will become more integrated in the future, and adequate safeguards must be developed now so unmanageable privacy problems won't arise. Some examples of illegal access to medical records are given.

*(0610)*68*ac*cb*cc*cd*mb*ne

Barr, R. "Lack of Computer Security Held a Boon to Big Brothers." ELECTRONIC NEWS, 13 February 1968, p. 35.

*(0620)*70*ad*cd*dc*jg

Barritt, J. S. "Fire Protection for Computer Rooms." INSURANCE ACCOUNTING AND STATISTICAL ASSOCIATION, 1970.

*(0630)*67*ae*ag*cb*da*dd*de*ed*fv*gh*hr*lb*x2

Barron, D. W.; Fraser, A. G.; Hartley, D. F.; Landy, B.; and Needham, R. M. "File Handling at Cambridge University." AFIPS CONFERENCE PROCEEDINGS, Spring Joint Computer Conference, Vol. 30, 1967, pp. 163-167.

The authors describe in detail the file handling facility of the Cambridge University Titan computer. A file owner can extend some or all of seven privileges to one or more specified part owners. Privileges can be acquired by any non-specified individual who can quote an alphanumeric key specified by the file owner. A file user can be acting in one or all of these capacities: owner, part owner, key holder, and general user. All files are classified as either archives files, working files, temporary files, or system files. The eight million word disk storage is augmented with magnetic tape because of the limited disk storage, and to hold backup copies of files (copied every twenty minutes) in case of file destruction from system failures.

*(0640)*71*ab*cb*cc*da*db*ed*fs*hd*lb*x2
Bartram, Peter. "Software Security." DATA SYSTEMS, December 1971, pp.16-17.

Privacy and security issues, although related, are concerned with very different matters. Privacy involves moral and ethical questions, and security is concerned with purely technical safeguards. Computer security threats can be categorized by the techniques of abuse or by the level of organization required by the criminal to violate the system (accidental disclosure, unskilled casual entry, entry by skilled technician, ..., entry by organizations with massive funds). Five safeguards are recommended: computer staff given clear idea of professional standards expected of them, cryptography for remote transmission, system threat monitoring, password system for access control, and physical processing restrictions. The British Computer Society feels that an individual should have the right to see his files by paying only a small service fee to cover expenses.

*(0650)*70*ab*cb*cc*db*en*ff*fl*kb*kd*lb*nf*x3
Bates, Robert E. "Auditing the Advanced Computer Systems." MANAGEMENT ACCOUNTING, June 1970, pp. 34-37.

In most second generation computing systems, auditors were not concerned with initial EDP design and development. However, third generation systems will require auditor involvement from the initial design proposals through implementation and system testing. The responsibilities of the auditor should include: ensuring that no functional areas have been inadvertently omitted; reviewing system design (as it progresses) for completeness; determining that adequate measures are taken to insure appropriate documentation, debugging, and quality assurance; insuring documentation is complete and meets standards; insuring that there are adequate malfunction handling procedures; and examining the process of inputing and disseminating data. Several differences between second and third generation environments are also discussed.

*(0660)*70*ab*bg*cb*cc*cd*dg*ei*el*fb*fd*ff*fv*fx*fy*ga
*gg*hd*hu*ii*je*kd*lb*nb*nh*x3
Bates, William S. "Security of Computer-Based Information Systems." DATAMATION, May 1970, pp. 60-65.

The purpose of this article is to acquaint business managers with information system vulnerabilities, and to present a framework upon which an organization may build and develop to suit its specific requirements. An organization should ask itself: what would be the cost of replacement of current computerized data, are the assets accounted for by the EDP system safe from theft and fraud, are current, safely located backup files kept, do contingency plans exist, and what are the short term effects of files lost without backup? Several examples of actual computer crimes and disasters are given. The security framework views safeguards as providing the following rings of protection: (1) physical, hardware, and software safeguards; (2) backup files, documentation, and sites; (3) auditing and safeguard testing; and (4) insurance. A number of common physical, hardware, and software safeguards are briefly described. The author believes that top management involvement with security is essential.

*(0670) *72*ab*bg*cb*cc*cd*dg*ea*ec*ed*ei*el*eq*gg*hc*hg *ja*jd*je*jf*jh*lb*nh*nn*x3
Beardsley, C. W. "Is Your Computer Insecure?" IEEE SPECTRUM, January 1972, pp.67-78.

This article is a good summary of 10-20 other security articles. Fourteen examples of computer crimes and disasters are given. Joe Wasserman's and Willis Ware's frameworks for viewing computer security threats are described. A good discussion is given on the myths of magnetic tape vulnerability to magnets. Even the largest magnets must usually be placed within five inches of a magnetic tape to damage it, but small magnets can destroy tapes. Temperature and humidity are usually greater threats than magnetism. A discussion on electromagnetic monitoring claims that monitoring radiation from a distance greater than three feet is impractical in most situations. A good summary of numerous user identification techniques and their relative advantages is presented. A brief discussion (taken from Garrison's paper) is given on three different EDP cryptography techniques and their relative advantages. Some hardware and procedural techniques for insuring operating system and production program integrity are given. Finally, physical security considerations, threat monitoring, auditing, and personnel integrity are briefly covered.

*(0680) *67*ac*cb*cc*gg*ka*lb*md*nl*nm
Behrens, Carl. "Computers and Security." SCIENCE NEWS, 3 June 1967, pp. 532-533.

This article summarizes the AFIPS 1967-SJCC proceedings on computer security. The dangers of a proposed national databank and security problems peculiar to time-sharing systems are discussed. Lawmakers and the general public are becoming concerned with privacy issues. Federal regulations may be the result.

*(0690) *68*ae*cb*ep*gh*mh
Bellino, J. A.; Purzychi, A. Z.; Costello, L. B.; Dzierzawski, D. "RFI Suppression and Mil-Std-188B

Conversion of Model 28 Teletype Apparatus." PROCEEDINGS OF THE ELECTROMAGNETIC COMPATIBILITY SYMPOSIUM, 1968, p. 16-22.

*(0700)*70*ab*cc*da*f1*kb
Bendel, David. "Trade Secret Protection of Software." GEORGE WASHINGTON LAW REVIEW, July 1970, pp. 909-957.

*(0710)*66*ac*cc*da*hd*mc*md*nm
Bengelsdorf, I. S. "Computers Taking Over Tax Collection: Your Financial History Recorded on Tape." LOS ANGELES TIMES, 3 April 1966, Sect. A, p. 1.

The author briefly describes the upcoming computerization of the IRS. Questions are asked as to whether similar automation will occur in educational, military, medical, political, and employment fields. How will the privacy of personal information be protected?

*(0720)*72*ab*ah*al*cb*ec*ed
Bensoussan, A.; Clingen, C. T.; and Daley, R. C. "The MULTICS Virtual Memory: Concept and Design." COMMUNICATIONS OF THE ACM, May 1972.

This article will give the reader a clear understanding of why virtual memory is inherently safer than conventionally addressed memory.

*(0730)*71*ab*cd*dc*jg*mh*mi
Bentley, R. R. "Uninterruptible Power Supply Protected NASA Computer During Earthquake." COMPUTERS AND AUTOMATION, May 1971, p. 33.

The computer complex in NASA's Jet Propulsion Laboratory continued to aid returning Apollo 14 astronauts during one of California's strongest earthquakes.

*(0740)*70*ae*bc*cc*cd*jg*na
Berg, Philip J. "Data Center Disaster." GUIDE 30 PROCEEDINGS, GUIDE International Corporation, 1 Illinois Center, 111 East Wacker Drive, Chicago, Illinois 60601, 27 May 1970.

Mr. Berg tells how Applied Data Research survived a plane falling into its computer room.

*(0750)*70*ad*bc*cc*cd*jg*na
Berg, Philip J. "The Plane Facts About Data Accidents." APPLIED DATA RESEARCH INC., Princeton, New Jersey, May 1970.

How Applied Data Research survived a plane falling into its computer room is the subject of this article.

*(0760)*71*ac*ai*bc*cc*dc*fv*x2
Berg, Philip J. "User Tells How 'Lucky' Accident Brought

Awareness." COMPUTERWORLD, 30 June 1971, p. S6.

A burst water pipe taught a Washington data center a lesson about backup. The following list is proposed as the minimum requirements in order to minimize physical damage and expenses in case of a disaster: create backup files, provide safe storage for these files, test the backup system periodically, avoid program interdependancy, purge useless material but make absolutely sure it is useless, document procedures comprehensively, and try to make backup arrangements with a local facility having similar equipment. The author also states that the entire backup system could be automated.

*(0770)*72*ad*ca*cc*lb*nn*np*x3

Bergart, Jeffery G. "Computer Security, Access Control, and Privacy Protection in Computer Systems." Master's Thesis, Moore School of Electrical Engineering, University of Pennsylvania, Philadelphia, Pennsylvania, August 1972, 87 pp.

This a selected annotated bibliography of some 85 important works in the field of computer security. The bibliography is organized into the following sections: Privacy Protection and Access Control (general discussion, abstract models, working systems, and hardware protection); Computer Security (general discussion, cryptography, bibliographies); Business and Management Overview; and Social and Legal Implications. A majority of the articles are in the first section. Most of the articles are academic and research oriented. The annotations average 200 words in length but vary from 40 words to over 1000. The quality of the annotations also varies considerably. The author shows how one work is related to and influenced by other works, and this adds considerable value to the bibliography. This thesis should be very useful to computer engineers and systems designers, but its value to non-technical individuals is questionable.

*(0780)*72*ad*ca*cc*lb*nn*np*nz*x3

Bergart, Jeffery G.; Denicoff, Marvin; and Hsiao, David K. "An Annotated and Cross-Referenced Bibliography on Computer Security and Access Control in Computer Systems." AD-755 225, National Technical Information Service, Springfield, Virginia 22151, November 1972, 57 pp., $4.50.

This report is really Jeffery Bergart's master's thesis entitled "Computer Security, Access Control, and Privacy Protection in Computer Systems". The only differences between the report and the thesis are the title and purchase price. The thesis annotation summarizes the contents of this publication,

*(0790)*71*ab*cc*da*dc*fy
Bergman, H.W. "A Vital Records Security Program." BEST'S REVIEW: Life/Health Insurance Edition, September 1971.

*(0800)*71*ab*cb*cc*cd*fx
Berson, T. A. "Sleuthing Your Data Center." COMPUTER DECISIONS, June 1971, p. 6.

*(0810)*70*ac*ai*bc*dc*hg*mc*ne
"Best Data Sabotage Plan Wins." COMPUTERWORLD, 14 October 1970.

Two Harvard graduate students, upset by abuses of credit card companies and impersonal billing systems, are sponsoring a contest to devise the best method of destroying computerized information. The October 28 issue reported that the contest was cancelled due to lack of interest.

*(0820)*67*ab*cc*dc*dd*de*fz*ka*kd*ma*nl*nm*x1
Bigelow, Robert P. "Legal and Security Issues Posed by Computer Utilities." HARVARD BUSINESS REVIEW, September 1967, pp. 150-161.

The legal considerations of computerizing or not computerizing business operations, important considerations in writing a contract with an information utility, security of computerized files, likely privacy threats and regulation if various organizations merge their customer databanks, antitrust aspects of competitors using the same information utility, and future government regulation are all discussed. Unfortunately, most of this article is now obsolete. Some utility contract considerations are; who will own the developed programs; will documentation be supplied; will firm be protected against copyright infringement claims when using information supplied but not owned by the utility; how often can programs be updated; is program performance guaranteed; is the utility liable for delayed program development, what hours of the day will service be available; and is the utility liable if it loses the firm's records or fails to provide service because of a disaster.

*(0830)*68*ab*cc*fz*f1*nl
Bigelow, Robert P. Legal Aspects of Proprietary Software." DATAMATION, October 1968.

A survey of copyrights, patents, contracts, trademarks, and trade secrets is given. However, a large part of this article is now out-of-date.

*(0840)*69*ab*cc*dd*de*fz*hf*hi*ka*ma*mb*nj*nl*nm*x2
Bigelow, Robert P. "Some Legal Aspects of Commercial Remote Access Computer Service." DATAMATION, August 1969.

This article is largely an updated version of an earlier 1967 article by Bigelow entitled "Legal and Security Issues Posed by Computer Utilities" in the HARVARD BUSINESS REVIEW. However, this article tends to take more of a service bureau viewpoint. Its primary purpose is to review some of the legal problems which may arise in the establishment and operation of a remote access service bureau. Some of these problems are: ownership of developed programs, liability for continuous availability of service, warranty on database accuracy, guarantee of no illegal information access by other users, protection against users getting free computing time, civil suits by individuals whose private information was wrongly exposed, and possible future government regulations. A distinction is also made between computational and informational service bureaus. Some parts of this article are now outdated.

*(0850)*65*ad*cb*da*ec*ed*eh*ej*el*gg*gh*hd*lb*mh*nb
*x3

Bingham, Harvey W. "Security Techniques for EDP of Multi-Level Classified Information." RADC-TR-65-415, Rome Air Force Development Center, Griffis Air Force Base, New York; or AD-476 557, National Technical Information Service, Springfield, Virginia 22151, December 1965, 195 pp.

This is the final report of an eight month study by Burroughs Corporation for the U.S. Air Force. The report is essentially a very detailed and highly technical description of a proposed multiprogramming, multiprocessing, time-shared computer system designed to concurrently process multi-level classified information. The study and report did not consider long distance communications problems and cryptography. The system was to be implemented on a Burroughs D825 computer.

Some of the recommended hardware safeguards include: dual mode processors with privileged instructions; system interrupt required to enter the control mode; flag bits for control of memory words; address checks against access-differentiated memory bounds; parity checks on intermodule data transfers; I/O processors that verify connections, check memory addresses against bounds, and confirm security classification of record headers; physical keys needed for terminal operation; bulk file control of physical record integrity; lock control over write permission; and flag bit setting to permit supervisor establishment of control programs. Some recommended software safeguards are: checking of access requests against user security profiles, verification of memory bounds and blanking, redundant programming, and monitoring/logging of job execution and I/O operations. An analysis is made of the cost of software protection in terms of additional instructions and executions, and of hardware protection in terms of "equivalent flip-flops". Tables exist for all the hardware and software techniques considered.

This report is somewhat out-of-date, but is still worth reading by those concerned with designing secure computer systems.

*(0860)*69*ab*cc*fc*ff*fg
Binns, James. "Why Man to Man Defense for EDP Audit Control?" DATA MANAGEMENT, October 1969.

The need for cooperation between the programming and auditing departments is discussed.

*(0870)*70*ac*ai*cd*dd*gd*jh
"Blackouts Inevitable." COMPUTERWORLD, 2 September 1970, p. 1.

*(0880)*71*ab*cd*dd*gd*jh
Blumenthal, F. "Do You Love Your Computer? Keep It Warm." PARADE, 4 April 1971, p. 24.

The need for backup power sources is discussed.

*(0890)*63*ab*cc*ff*kd*la
Boni, Gregory M. "Impact of Electronic Data Processing on Auditing." THE JOURNAL OF ACCOUNTANCY, September 1963.

This article discusses EDP auditing procedures before the time-sharing era. Although the article is out-of-date, parts of it are still valuable.

*(0900)*70*ae*cb*ea*ed*ef*lb
Booth, D. F. "File Security for a Shared File, Remote Terminal System." CONFERENCE ON COMPUTERS: PRIVACY AND FREEDOM OF INFORMATION, Queen's University, Kingston, Ontario, Canada, May 1970.

*(0910)*70*ac*ai*bb*db*hl*hm*ii*mh
"Bootleg Bribe Buys Computer Time." COMPUTERWORLD, 30 September 1970.

A civilian bribed a government employee with a few bottles of liquor to obtain a run on a secret Pentagon computer.

*(0920)*72*ae*ag*cb*db*dd*ei*gh*ht*lb*ng*x3
Borgenson, Barry R. "Dynamic Confirmation of System Integrity." AFIPS CONFERENCE PROCEEDINGS, Fall Joint Computer Conference, Vol. 41., 1972, pp. 89-96.

This paper is concerned with techniques for detecting computer system malfunctions. It is quite technical and requires a good understanding of computer technology to be fully understood. Concurrent confirmation of a system's integrity means that the integrity of the system is being monitored concurrently with each use. Dynamic confirmation of a system's integrity identifies parts of the system that must have continuous integrity, and the integrity of the rest of the system is then confirmed only periodically.

For a general-purpose, time-sharing system, the method of checking processors non-concurrently is very powerful because simple, relatively inexpensive schemes will suffice to guarantee the security of a user's environment. The disadvantage of dynamic confirmation is that some faults that could contaminate a user's information may not be detected. The dynamic confirmation concept has its most applicable use in design of fault-tolerant systems. Fault-tolerant systems are designed using a "solitary fault" assumption, and a large part of this paper is devoted to showing this assumption is viable. The last half of this paper describes in detail the integrity confirmation features of the University of California "PRIME" computing system which has 5 processors and 13 memory blocks.

*(0930)*69*ad*cc*da*ka*mj*nm

Boruch, Robert F. "Eduation Research and the Confidentiality of Data." ACE Research Reports, Vol. 4, No. 4, 1969.

Privacy issues related to the "ACE" databank which stores biographical data on college freshmen are discussed.

*(0940)*71*ab*cb*da*hd*kb*kg*mj

Boruch, Robert F. "Maintaining Confidentiality of Data in Eduational Research: A Systematic Analysis." AMERICAN PSYCHOLOGIST, May 1971, pp. 413-430.

*(0950)*72*ae*ag*cc*da*de*eh*eq*fh*fj*hd*he*ls*ka*mb*ng
*nl*nm*x3

Boruch, Robert F. "Security of Information Processing: Implications From Social Research." AFIPS CONFERENCE PROCEEDINGS, Fall Joint Computer Conference, Vol. 41, 1972, pp. 425-433.

Many social research programs are characterized by stringent requirements that identifiable data collected on the subjects of research be kept confidential. The increasing number of sensitive and controversial research efforts have caused social researchers to become increasingly interested in legal, administrative, and technical safeguards. This paper discusses in detail some security problems and safeguards in social research which are relevant to information processing activities. The author suggests that a rough continuum of computerized personal record databanks be considered. At one end is an "auditing function" where identifiable records serve as a basis for making evaluative judgments about an individual. At the other end is the "research function" where the records serve as a basis for appraising a group's condition with respect to some social theory. Security requirements will vary along this functional continuum. Some of the safeguards used by social scientists are: physical separation of identifiers and statistical data into separate files with each file having code numbers that are matched to the other file code numbers through a secret cross-reference dictionary; introducing random errors into the personal records without jeopardizing the integrity of the total data for statistical use; and using remote terminals or having the respondent punch his responses out on a special card to reduce the number of personnel who must handle the input data. The author feels that a national data registry and development center would be of significant value in reducing redundancy in collection and maintenance of data and in providing the researcher with information on the likelihood of privacy problems. Some security areas in need of future research are briefly suggested.

*(0960)*72*ab*cc*da*he*mj
Boruch, Robert F. "Strategies for Eliciting and Merging Confidential Social Research Data." POLICY SCIENCES, September 1972, pp. 375-397.

*(0970)*71*ab*cb*cc*cd*dg*eq*ff*fq*fv*hd*hq*hr*lb*x1
Bournazos, Kimon; and French, Norman E. "Information Management and Privacy in Business." DATA MANAGEMENT, July 1971, pp. 18-23.

First, a brief discussion is given on safeguards for natural disasters, fraud, and sabotage. A few examples are then presented which indicate sophisticated EDP auditing methods will be able to perform audits far better than those now performed by manual checks. The following causes for human error are given: monotonous work, poor lighting, glaring work surface, improper seating, crowded working areas, inadequate ventilation, and poor temperature control. Some examples of company confidential files are: market research data, company business plans, pricing intentions, future projects, and employee personnel records. The last half of this paper briefly describes some cryptography methods and presents a specific method for implementation.

*(0980)*65*ab*cc*ff
Boutell, Wayne. "Auditing Through the Computer." JOURNAL OF ACCOUNTANCY, November 1965, pp. 41-47.

*(0990)*65*aa*cc*dg*ff*kd
Boutell, Wayne. AUDITING WITH THE COMPUTER. The University

of California Press, Berkeley, California, 1965, 181 pp.

This is one of a small number of books that deal with the relationship between the CPA and the computer.

*(1000)*66*ab*cc*ff
Boyle, E. T. "What the Computer Means to the Accounting Profession." JOURNAL OF ACCOUNTANCY, January 1966, pp. 56-67.

*(1010)*72*aa*dg*ha*lb
Bradley, John. THE VULNERABILITY OF THE DIGITAL COMPUTER. Looseleaf, National Computer Research Institute, Washington, D. C., 1972, $140.00.

*(1020)*64*ab*cc*fm
Brandon, D. H. "Computer Operations Standards." COMPUTERS AND AUTOMATION, September 1964, pp. 32-36.

*(1030)*73*ab*cb*dg*ec*ed*ee*ef*ei*el*em*en*fi*ha*hi*hm *ng*ni*x3
Branstan, Dennis K. "Privacy and Protection in Operating Systems." COMPUTER: Magazine of the IEEE Computer Society, January 1973, pp. 9-17.

This article summarizes the discussions presented at an IEEE workshop on privacy and protection in operating systems. The workshop was held in Princeton, New Jersey on June 12-14, 1972. The following topics were discussed in detail: designing a secure operating system on present hardware, designing new hardware protection facilities, weaknesses of current systems' protection features, and methods of continually monitoring a secure system. Dennis Tsichritzes discussed the University of Toronto's Project SUE, a two year effort to implement a secure operating system on an IBM 360 computer. He also presented an interesting list of twelve unresolved questions concerning secure operating system design criteria. James Anderson and Daniel Edwards studied several current operating systems and discussed the following threats: clandestine code changes, residue, incomplete parameter checking, security bypass mechanisms, asynchronous input/output, user interrupts, and "Trojan Horse" attacks. Michael D. Schroeder discussed the "memoryless subsystems" and "mutually suspicious cooperating subsystems" protection problems. C. V. Srinivasan presented his framework for a theory of protection. The Cambridge University protection mechanism, the University of California's PRIME Project, and MIT's MULTICS system hardware protection were also discussed. A few conclusions reached from other presentations are briefly stated below. Security "add-on" packages, password systems, audit trails, output labeling, and single access controls all offer some

protection, but could be easily bypassed by clever programmers. Protected restart capability and dynamic reconfiguration of hardware after "soft" system failures are mandatory for good protection. Users should have a decision on how to protect their information.

Another workshop on social issues, physical protection, and methods of user verification was held during December 1972.

*(1040)*71*ab*bb*bc*da*db*dc*ga*gf*ii*jf*jg*x1
Bray, Melvyn. "How Safe Is Your System?" DATA SYSTEMS, December 1971, pp. 12-15.

This article briefly discusses some computer threats and appropriate countermeasures. Some considerations in implementing a fire prevention program are presented. Several different types of burglar alarms are also briefly described. Finally, computer bombings, fraud, and illegal data access by remote terminal are mentioned.

*(1050)*70*ab*cc*da*f1*hc*x2
Breyer, Stephen. "Uneasy Case for Copyright: A Study of Copyright in Books, Photocopies, and Computer Programs." HARVARD BUSINESS REVIEW, December 1970, pp. 281-351.

When this article was written Congress was considering a major expansion of the 1909 copyright act. Proposals before Congress to lengthen the copyright protection period and increase its scope in the areas of computer programs and photocopying are considered in length. The author concludes that: the current copyright period is too long; making single xerox copies of magazine articles or extracts from books should be legalized; small groups should be able to store copyrighted material in computers for research purposes; and computer programs should not receive copyright protection. Pages 340 to 350 demonstrate that computer program copyright protection is largely worthless for the majority of system, application, and general purpose programs. However, some of the arguements used against copyright protection may now be invalid.

*(1060)*68*ad*cc*da*fe*fh*fj*fk*hd*nh*nm
Brictson, R. C. "Some Thoughts on the Social Implications of Computers and Privacy." SP-2953, Systems Development Corporation, 2500 Colorado Avenue, Santa Monica, California 90406, 14 March 1968.

This article discusses: the public's fear of computers, a framework for inquiry into the privacy problem, responsibilities of business and government for insuring privacy, examples of computer privacy issues, and recommendations for improving privacy of computerized information. The framework considers information from the following viewpoints: acquisition, access, dissemination, retention, revision (updating, rejoinder, and redress), destruction, and time cycles. A professional code of ethics is proposed. It is recommended that databank owners be required to specify the databank's benefits, potential risks, safeguards, countermeasures, penalties, and sanctions.

*(1070)*72*ac*ai*cb*cc*cd*dg*nf*ng*nh*ni*nm*x4
Bride, Edward J. "AFIPS System Certification Would Help Protect Public." COMPUTERWORLD, 5 April 1972, p. 1.

AFIPS has started a program to establish recommended "system review procedures" for large-scale computing systems. The first system review manual will deal with security and privacy issues. It was to be drafted in late 1972 and tested in early 1973. This manual will establish checklists for users and designers to follow, and is likely to be divided into three sections concerning: ideal concepts, questions to ask, and mistakes or consequences to avoid. Later manuals will cover topics such as: operational audits, performance reviews, acceptance tests, system reliability, and data collection. Overall system certification is one long-range goal of this program.

*(1080)*71*ac*ai*cc*cd*dc*fw*jg*x3
Bride, Edward J. "After the Fire, Where Do You Put the New System?" COMPUTERWORLD, 13 October 1971, p. 1.

The contingency plan for disaster should include a recovery location that could be used at least temporarily. Checks should be made to insure that this recovery location has sufficient electrical power, air conditioning, working space, physical security, and user convenience. The fire protection plan should include the following steps: prevention, detection, shutting down procedures if sufficient time is available, personnel evacuation, and fighting the fire. Several specific "shutting-down" considerations are listed.

*(1090)*70*ac*ai*be*cc*de*ff*hr*kd*me
Bride, Edward J. "Audit Trails Lost in Computerization." COMPUTERWORLD, 29 April 1970.

Daytona Beach, Flordia computerized its records but did not allow for sufficient information to be printed out. Audit trails were not possible, and a complete audit could not be performed.

*(1100)*71*ac*ai*bb*be*cc*hk*hp*hv*ka*la*me*mf*x2
Bride, Edward J. "Bad Imput Causes Court Errors." COMPUTERWORLD, 13 October 1971, P. 1.

A Philadelphia computer information system that automatically sends warnings, warrants, or summons to persons having received traffic violation tickets has been plagued by file updating delays, data input errors, and data input fraud.

*(1110)*71*ac*ai*ba*fv*jc*mc*x2
Bride, Edward J. "Bank's Tapes Stolen for Ransom." COMPUTERWORLD, 20 October 1971, p. 4.

$1.8 million in cancelled checks plus two reels of magnetic tape were stolen in a shipment between two Bank of America offices. The robbers offered to return the checks and tapes for ransom but backup tapes foiled thier plan.

*(1120)*71*ac*ai*dc*dd*de*fw*mc*ne*x2
Bride, Edward J. "Businesses Not Security-Conscious." COMPUTERWORLD, 12 May 1971, p. 1.

The proceedings of the American Bankers' Association Automation Conference are briefly summarized. Only 60 of the 1,500 people present attended a security session, and only half of these attendees had, or were developing, a formal disaster recovery plan. The frequencies of occurrence of various security problems were said to occur in the following descending order: human errors, power failures and brownouts, hardware failures, civil disorders, and fires. "Conversion fiascos" were said to be the major source of long-range problems.

*(1130)*71*ac*ai*bd*cd*gd*jh*me*x2
Bride, Edward J. "City DPers Seek Power Crisis Funds." COMPUTERWORLD, 7 April 1971, P. 1.

The New York city government may be forced to spend millions of dollars to protect its computing equipment from frequent electrical power reductions and failures. Adequate power is essential for some operations like the police departments' SPRINT dispatching system.

*(1140)*73*ac*ai*cc*dg*fc*ff*kd*x1
Bride, Edward J. "Auditor-DPer Cooperation 'Only Way' to Prevent Fraud." COMPUTERWORLD, 13 June 1973, p. 10.

Reeling from criticism surrounding the recent Equity funding scandal, auditors called on their colleagues to participate in computer systems design, and demanded similar action from their DP counterparts. Paul Ton, a consultant with Arthur Anderson & Company, believes that the DP manager should assume the role of the auditor. This would assure better systems design, and the increased communication between departments would reduce distrust. DP technicians should ask auditors what controls they want implemented to assure qood security. Thomas Samson, partner with Arthur Young & Company, claimed that DP managers, not auditors, are responsible for control procedures. This article gives the impression that auditors want more involvement from DP personnel so that they can avoid having to learn more about computer systems.

*(1150)*71*ac*ai*bb*bd*db*dd*fi*hv*mk*na*x2
Bride, Edward J. "Critique of Detroit Fiasco: ACM Releases DP Voting Report." COMPUTERWORLD, 20 October 1971, p. 1.
This article briefly summarizes the contents of a guide by ACM on avoiding problems likely to occur in switching to computerized voting systems. The guide is based on an ACM investigation of the delays and discrepancies in the 1970 Detroit elections. No feasibility study was performed before computerizing Detroit's voting system; equipment ran at about 10% of capacity; and organized conspiracy could not be ruled out. The public's apathy on this matter caused ACM to do the investigation.

*(1160)*70*ac*ai*bc*bd*dc*dd*jf*me
Bride, Edward J. "DP Center Invaded." COMPUTERWORLD, 15 July 1970, p. 1.
The Massachusetts State Welfare Office was invaded by unhappy welfare recipients who claimed the computer was responsible for check distribution delays. The invaders left after a three hour seige of the computer center. No damage was done.

*(1170)*71*ac*ai*cd*dc*ge*jg*x2
Bride, Edward J. "DP Centers Find New Fire Extinguishing Agent System." COMPUTERWORLD, 10 March 1971, p. 6.
Halon 1301 is becoming a popular fire extinguishing agent. Unlike carbon dioxide, Halon 1301 has a low toxicity so personnel need not be evacuated during a fire. Either smoke detectors, thermal switches, or temperature-increase devices can be used to cause release of the extinguishant.

*(1180)*71*ac*ai*cc*dg*fz*ma*nj*x1
Bride, Edward J. "Few Rules on Software Liability Said to 'Frustrate' Users, Hamper Contracts." COMPUTERWORLD, 26 May 1971, p. 6.
Poor performance of software is making it difficult to fit the liability of software suppliers into today's legal system. There are very few specific rules regarding software liability. It is suggested that contracts be written so both sides will know their legal liabilities. A user must expect to pay for the protection he receives from a contract.

*(1190)*70*ac*ai*cb*cd*da*db*dc*gf
Bride, Edward J. "Firms Offer Card, Key Systems for Data Security." COMPUTERWORLD, 26 August 1970.
Key reader devices are described which can limit

access to the computer room or limit control of the computer to operators possessing a properly coded plastic key.

*(1200)*72*ac*ai*cb*cc*ng*ni*x2
Bride, Edward J. "FJCC Explores Data Protection." COMPUTERWORLD, 6 December 1972, p. 1.

Committees, agencies, societies, and corporations will all be taking advantage of the AFIPS Fall Joint Computer Conference by presenting reports on the problems of data security. A working session will discuss a 300-400 item questionnaire for judging a system's security. Overlapping efforts of other organizations are viewed as beneficial.

*(1210)*73*ac*ai*cb*dg*ed*fb*gh*ng*x2
Bride, Edward J. "IBM, Security Test Sites Vie on Software Strength." COMPUTERWORLD, 13 June 1973, p. 1.

This article describes the highlights of three security sessions at the 1973 National Computer Conference. Although the first results of IBM's five year, $40 million security study won't be available until next spring, some preliminary results were discussed. It was suggested that the IBM Resource Security System (RSS) will cost users about two percent in overhead costs. But an official from one of the four test centers said the security software degraded response time anywhere from eight to twenty-five percent. However, IBM has no plans to make RSS available as a product or free package. RSS is installed at all of the sites in an operational mode, rather than in a test or research environment. Two known "holes" continue to exist in the RSS software, but TRW, one of the test sites, has managed to plug 108 weak spots.

Richard Mills of First National City Bank suggested that the discussion on security was too technically oriented, and should instead focus on auditing, planning, monitoring, and physical controls. He asked, "Are we building steel doors in paper walls?" Dr. Edwin Golding of the U.S. Treasury Department stated that the weakest link in a secure system is the employee who can be compromised. Several other panel members agreed with Golding's statement. Peter Browne of State Farm Mutual stated that computer users and manufacturers both have responsibilities in solving security problems. The user responsibilities include: security awareness, risk management, management control, physical security, and auditing. Several security checklists were also presented.

*(1220)*72*ac*ai*cc*dg*fy*hf*hg*lb*x3
Bride, Edward J. "Insurance May Be Cheaper Than Security."

COMPUTERWORLD, 6 September 1972,p. 3.

A group of computer security experts feels that users of time-shared systems may find it cheaper to insure their data than to protect it by developing software safeguards. It's noted that current safeguard techniques can not insure good protection from a malicious penetrator. Unintentional disclosure of information is occurring less frequently. Some members felt that building new safeguards into systems is the proper next step, while others felt that correct implementation of currently available techniques would be sufficient. It was noted that most users aren't aware of their security requirements.

*(1230)*71*ac*ai*cc*dg*fy*fz*ma*mb*x2

Bride, Edward J. "Lawyer's Warning: Let Customer Beware in Computer Contract." COMPUTERWORLD, 13 January 1971, p. 1.

Many service bureaus attempt to have their customers sign contracts that free the service bureau from liabilities resulting from: processing errors, incomplete utility programs, delays in processing, and even negligence. Most service bureaus can obtain insurance against lawsuits, but they usually pass the cost onto customers requiring legal protection. The cost of insurance protection may be justifiable, especially for users located in areas where only one bureau is economically available.

*(1240)*71*ac*ai*ba*da*ha*ii*lb*ma*nj*x2

Bride, Edward J. "Milestone Near in Program Theft Case." COMPUTERWORLD, 21 July 1971, P. 4.

A former Information Systems Design employee faces trial for allegedly tapping that firms computer over telephone lines to steal a plotting program valued at $15,000 to $25,000. The program was needed to win over an Information Systems Design customer to the defendant's new employer.

*(1250)*72*ac*ai*cc*da*fh*fj*hd*ka*mb*nl*nm*no*x3

Bride, Edward J. "NAS Warns of Despair in Privacy Invasion Fight." COMPUTERWORLD, 25 October 1972, p. 4.

This article reviews a 500 page National Academy of Sciences report written by Alan Westin and Michael Baker. The report firmly states the need for databank controls, but also claims that the privacy problem is not as bad as most civil libertarians believe. 55 organizations with highly advanced computer applications were studied. It was learned that in most cases computerization of personal files has not yet resulted in significantly greater privacy intrusion. Most companies still rely on paper files for sensitive information storage. However, the computerized files were receiving more extensive use, and some files would not have been feasible without use of the computer. The authors warn that today's worst danger is the public's attitude that the fight for a reasonable personal privacy/public need-to-know relationship has been lost. The report predicts increased ease of data sharing among organizations, and recommends several laws and regulations be implemented.

*(1260)*73*ac*ai*cb*cc*cd*dg*mh*x1
Bride, Edward J. "Navy Users Told 100% Security Unreachable." Computerworld, 16 May 1973, p. 1.

Commander Jan Prokop, director of the ADP Equipment Selection Office in the Navy Department, told those attending The Fifth Annual Data Processing Seminar, of a joint Navy user group, that 100% secure computer systems will probably never be developed, and users should spend their money where it will do the most good in particular situations, such as physical access control and security clearances for personnel. He also described the following remote access threats first developed by H. E. Peterson and R. Turn: browsing, masquerading, trap doors, between-the-lines entry, and piggy-back entry.

*(1270)*71*ac*ai*bd*cd*dd*gd*jh*x1
Bride, Edward J. "New Brush With Power Mess, DP Users Without Backup Lucky." COMPUTERWORLD, 25 August 1971, p. 1.

Some computer users have indicated that they have lost files during prior power brownouts and failures, but luckily the lost files were not of critical importance. Significant voltage fluctuations can cause dropped bits of information, loss of data in core, or even physical damage to the computer. Two voltage monitors for computers are commercially available. IBM's 370 series has a voltage regulator in its hardware which protects against short fluctuations in voltage. Most computers have an automatic power-down feature to protect hardware circuits when line voltage gets too low.

*(1280)*72*ac*ai*cc*he*md*nm
Bride, Edward J. "Panel Warned of SS Number Trend." COMPUTERWORLD, 30 August 1972, p. 1.

The Department of Health, Education, and Welfare is studying the implications of a trend toward the use of the social security number as a universal identifier.

*(1290)*70*ac*ai*bc*cd*dc*fv*ga*hi*jd*md*x2
Bride, Edward J. "Radar Wipes Out IRS Tapes: Consultant Cites Poor Ground." COMPUTERWORLD, 30 December 1970, p. 1.

Thousands of tax records were erased by an airport radar that was located within 200 yards of a new IRS computer center. Significant amounts of information were forever lost because many destroyed files had no backup.

*(1300)*71*ac*ai*bd*cd*dd*gc*gd*jh*x1
Bride, Edward J. "Stoppages Beset Dartmouth T/S." COMPUTERWORLD, 3 February 1971, P. 1.

The Dartmouth Time Sharing System was inoperative for two days because no power supply testing device was available. A spare power supply was incorrectly wired. Voltage transients were introduced into the system when this spare power supply was tested. Dozens of integrated circuits were destroyed.

*(1310)*71*ab*bb*db*fh*if*ka*mc*nm*no*x1
Brooke, Phillip. "Protection of Privacy Vital in any Improved Bank Computer Program." AMERICAN BANKER, 6 May 1971, p. 1.

This article reviews a National Academy of Science's project headed by Alan Westin. For a Review of the 500 page final report on this project see "NAS Warns of Despair in Privacy Invasion Fight," by Edward Bride in the October 25, 1972 issue of COMPUTERWORLD. Westin studied 55 different organizations for this project, including three banks. He claims that banks keep personal data on marital stability, drinking habits, expenditures, and sexual preferences. When some New York banks were recently legally blocked from getting access to personal arrest records, they engaged in bribing police officers to get the information. However, banks were not found to be collecting more personal information for computerized files than they kept for paper files.

*(1320)*72*ab*cc*ff*ni
Brown, H. L. "Auditing Computer Systems." MANAGEMENT ACCOUNTING, September 1972, pp. 23-26.

The article contains a questionnaire for determining the usefulness of computer generated reports.

*(1330)*69*ab*cc*ff
Brown, H. L. "Current Problems of Real-Time Auditing." MANAGEMENT ACCOUNTING, May 1969, pp. 53-54.

*(1340)*68*aa*cc*dg*ff*kd
Brown, H. L. EDP FOR AUDITORS. John Wiley and Sons, 1968.

*(1350)*71*aa*cb*cc*cd*eo*fk*fq*fr*fv*np
Brown, William F. (ed.) COMPUTER AND SOFTWARE SECURITY. Advanced Management Research International Inc., 280 Park Avenue, New York, New York 10017, 1971, 208 pp., $29.50.

This book essentially contains the proceedings of AMR's seminar on computer security. Physical security, implementing a security program, legal matters, backup, insurance, auditing, software safeguards, and cryptographic techniques are all covered in varying levels of detail. A bibliography is also included.

*(1360)*72*ab*cb*cc*cd*dg*fy*gg*nb*nf*x3
Browne, Peter S. "Blueprint for Computer Security Drawn by State Farm Specialist." THE NATIONAL UNDERWRITER: Property and Casualty Insurance Edition, 16 June 1972, pp. 47-49.

A six step methodology for implementing a computer security program is given. The six steps are: (1) determine the configuration of hardware and software, list and flowchart the major processing tasks, and list the current operation and control procedures; (2) determine the value of equipment, media, and documentation; (3) perform a "threat analysis" by trying to find all possible risks to your installation; also determine for each major file the cost to your company if that file was destroyed, disclosed, or modified; (4) set specific requirements for the protection of data, programs, and other assets, and for the timeliness of each major task; (5) estimate the cost of reducing the current level of vulnerability; and (6) select a set of economical and effective safeguards.

Any company, no matter how small, should have at least one person responsible for data processing security. Top management support is also necessary. It would be wise for a company's security personnel to visit other EDP installations before attempting to design their own program. Five protection strategies are given. They are: isolation (passwords, guards), encryption, deterrence (auditing, system monitoring), insurance, and delegation (using a service bureau). Use of insurance is best where adequate protection is very expensive and the threat probability is very low.

*(1370)*72*af*cb*cc*lb*np*nn*x4
Browne, Peter S. "Computer Security - A Survey." DATABASE: Quarterly Newsletter of ACM's Special Interest Group on Business Data Processing (SIGBDP), Vol. 4, No. 3, Fall 1972, pp. 1-12.

This article contains an excellent 4 page introduction on various aspects of computer security. The introduction discusses where the current state-of-the-art lies; what is most commonly being done in practice; and what needs to be done in the near future. The following security topics are also briefly mentioned: definitions of security, privacy, and integrity; batch versus time-sharing environment; user identification and authorization; the security 'objects' (people, data, etc.) of a system; system monitoring; cryptology; designing security into the computer versus implementing security controls outside the computer; need for classification of threats; recovery plans; security checklists; existing systems; and future areas of research.

A partially annotated bibliography of 228 articles follows the introduction. The articles in this bibliography cover almost every aspect of computer security. Some are highly technical while others are very basic and non-technical. A large number of these articles are from symposiums, workshops, and conferences of the ACM. Many other articles are from nebulous publications that wouldn't normally be found without a good deal of searching. Several valuable books are also included. As of January 1973, this was probably the best and most comprehensive computer security bibliography. Unfortunately, only part of the bibliography is annotated, and most annotations are quite brief. The author often did not supply enough publication information to enable the reader to easily obtain a desired article.

*(1380)*71*ae*cc*da*db*gg*nm*nn

Browne, Peter S. "Data Privacy and Integrity: An Overview." ACM Special Interest Group on File Description and Translation (SIGFIDET) Workshop, 11 November 1971.

This article is the predecessor to "Computer Security - A Survey" by Browne.

*(1390)*71*ae*cb*ee

Browne, Peter S.; and Steinauer, Dennis. "A Model for Access Control." ACM Special Interest Group on File Description and Translation (SIGFIDET) Workshop, 11 November 1971, pp. 241-262.

The file authorization problem is discussed, and a conceptual model based on the work of Weissman is developed. The authors believe that Friedman's compartmentalization scheme for grouping data with similar access restrictions, Graham's hierarchical classification scheme using concentric rings, and Lampson's domain mechanisms for grouping capabilities of objects are not satisfactory solutions to the access control problem.

*(1400)*65*ab*cb*cc*gg

Buckley, John L. "Computers, Automation, and Security." LAW AND ORDER, March 1965.

*(1410)*65*ab*cb*cc*dg*mf

Buckley, John L. "The Future of Computers in Security and Law Enforcement - Part 1." LAW AND ORDER, August 1965, pp. 36-38.

The advantages and disadvantages of using computers as security devices or in law enforcement are discussed. Future applications and the security problems which result from using computers are examined.

*(1420)*65*ab*cb*cc*dg*mf
Buckley, John L. "The Future of Computers in Security and Law Enforcement - Part 2." LAW AND ORDER, September 1965, P. 48.

The advantages and disadvantages of using computers as security devices or in law enforcement are discussed. Future applications and the security problems which result from using computers are examined.

*(1430)*00*ae*cd*dc*jg
"Burning Facts." SAFE MANUFACTURERS NATIONAL ASSOCIATION, 366 Madison Avenue, New York, New York 10017.

This is a brochure defining the specifications of safes used to protect various non-paper computer I/O media.

*(1440)*71*ac*ai*cc*cd*gg
"Burns Takes Security Seriously." COMPUTERWORLD, 13 January 1971, P. 14.

*(1450)*70*ab*cc*cd
Burt, K. H. "Computer Center Security, Protecting the Achilles Heel." BANK ADMINISTRATION, April 1970, pp. 36-39,

*(1460)*69*ad*ca*ea
Busch, G. E. "Applications of Electro-Optical Fingerprint Correlators." PROCEEDINGS OF CARNAHAN CONFERENCE ON ELECTRONIC CRIME COUNTERMEASURES, University of Kentucky, Lexington, Kentucky, 1969, pp. 90-97.

*(1470)*70*ad*cb*da*el*he*mh
Bushkin, A. A. "A Technical Context for Multi-Level Security in a Multiplexed Computer System." SEMINAR ON PRIVACY: LEGAL AND TECHNICAL PROTECTION IN THE COMPUTER AGE, October 1970, 12 pp.

Basic requirements for a secure system are described. Some of these requirements are: program readable hardware configuration status switches; known responses for all possible operation codes; and need-to-know lists for each file. The problem of constructing top secret information from reading only secret information is then examined. Finally, ten design guidelines for a monitoring system are proposed.

*(1480)*73*af*cc*np*x2
BUSINESS PERIODICALS INDEX. The H. W. Wilson Company, New York, New York, 1958-, (Monthly, with annual cumulations

every June).

This is a cumulative subject index to English language periodicals in the fields of accounting, advertising, public relations, automation, banking, communications, economics, finance, insurance, labor, management, marketing, taxation, and trades. The desired articles can be found under the subject index "Computers - Security Measures". Each annual cumulation contains about 2,000 entries on computers and electronic data processing, and about 25 on computer security measures. Most of the security entries are concerned with management controls and operating procedures. These entries are typically from sources such as THE OFFICE, BUSINESS HORIZONS, BANKING, DATA MANAGEMENT, DATAMATION, BUSINESS WEEK, FINANCIAL EXECUTIVE, HARVARD BUSINESS REVIEW, and ELECTRONIC NEWS.

*(1490)*69*ac*cc*da*hd*ii*x2

"Business Spies Still Busy." INTERNATIONAL MANAGEMENT, June 1969, pp. 58-59.

The major focus of business espionage has shifted from trade secrets to mergers and acquisitions. Drug, chemical, and financial companies are particularly vulnerable. Estimated U.S. espionage losses are 2 to 5 billion dollars annually. Some of the types of information business spies attempt to obtain are: who owns the target-company stock, where do they live, what has been the stock's trading pattern, past business deals, personal grudges among management, management weaknesses, and the company's countermeasure plans to prevent takeover. The weakest part of most company security systems are the employees. One company found that more than 10% of its engineering job applicants had falsified their educational credentials. Any data stored on a remote-access, time-shared computer can be illegally accessed by most skilled business spies. Microphones and transmitters about the size of a pin head can now be easily obtained.

*(1500)*71*ac*ai*cc*de*ne

"Businesses Not Security Conscious." COMPUTERWORLD, 12 May 1971, p. 1.

*(1510)*73*ae*cb*dd*ec*ed*ei*ht

Buzen, J. P.; Chen, Peter P.; and Goldberg, Robert P. "Virtual Machine Techniques for Improving System Reliability." PROCEEDINGS OF THE ACM WORKSHOP ON VIRTUAL COMPUTER SYSTEMS, 26 March 1973.

*(1520)*70*ac*ai*bb*db*hp*kb*kd*mc
"Calculated Computer Errors Manipulate Three Banks' Security; $1 Million lost." COMPUTERWORLD, 25 March 1970, p. 1.

$1 million was embezzled from two New York banks by four men. A bank employee arranged to make check deposits appear as cash deposits. These fake cash deposits were used to cover checks quickly drawn from one bank and deposited in the other bank.

*(1530)*71*ab*bc*cd*dc*ga*jg
"California Earthquake." COMPUTERS AND AUTOMATION, May 1971, p. 33.

*(1540)*71*ac*ba*da*hc*ii*lb*ma*x1
"Californian Charged With Data Snatching From Rival Computer." WALL STREET JOURNAL, 4 March 1971, p. 13.

A former Information System Design employee was caught tapping that firm's computer over telephone lines to steal a plotting program valued at $15,000 to $25,000. The program was needed to win over an Information Systems Design customer to the defendant's new employer.

*(1550)*71*ab*bb*cb*cc*cd*dg*ha*ne*x1
"Can Your Computer Keep a Secret?" INDUSTRY WEEK, 1 February 1971, pp. 46-48.

This article attempts to briefly point out many different types of threats to computers and computerized data. It tries to convince the reader that more than superficial security measures are necessary for adequate protection. The article is filled with brief comments by Harvey S. Gellman and Dennis Van Tassel, two computer security experts. Several actual cases of fraud are also briefly described. The paper is directed to those who are unaware of the importance of computer security. Nothing new or unusual is presented.

*(1560)*70*ac*ai*da*mb*nm
"Canada Builds Debtor Data Bank." COMPUTERWORLD, 30 December 1970, p. 1.

*(1570)*68*ab*cd*da*dc*gf
Cantor, Lon. "Electronic Intrusion Alarms." ELECTRONICS WORLD, September 1968, pp. 44-46.

*(1580)*70*ac*bc*bd*be*cc*dc*dd*de*fz*hr*ht*hu*hv*kb*ke
*kf*mi*nj*nk*x2
Carley, William M. "On the Defense: Computer Companies are Hauled into Court by Flurry of Lawsuits." WALL STREET JOURNAL, 30 November 1970, p. 1.

Several recent, interesting examples are given of computer manufacturers and software developers being sued

for delivering systems to customers that wouldn't work or worked incorrectly. In three of these examples, the customer's business was thrown into chaos. In two other examples, compensation was also being requested for poor maintenance service and delayed delivery. In one case, TWA is suing Burroughs for $70 million for providing an unreliable, incomplete, and defective passenger reservations system. The suit alleges that Burroughs misrepresented itself as a pioneer with extensive experience in developing such systems. Burroughs claims that the system meets all of TWA's contract requirements. Computer companies have been successfully sued in about half of the cases brought into court. However, computer companies like to settle out of court if at all possible, and they almost always try to avoid publicity.

*(1590)*71*ab*cd*ga*gf*mc*x1

Carlson, Paul. "A Bank Protects Its 'Memory'." BANKING, April 1971, pp. 38-39.

Elaborate physical safeguards taken by the Bank of California to protect its new computer service center are described. Some of these safeguards are: TV screening of the parking lot, all building entrances, and sensitive EDP areas; electronically controlled doors, many being bulletproof and having a mantrap design; guard control of all sensitive areas; maximum security vaults; and very sensitive fire detection systems. The same building is also used to handle currency.

*(1600)*69*ab*bb*cc*db*el*en*ff*fg*fn*hj*hk*hl*hm*hn*if *kb*la*x3

Carmichael, D. R. "Fraud in EDP Systems." THE INTERNAL AUDITOR, May 1969, pp. 28-38.

This article was written to make internal auditors aware of the possibilities of fraud in EDP systems. It demonstrates that access to valuable assets is not necessary to commit fraud. The three basic methods of EDP fraud are: console intervention, irregular program and master file maintenance, and manipulation of input data. These three methods are discussed in detail, and three actual plus six hypothetical examples are given. The actual examples are discussed in depth. Manipulation of input data requires the least specialized knowledge, is the easiest to accomplish, and occurs more frequently than the other methods of EDP fraud. Possible fraud techniques that could be performed by a computer operator, a programmer, a system supervisor, and other personnel are considered. The following safeguards were proposed to prevent those techniques: a computer or manual log of all console operations - reviewed by an independent party; standard operating procedures for every type of processing interrupt; an initial count and later recounts of the number of input documents; standard authorizing procedures for program modifications; separation of operating, systems, and program personnel; a special independent control group to verify output on a sample basis; and sequential prenumbering of all documents.

*(1610)*70*ac*ai*mf*ng
Carney, P. L. "Police Say Mafia's DP Use Impedes Crime Prevention." COMPUTERWORLD, 2 December 1970, p. 1.
Police officials discuss the probability of organized crime utilizing computers through front organizations and service bureaus.

*(1620)*70*ac*ai*bb*da*db*kq*mf*x2
Carney, P. L. "'Suspected Campanies' on Crime Commission Lists." COMPUTERWORLD, 30 December 1970, p. 1.
A survey of seventy-two known Mafia connected businesses in the Chicago area indicates that none are in the computer manufacturing or service industry. In fact, none of these companies owned a computer, but ten percent used service bureaus. It is alleged that the Mafia owns two CDC computers in New Jersey. The Mafia could make good use of a computer system. Information transmission could be made more secure, and business records could be manipulated more easily as well as stored more securely.

*(1630)*70*ac*ai*cc*dc*fp
Carr, Peter F. "Datafile Reconstruction Insurance Left to Unaware." COMPUTERWORLD, 19 August 1970.

*(1640)*70*ac*ai*cd*da*db*dc*gf
Carr, Peter F. "Limiting Access to Centers Called a Major Problem." Computerworld, 24 June 1970, p. 1.

*(1650)*70*ac*ai*cc*dc*fv*ne
Carr, Peter F. "Most DP Centers Lax in Arranging Backup Facilities." COMPUTERWORLD, 15 July 1970, p. 4.
Robert Jacobson is quoted on techniques for planning a computer backup program.

*(1660)*69*ab*da*je
Carroll, John M. "Bugging the Big Brains." EXECUTIVE, December 1969, p. 46.

*(1670)*71*ab*ba*bb*cb*cc*cd*da*db*dc*ea*el*fq*fv*ga*gg *hd*hj*je*jf*lb*x1
Carroll, John M. "How Safe is Your Computer?" BUSINESS QUARTERLY, Autumn 1971, pp. 86-89.
Computer hazards are classified as: physical attacks, electronic subversion, remote penetration, and electronic surveillance. The following common safeguards

are recommended: locate the computer room on an upper (not top) floor without exterior walls; the tape library should be in a separate room with a librarian always present; keep a log of all personnel in the computer room; keep three generations of backup of valuable tapes; separate and rotate personnel duties; write programs in high-level languages and copiously document; validate program integrity; use one-time passwords or a call-back system for remote access terminals; monitor all significant events; and encipher sensitive transmitted data. Security safeguards are expensive not only in monetary terms, but also in terms of storage space, processing time, personnel inconvenience, and morale. This paper was directed at managers generally unfamiliar with security issues. Nothing really new is presented.

*(1680)*70*ab*ae*cb*cc*da*eb*ee*eh*er*ha*hd*hf*ng*nm*x3
Carroll, John M. "Privacy and the Computer." DATA SYSTEMS NEWS, August/September 1970, p. 10; or PROCEEDINGS OF THE CONFERENCE ON INTERDISCIPLINARY RESEARCH IN COMPUTER SCIENCE, University of Manitoba, 8 June 1970, pp. 27-74.

This paper presents a unique mathematical attempt to quantify certain aspects of privacy. The data for the mathematical model was obtained from forty-six questionnaires sent to federal and local governments, insurance and finance companies, etc.. Six modes of privacy invasion (direct intrusion, indirect intrusion, violation of confidence, exchange of information given willingly, inadvertent disclosure, and small-sample disclosure) and nine types of file modification (create K new files, destroy K existing files, add or delete questions to K files, split or merge K files, copy K files, exchange contents of K file pairs, restricted disclosure of selected portions of records) were studied. Some of the results are: elimination of some personal data files is the best way to enhance individual privacy; splitting up existing databanks into numerous low-density files will decrease privacy unless each of these low-density files is subject to regulation every bit as stringent as that imposed upon the original databank; deletion of information from files will contribute significantly to individual privacy; differential file access policies are not particularly effective; the most serious threat is proliferation of personal files followed by exchanging personal data among files, extracting data to augment other files, and increasing the amount of information stored. The reader should be warned that Carroll's privacy model has these debatable assumptions: there is a single probability of disclosure assigned to each file, and high-density files are potentially better regulated.

*(1690)*72*ae*ag*cb*cc*da*ea*ed*eh*hd*he*ka*mb*mc*md*mf*mg*mj*ng*nm*no*x4

Carroll, John M. "Snapshot 1971 - How Canada Organizes Information About People." AFIPS CONFERENCE PROCEEDINGS, Fall Joint Computer Conference, Vol. 41, 1972, pp.445-452.

This paper summarizes the results obtained by a Canadian Task Force on the magnitude and composition of personal data in public and private sectors, and the means by which such data are gathered, processed, stored, and disseminated. Over 2,500 questionnaires were mailed with the response rate being greater than fifty percent. The returned information was analyzed from each of these viewpoints: characteristics of the response base; characteristics of files; collection of data; custody, dissemination, and exchange of information; extent of computerization; characteristics of machines; utilization of computers; assessment of computerization; and rights of subjects. The organizations were classified as nurturing (concerned primarily with well-being of individual), business (dealing with the individual on a give and take basis), and authoritarian (interested primarily in insuring the individual conforms to society's norms). Some of the study's conclusions are: utilization of computers for handling personel records is relatively low both in the number of records computerized and the amount of information in each record; economics, rather than technical feasibility or data availability, has limited wholesale creation of databanks; most respondents had adequate safeguards for their centralized batch operations; a large amount of information exchanging is occurring; and international information exchanging is significant.

The Privacy and Computer Task Force Report is available for $2.50 from Communications Canada, Information Services, 100 Matcalfe Street, Ottawa, Ontario. For a comparable study of U.S. organizations read a book by Alan F. Westin and Michael A. Baker entitled DATABANKS IN A FREE SOCIETY.

*(1700)*71*ae*ag*ca*da*eb*ee*nb*ng*x2

Carroll, John M.; McHardy, Larine; Martin, Robert; and Moravec, Hans. "Multi-Dimensional Security Program For a Generalized Information Retrieval System." AFIPS CONFERENCE PROCEEDINGS, Fall Joint Computer Conference, Vol. 39, 1971, pp. 571-577.

This paper gives a very detailed description of a generalized information retrieval system - "GIRS". The system was written in FORTRAN and implemented on a PDP-10 computer. A multilevel protection scheme uses one or more passwords that determine: which of ten available processing functions can be used, which records can a user access, and which portions of records (items) can be accessed. By experimenting with this generalized information retrieval system, it is hoped that optimal trade offs between security and economy can be determined for a broad range of retrieval applications.

*(1710)*ab*ba*cb*cc*da*db*ea*ed*ej*el*eq*gh*hd*ia*ii
*je*kb*lb*ma*ne*nk*no*x3

Carroll, John M.; and McLellan, P. M. "The Data Security Environment of Canadian Resource-Sharing Systems." INFOR: Canadian Journal of Operational Research and Information Processing, March 1971, pp. 58-67.

Peterson's and Turn's list of information confidentiality threats in a time-sharing system is briefly described. Then several specific examples are given on how to illegally penetrate a PDP-10/50 system. The following countermeasures were presented: access control, processing restrictions, privacy transformations, monitoring procedures, and integrity management. Each of these countermeasures was further broken into 5 to 14 subcomponents, and each subcomponent was very briefly explained. An investigation of the effectiveness of these countermeasures against threats to the PDP-10/50 revealed: theft of hard copy printouts and card disks is the most severe threat, and the confidentiality of passwords is tenuous. A survey of 5 time-sharing computer manufacturers, and a survey of 16 Canadian time-sharing users revealed the following facts: all manufacturers were concerned about security; most manufacturers felt that present hardware and software techniques were inadequate and were conducting research; the password was the most common access control device; two manufacturers offered password protection at the file level; communication links are viewed by manufacturers as a major weakness; there appears to be no customer demand for cryptography; 7 of the 16 computer users did not use password access control protection; 5 of these used only an account number and the other 2 used name - account number - project number access control; none of the 16 users used one-time passwords, cryptography, or file level passwords; and in 9 of 16 user systems the operating staff and other users have the ability to read a user's files at will. These 16 users represented about 75 percent, by volume, of Canada's time-sharing services. Clearly, security precautions are lax among Canadian time-sharing computer users.

*(1720)*70*ae*ag*cb*da*ea*ec*ed*eq*hd*lb*ng*x3

Carroll, John M.; and McLelland, P. M. "Fast 'Infinite-Key' Privacy Transformation for Resource-Sharing Systems." AFIPS CONFERENCE PROCEEDINGS, Fall Joint Computer Conference, Vol. 37, 1970, pp. 223-230.

The first three pages of this paper are a summary of another article by the same authors entitled, "The Data Security Environment of Canadian Resource-Sharing Systems". The remaining five pages discuss in detail the authors' unique method of generating an infinite-key cryptographic transformation. The authors chose the infinite-key method over the short-key method because the former offers greater security and requires less storage. (For a discussion on the trade-offs between infinite-key and short-key methods read "Privacy and Security in Data Banks" by W. A. Garrison.) The authors used the additive congruential random number generation method and two generators to generate the infinite-key. They implemented this on a PDP-10/50 system and compared the results with those of a mixed multiplication congruential method proposed by IBM. Their method was significantly superior to the IBM method. Another unique advantage of Carroll's and McLelland's method is that the user can easily specify, within a wide range, different levels of encoding security. The less secure levels will use less processing time for encoding/decoding and therefore will be less expensive to use. The exact infinite-key used depends on the user performing a pre-specified mental transformation (known only to him and the computer) on a word given to him by the system when he "logs on". The speed of the new cryptographic transformation method is sufficient to keep up with normal data transfers between most processors and peripheral devices. The method can be implemented on almost any computer for a hardware cost of approximately $10,000.

*(1730)*73*ad*cc*cd*dc*gg*nf
"Catastrophe Prevention Management of the Computer Complex." American Management Association, Management Systems and Science Division, 135 West 50th Street, New York, New York 10020, (Seminar).

AMA has no plans to publish the proceedings of this seminar. It has been given several times in 1971 and 1972. Write to the above AMA address for more information.

*(1740)*72*ab*cc*fb
Chapin, N. "Successful Planning Techniques for Data Processing Managers." DATA MANAGEMENT, September 1972, pp. 35-38.

*(1750)*70*ab*cc*db*de*hk*hp
Charlton, W. L. "The Interaction of Clerical and Punching Processes in Data Input." THE COMPUTER BULLETIN, October 1970, pp. 345-346.

*(1760)*66*ad*cc*da*hd*ka*mb*md*nm

Chartrand, R. L. "Information Concerning the Proposed Federal Data Center." TK 6565C, SP 112, The Library of Congress Legislative Reference Service, Washington, D.C., 10 August 1966.

This report reviews the recommendations for establishment of a federal data center given by the Ruggles report and the Dunn critique of the Ruggles report. A list of safeguards against accidental disclosure is also given.

*(1770)*68*ae*cb*cc*dg*ni
"Checklist for Evaluation of Data Processing Systems." NCUMA CONVENTION, Phoenix, Arizona, 1968.

*(1780)*72*ab*cd*dc*ge*x2
Cholin, Roger R. "Halon 1301 and Computer Fires." DATA MANAGEMENT: Conference Issue, Vol. 10, September 1972, pp. 75-77.

Halon 1301 is a gaseous fire extinguisher agent that is ideal for use in computer rooms. It doesn't have the toxicity of çarbon dioxide extinguishants nor is it harmful to electronic equipment as are water extinguishants. This paper describes a series of tests by Underwriters Laboratories which prove that the decompostition of Halon 1301 into HF and HBr at 900 degrees fahrenheit will not harm operating computers. Several other extinguishing characteristics of Halon 1301 are given.

*(1790)*71*ab*bg*cb*cc*cd*dg*fp*fv*fy*f1*ge*gf*gg*gh*hd
*je*jf*jg*nb*nn*x2
Chu, Albert L. C. "Computer Security: The Corporate Achilles Heel." BUSINESS ADMINISTRATION, 1 February 1971, pp. 32-38.

This article presents a broad and brief overview on most aspects of computer and data security. It is essentially a summary of approximately fifteen to thirty other security articles. No topics are covered in depth. Fifteen examples of actual computer crimes and disasters are briefly described. Computer and data security is said to involve an interface of physical security, personnel security, procedural security, audit controls, and insurance. Two completely automatic tape storage and delivery systems are described. Short discussions are given on: computer room architecture, physical access control, fire extinguishants, backup files, embezzlement, trade secrets, wiretapping of remote access terminals, security responsibility, and security cost. This would be a good introductory article for those completely unfamiliar with the problems of computer and data security. COMPUTER SECURITY MANAGEMENT by Dennis Van Tassel is a good introductory book on this subject.

*(1800)*71*ab*da*md*nm
Chu, Albert L. C. "The Need to Know - The Right to Privacy." BUSINESS AUTOMATION, June 1971, pp. 31-35.

This article gives a broad review of the conflict between society's need for fast access to accurate information and the individual's right to maintain a sufficient amount of personal privacy.

*(1810)*73*ac*ai*cc*da*lb*mb*mf*nl*nm*x1
"Citizens' Committee Formed to Oversee Crime Net Privacy." COMPUTERWORLD, 3 January 1973, p. 1.

The Massachusetts Privacy and Security Council, made up of lawyers and interested citizens, is one of the first, if not the first, citizens' review-type panel to oversee privacy considerations in police information systems. One of their first tasks is to determine whether Massachusetts will tie into the FBI's criminal history system.

*(1820)*60*ab*cc*da*db*dd*ff*kd*la
Clive de Paul, C. "Problems of Auditing Data: The External Auditor and Computers." THE COMPUTER JOURNAL, 1960.

*(1830)*72*ab*cd*dc*ge*jg*mc
"CO2 Fire Extinguisher System Protects Computer Center." MAGAZINE OF BANK ADMINISTRATION, October 1972, p. 90.

This is an example of one bank's approach to protecting its computer installation from fire.

*(1840)*72*af*ak*ca*da*eq
Cocke J.; and Raviv, J. "Data Compaction and Security System." IBM TECHNICAL DISCLOSURE BULLETIN, Vol. 14, No. 8, January 1972, pp. 2427-2430.

The article describes a varible state coding system that can simultaneously serve the needs of data compaction and data security. The system makes a character-by-character random selection of encoding tables for compacting and encoding input data.

*(1850)*71*ae*cb*cc
Codd, E. F.; and Dean, A. L. (eds.) "Data Description and Control." ACM Special Interest Group on File Description and Translation (SIGFET) Workshop, 11 November 1971.

*(1860)*72*ab*cb*da*db*ea*lb
Coiner, L. M. "Controlled Access System Uses Mag Cards to Restrict Entry for Tighter Security." ADMINISTRATIVE MANAGEMENT, December 1972, p. 14.

*(1870)*70*ab*cc*dd*fi*fo
Collins, D. B. "Documentation and Debugging." DATA MANAGEMENT, September 1970, pp. 107-115.

*(1880)*71*ab*cb*da*ed*ef*eh*lb

Collmeyer, A. J. "Data Base Management in a Multi-Accessed Environment." ÇOMPUTER, Magazine of the IEEE Computer Society, November 1971, pp. 36-46.

A Data Base Management System is defined as a network of logical subsystems where each of the subsystems performs a special function consistent with its role in the network. The problems of shared files are discussed, and three approaches to file sharing are developed. The difference between these approaches are emphasized so as to make comparison between them easier. Because the security problem is of critical importance in a multi-accessed environment, a brief discussion of file integrity and file security is included.

*(1890)*69*ae*ag*cb*cc*da*de*eh*fd*fh*fs*fu*hd*ih*ka*mb *md*nc*nf*nm*x3

Comber, Edward V. "Management of Confidential Information." AFIPS CONFERENCE PROCEEDINGS, Fall Joint Computer Conference, Vol. 35, 1969, pp. 135-143.

This article is primarily concerned with protecting the privacy of information stored in large databanks. Only procedural safeguards are considered in depth. The following key factors are considered which could serve as a foundation for a basic privacy control system: criteria for deciding what constitutes an unwarrented invasion of privacy; the difference between private and confidential information; areas sensitive to intrusion; intercompany data integration; data verification; data classification; potential threats to privacy; and system design considerations and procedural safeguards for minimizing privacy violations. The author drew the following conclusions from analyzing the above key factors: the integrity and security of any personal information system will ultimately depend on human factors; personnel standards, a strong policy, and discipline are necessary; the individual must have the right to inspect and correct his file; a realistic data purge policy is required; training and policy education of all system users is needed; and a databank licensing scheme needs further consideration.

*(1900)*68*ab*cc*df*dg*fy*fz*kb*ma*x1

"Companies With Outside EDP Services Warned of Particular Risks." MANAGEMENT SERVICES, November 1968, pp. 12-13.

The following four types of risks are common enough to warrant insurance protection if they are not adequately covered in the service bureau contract: loss of cards, tapes,and valuable records; fraud loss resulting from collusion between company and service bureau personnel; errors and omissions; and business interruption losses resulting from delayed data processing.

*(1910)*65*ad*al*cb*ed*gh*lb*x1
"The Compatible Time-Sharing System: A Programmer's Guide." P. A. Crisman (ed.), MIT Press, Cambridge, Massachusetts, 1965.

MIT's Compatible Time-Sharing System is described. It has a file system organized as a tree structure and provides for sharing of files through links between branches of the tree. The access modes are read, write, protected, or any combination thereof. These modes may be assigned at the time the link is established, on a user-by-user basis.

*(1920)*69*ae*cc*cd*da*db*dc*fs*ga*mh
Compton, Laurence B. "The Air Forces' Internal Control Program for Personnel and Physical Facilities." American Management Association Conference on Security and Catastrophe Prevention Management of the Computer Complex, November 1969.

*(1930)*71*ab*bc*cc*cd*dc*gf*jf*x1
"The Computer: A Target." DUN'S REVIEW, January 1971, pp. 34-36.

This article shows that most businesses have grossly inadequate safeguards to prevent sabotage of their computer installation. Two sabotage examples are briefly described, and several reasons are given as to why better protection is unquestionably necessary. However, the statement "a small quarter-size magnet can destroy 50,000 tape reels in minutes" is a gross exaggeration.

*(1940)*73*ab*np*x2
COMPUTER ABSTRACTS. Technical Information Company, Martins Bank Chambers, P.O. Box 59, St. Helier, Jersey, British Channel Islands, 1957-, (Monthly, with annual cumulative index).

Each monthly publication reviews about 300 articles. U.S. government reports, patents, and books are also reviewed. Although the publisher is located in Britain, almost all the entries are from American journals and magazines. A subject index containing "privacy" and "security" indices enables easy location of security articles. However, only about one or two articles on computer security can be found in each monthly issue.

*(1950)*73*af*cc*np*x1
COMPUTER AND CONTROL ABSTRACTS. Institution of Electrical Engineers and Institute of Electrical and Electronic Engineers Inc., 345 East 47th Street, New York, New York 10017, 1966-, (Monthly, with semi-annual cumulations).

This publication abstracts thousands of articles on computers every month. A significant number of the articles abstracted are from foreign countries. The abstracts are divided into four subject regions entitled: Systems and Control Theory, Control Technology, Computer Programming and Applications, and Computer Systems and Equipment. These abstracts are very well written and average about ninety words in length. Unfortunately, only seventy articles on computer security were abstracted in the period 1966-1973. These seventy articles are a mixture of highly technical and very non-technical material. A majority of them can easily be found in other reference sources. However, about fifteen of these articles were from other countries such as England, Germany, The Netherlands, and Austrailia, and they were not located in any other reference source.

*(1960)*70*ac*ai*bc*cd*dc*jf
"Computer Bomb Damage Studied." COMPUTERWORLD, 9 September 1970.

*(1970)*70*ac*ai*cc*cd*dg*no
"Computer Center Security System Surveyed." COMPUTERWORLD, 14 June 1970, p. 1.

*(1980)*71*aa*cc*db*dd*de*eh*el*fe*ff*fg*fh*fi*fn*fp*fq
*fv*fx*hj*kb*kd*nf*no*x4
COMPUTER CONTROL GUIDELINES. Canadian Institute of Chartered Accountants, Auerbach Publishers, 1101 State Road, Princeton, New Jersey 08640, 1971, 136 pp., $10.00.

This excellent book is the result of a very large study performed by the Canadian Institute of Chartered Accountants. It is complete, well written, and handsomely organized into seven chapters and twenty-five control objectives. Each control objective is discussed from the viewpoint of minimum control standards. Minimum control standards are defined and specific control techniques are classified under the appropriate standards. Other control standards, beyond the minimum ones, are presented where appropriate. The seven chapters of the book are entitled: Pre-Installation Controls, Organizational Controls, Development Controls, Operations Controls, Processing Controls, Documentation Controls, and Outside Data Center Controls. Two examples of the twenty-five control objectives are: insure the adequacy of management trails, and insure the completeness of data processed by the computer. A sixteen page summary of objectives, minimum control standards, and techniques is also given. A second book resulting from the same study will soon be published. It will deal with minimum audit standards, and acceptable techniques for evaluating these audit standards.

*(1990)*70*ab*cb*cc*dg
"Computer Data Protection." INDUSTRIAL SECURITY, No. 4, 1970, pp. 20-29.

*(2000)*69*ab*ca*lb*ng*x2
"Computer Designs Tamperproof Computer." DATA MANAGEMENT, September 1969, p. 55.

The Advanced Research Projects Agency of the U.S. Department of Defense has provided a two and one half year grant to Case Western Reserve University in Cleveland for research and development of a coherent structure for computer system design. Developing this coherent structure will be the first step toward a computerized design system for designing a new race of reliable and secure computers. Edward L. Glaser is head of the design team which includes engineers, mathematicians, graduate students, and a PDP 10/50 computer.

*(2010)*72*ab*np*x3
COMPUTER DIRECTORY AND BUYERS' GUIDE: 18TH ANNUAL EDITION. COMPUTERS AND AUTOMATION, Berkeley Enterprises (publ.), 815 Washington Street, Newtonville, Massachusetts 02160, 30 August 1972, 180 pp.

This issue categorizes almost all U.S. data processing service and manufacturing companies as to the types of services and products offered. On page 83, under the sub-heading "security systems and equipment" there are listed approximately forty companies. Of these forty companies, eight are primarily security equipment manufacturers, and seven are primarily computer security consultants. The other twenty-five firms only have secondary interests in security.

*(2020)*70*ac*ai*bb*cc*db*hj
"Computer Frauds Seen as Danger to EDP Operations." COMPUTERWORLD, 26 August 1970, p. S-5.

*(2030)*70*ab*cc*cd*dg*gg*mc*nf*x1
"Computer Growth Calls for Security in Banks." DATA MANAGEMENT, September 1970, p. 156.

This news bulletin briefly summarizes a speech by Richard F. Cross before the Second National Conference on Bank Security. Mr. Cross states that computer security involves: (1) placing a value on the computer operation, (2) a thorough analysis of all possible threats, and (3) insurance coverage. Protection involves an interface of physical security, personnel security, procedural security, audit controls, and insurance. (Apparently, Mr. Cross has left hardware and software protection considerations to the computer manufacturer.) Several specific safeguard techniques were then discussed. Some of them are: site selection and construction, air conditioning, personnel access to computer room, employee loyalty and honesty, and backup emergency plans.

*(2040)*70*ab*cd*df*gd
"Computer Power in Small Packages." ELECTRONIC WORLD, 5 January 1970, p. 51.

The paper describes a self-contained power distribution console using circuit breakers and voltage regulators to provide continuous power to a computer installation.

*(2050)*71*ab*cd*dc*ga
"Computer Protection - Highlights of Protection for Data Processing Rooms." THE SENTINEL, Factory Insurance Association, Boston, Massachusetts, November 1971.

*(2060)*68*ac*bb*bc*be*db*dc*de*x1
"Computer Room Disaster Sent Companies Scrambling to Protect Precious Files." WALL STREET JOURNAL, 14 Novermber 1968, p. 1.

The dangers of fire, flood, sabotage, and fraud have been overlooked by many companies rushing to automate bookkeeping chores. A Los Angeles credit firm lost $10,000 when a service technician accidently erased a disk containing 80,000 accounts. A disgruntled army officer caused an army computer to erase itself shortly after he retired. One computer was destroyed when a fire in the room below caused the computer room floor to collapse.

*(2070)*69*ab*cc*cd*dg
"Computer Security." INDUSTRIAL SECURITY, December 1969, pp. 18-37.

*(2080)*72*ad*cc*cd*np*x2
"Computer Security, Backup, and Recovery: A Selected Bibliography." Canning Publications Inc., 925 Anza Avenue, Vista, California 92083, 20 January 1972, 8 pp.

This bibliography contains entries for 59 periodicals, 11 books or proceedings, 10 reports, and 3 seminars. Nearly all of these entries are concerned with physical security or management control and operating procedure security. Most of these entries can be found in other reference sources. None of the entries are annotated.

*(2090)*72*ab*bg*cc*dg*fd*ff*fg*fi*fj*fk*fp*fq*ft*fv*fy
*hg*hj*kb*kd*la*nf*x4
"Computer Security: Backup and Recovery Methods." EDP ANALYZER, January 1972, pp. 1-15.

The following aspects of computer security are discussed in a complete and easily readable manner: Data and Program Backup (classifying programs and files, causes of backup being ineffective, items needing backup, recovery points, daily backup systems, grandfather-father-son procedures, several examples of actual backup systems, software package for supporting backup); Hardware Backup (alternate site prospects, identification of critical jobs, checking equipment configuration and operating system used at backup site, type of agreement with party providing backup, threats to backup site, storing backup files at backup site); Internal Control (embezzlement and fraud, malicious damage, separation and rotation of duties, personnel security checks, examples of malicious damage by disgruntled employees); Insurance (equipment coverage, media coverage, extra expense coverage, business interruption coverage); and Funding the Computer Security Program (security is expensive, evaluate the problem, get top management involved, develop a plan, search for funding). Problems associated with remote access terminals are not discussed because they were covered in the May 1970 issue of EDP ANALYZER entitled "Security in the CDB". This report is the second of a two part series. The first part entitled "Security of the Computer Center" is in the December 1971 issue.

*(2100)*70*ab*cb*cc*cd*gh*ma*x1
"Computer Security is Sensitive Area." INDUSTRY WEEK, 5 October 1970, pp. 13-14.

A few General Electric managers are quoted on statements relating to the security of their $100 million time-sharing service which currently serves 150 major U.S. firms. If one of G.E.'s three centers would be completely destroyed, the data would still be physically available at one of the other two centers. G.E. feels that the smallest worry a customer should have is whether his data is safe. No specific safeguards were mentioned.

*(2110)*73*ab*bb*db*hj*hk*hm*if*ii*mc*x2
"The Computer Thieves." NEWSWEEK MAGAZINE, 18 June 1973, pp. 109-112.

Four examples of recent computer related crimes are presented. In one example, a chief teller at a branch of New York's Union Dime Savings Bank embezzled away more than $1.5 million over three years simply by manipulating inactive accounts in the bank's computer. He was caught by accident when police investigating another case found that the teller was betting as much as $30,000 daily through a bookmaker. In another example, a person devised a technique to order expensive communications equipment directly from a Pacific Telephone and Telegraph computer simply by using his touchtone telephone. He was so successful he set up a ten man company to sell the equipment, and only got caught when his employees became dissatisfied and turned him in.

A disturbing fact is that most of today's computer criminals are caught by accident. The extraordinary complexity of many of today's computer programs is at least partially responsile for this. The typical computer criminal works with accomplices and doesn't have any characteristics to distinguish himself from fellow honest employees.

*(2120)*70*ab*cc*cd*dg*gg*x1
"Computer Vulnerability - A New Business Risk." THE NEW YORK CERTIFIED PUBLIC ACCOUNTANT, March 1970, pp. 237-239.

The rapid growth in EDP over the past decade has created a new business risk - computer vulnerability. Hazards which most EDP systems are subject to are: environmental disaster, mechanical failure, operator error, program error, theft, fraud, and sabotage. Security has been achieved in the past because a limited number of people understood EDP. This will not be true in the near future. It is suggested that management implement the following safeguards: insure that all programs have sufficient internal and external checks; maintain duplicate files; control physical access to computer room; and organize an independent security control group.

*(2130)*72*ab*bb*cc*db*ff*x1
"Computers Breed New Type of Criminal." DATA MANAGEMENT, August 1972, p. 36.

U.S. business fraud losses are now $1 to $3 billion annually. An increasing number of cases are involving the computer. Three brief examples are given. In one example, an EDP manager was handicapping horses and running a bookmaking operation on his company's computer. Most fraud can be prevented by vigilant internal controls. Rotating duties, maintaining logs, controlling passwords, and periodic personnel investigations are also useful.

*(2140)*69*ab*bb*cc*db*ff*mc*x1
"Computers: Embezzlement From Banks." CERTIFIED ACCOUNTANTS JOURNAL, November 1969, pp. 639-640.

Two examples of bank fraud are given. In one example, an EDP manager stole $81,000 by instructing the computer to write checks to fictitious persons. In the other example, a manager in charge of bank operations stole $250,000 by having the computer transfer funds from an interest revenue account to his employee stock plan account. Separation and rotation of duties and frequent auditing by specially trained computer auditors are recommended.

*(2150)*70*ac*bb*db*hj*if*mc*x1
"Computers Outfoxed, But Not the Police, in Check-Kiting Caper: Theft Exceeding $880,000." WALL STREET JOURNAL, 13 March 1970, p. 15.

A fraud case involving a former branch manager from Bankers Trust Company, a vice president of National Bank of North America, and three brothers is discussed. Deposit slips were made out as cash transactions when only checks were deposited. The computers then assumed that the accounts contained sufficient funds to cover checks subsequently drawn because cash transactions were recorded as immediate deposits. In the final month before the fraud was detected, $9 million worth of checks had been kited between the two banks.

*(2160)*67*ab*cb*cc*da*db*dc*gg*hd*lb
"Computers: Safeguarding Time-Sharing Privacy: An All-Out War on Data Snooping." ELECTRONICS, 17 April 1967, pp. 157-159.

Various safeguards used to prevent unauthorized access in time-sharing systems are presented.

*(2170)*73*ac*ai*bg*cc*cd*nm*np*x4
COMPUTERWORLD. Computerworld Inc., 797 Washington Street, Newton, Massachusetts 02160, 1967-, (Weekly).

This weekly newspaper has articles on computer security and computer privacy in almost every issue. There are frequent stories on actual occurrence of sabotage, fraud, and disastrous accidents.

*(2180)*70*ac*ai*bb*bc*db*cc*cd*da*db*dc*ed*ff*fy*ga*hc*ma*x2
"Computerworld: 1970 Environment and Security Supplement." COMPUTERWORLD, 26 August 1970, 8 pp.

This supplement contains several articles covering subjects such as fraud, auditing, insurance, disaster prevention, software protection, and service bureaus.

*(2190)*71*ac*ai*cb*cc*cd*dg*ja
"Computerworld: 1971 More Supplement." COMPUTERWORLD, 30 June 1971.

This supplement contains several articles covering subjects such as physical security (fire protection, power sources, etc.), control over the computer's environment, and unauthorized access through remote terminals.

*(2200)*73*ab*np*x1
COMPUTING REVIEWS. Association for Computing Machinery, 1133 Avenue of the Americas, New York, New York 10036, 1960-,

(Monthly, with annual cumulative index).

This periodical comprehensively covers the literature on computing and its applications. More than a thousand selected volunteer specialists provide critical evaluations of domestic and foreign books, technical papers, popular articles, films, and video tapes on every aspect of computing. Over 200 serial publications are scanned regularly for pertinent materials. Approximately one article concerning computer and data security can be found in each issue.

*(2210)*72*aa*cb*cc*cd*dg*fs*ga*gg*lb

CONFERENCE ON SECURITY TECHNIQUES (England). National Computing Centre Ltd., Manchester, Lancashire, England, 21 November 1972.

This conference was held in London on November 21, 1972. Presentations were given on the following six topics: data control, security in a multi-user installation, database security, personnel and organizational controls, computer data security in perspective, and physical security. Papers are available on these presentations, but only in condensed form.

*(2220)*69*ak*cb*cc*da*db*ea*ed*ei*ej*el*en*eq*fb*fc*fe *fu*fx*lb*nb*nc*x3

"The Considerations of Data Security in a Computer Environment." G520-2169-0, IBM Corporation, White Plains, New York, 1969, 36 pp.

This brochure is a guide to provide general management, systems designers, and operations management with various data security considerations in order to assess and minimize potential problems. Approximately three fourths of the brochure is directed toward systems designers. General management and operations management security considerations are each discussed in only three pages. Some of the more interesting and important security considerations are briefly stated below. Key factors in determining the extent of protection required are: equipment configuration, degree of data sensitivity, computer hardware, computer room architecture, acceptable reduced system efficiency, employee loyalty, involvement of outsiders, and the company's experience with security. One of the most important elements in a security program is that it be tested and audited regularly at random intervals. This testing and auditing should provide a review of the system's: current effectiveness, continuing appropriateness, level of complexity, checks and balances in staff assignments, training procedures for new users, and operation under special circumstances (meeting deadlines or correcting system errors). Accessing sensitive data may require identification of the person, terminal, and program. For identification of remote terminal users a magnetic-coded badge appears to have the best overall characteristics. The need for data security is dynamic, and an ever-present danger of "over-security" exists. Detailed analysis of audit logs make it possible to fine-tune each security technique and/or redesign files to further protect sensitive data to meet the installation's unique needs. Program testing has one of the greatest potentials for security exposure. System security routines and the associated tables are to a sensitive data processing installation as the vault combination is to a bank. At least one person per shift must be designated responsible for maintaining security.

A condensed outline of this brochure is given below. General management security considerations (interrelated factors, review techniques); systems designers security considerations (identification, design of authorization techniques, data file protection, audit procedures, program testing, communication lines); operation management security considerations (physical security, operating procedures, personnel).

*(2230)*72*ab*ah*ca*ed*ef*gh*ha*lb*nc*ng*x4
Conway, Richard W.; Maxwell, William L.; and Morgan, Howard L. "On the Implementation of Security Measures in Information Systems." COMMUNICATIONS OF THE ACM, April 1972, pp. 211-220.

The purpose of this paper is to discuss the nature of flexibility in a security conscious operating system and to relate the costs of security implementation and enforcement to that flexibility. Security decisions for a particular databank system may be recorded in a "security matrix" model where the columns of the matrix correspond to particular data items in the system, and the rows of the matrix correspond to potential users of the system. Each element in the matrix d(i,j), is a decision rule specifying the conditions under which user "i" is entitled access to the data item "j" and the actions that "i" is permitted to perform upon "j". Most of today's security systems are either a column model, where there is only one data item and a simple yes/no decision based on a password, or a diagonal model, where each file is uniquely identified with a particular user. In a real system the security matrix could become prohibitively large. However, the size could be reduced and made practical by: defining virtual users each representing a collection of users with identical security authorization; simplifying the entries in the matrix to only yes/no indicators; or by careful analysis of when and how the matrix should be interrogated. The authors feel that this third approach offers some real promise in reducing the cost of implementing such a security matrix.

First, a distinction needs to be made between access decision rules that are data dependent and data independent. Restricting a user from ever seeing a field named SALARY is a data independent decision rule, while restricting him to salaries less than $10,000 is a data dependent decision rule. The point to be made is that data independent decisions can be enforced by examining the request and appropriate matrix element just once - at translation time, whereas data dependent decisions need to examine the request and appropriate matrix element for each repeated access during execution time. Most writers and designers have recognized that data dependent decisions can only be enforced at execution time, and have planned the enforcement of all security decisions in this way. Since execution time enforcement is about ten times more expensive, this has given the false impression that all security enforcement is very expensive.

The authors also take a brief look at the following three security conscious systems: Hoffman's student health system at Stanford University; MIT's MULTICS system; and the ASAP file maintenance system used by the authors as a test system for their matrix model concept. The authors conclude that a general purpose operating system, such as OS/360, could be quite easily modified to add the matrix security model, but all enforcement would have to be done in execution time. To implement some translation time enforcement, the capabilities of the source language, such as COBAL or FORTRAN, would have to be somewhat restricted.

*(2240)*72*ae*ag*cb*da*ed*ef*gh*la*x3

Conway, Richard W.; Maxwell, William L.; and Morgan, Howard L. "Selective Security Capabilities in ASAP - A File Management System." AFIPS CONFERENCE PROCEEDINGS, Spring Joint Computer Conference, Vol. 40, 1972, pp.1181-1185.

The ASAP security system is mainly designed to prevent the casual user from gaining access to information he should not see. The determined professional would have little trouble going around these security measures. ASAP only supervises all requests for information entry, update, and retrieval which are written in the ASAP language. ASAP uses a dictionary that contains for each authorized user: a password identification, a description of the file subset accessible to him, and a description of the processing actions that he is permitted to execute. Every ASAP file can be divided into non-hierarchical security classes such as: personal/biographical information, financial information, and new product information. Each non-hierarchical security class is further divided into different levels of restricted access by use of a boolean expression that describes by content those records in the

file which a user is permitted to access. For example, a user may be restricted to access all personnel files of employees earning less than $15,000 (and) being employed less than five years with the company (and) working overtime. ASAP security tests are applied at the source language level. The authors believe that security checking at compile time is cheaper than at execution time. ASAP does not provide any execution time access control for use in a time-sharing environment.

*(2250)*69*ac*cc*cd*dc
Cook, A. D. "EDP Defends Against Disaster." ELECTRONIC NEWS, 29 December 1969, p. 33.

*(2260)*71*ab*cc*fm
Cook, C.; and Inoue, M. S. "Computer Center Operations Analysis." DATA MANAGEMENT, November 1971, p. 24.

*(2270)*68*ae*cb*ed*ei*el*lb
Corbato, F. J.; and Saltzer, J. H. "Some Considerations of Supervisor Program Design for Multiplexed Computer Systems." IFIPS CONFERENCE PROCEEDINGS, 1968.

*(2280)*65*ae*ag*cb*gh*lb*x2
Corbato, F. J.; and Vyssotsky, V. A. "Introduction and Overview of the MULTICS System." AFIPS CONFERENCE PROCEEDINGS, Fall Joint Computer Conference, Vol. 27, 1965, pp. 185-196.

This paper attempts to give a detailed discussion of MULTICS design objectives as they relate to major areas of the system. The paper is not very technical and can be understood by those with a minimal knowledge of computers. Protection of private files and isolation of independent processes were considered to be of critical importance when designing the system. System programming is done with the same facilities, tools, etc., available to the ordinary user. The file system was designed with the presumption that there will be mishaps, so an automatic file backup mechanism was provided. It was expected that the ultimate limitation on the user of the system will be the knowledge which he has of it.

*(2290)*70*ac*ai*cc*dc*fy*jf*mj
"Costlier Protection Hits Campus Centers." COMPUTERWORLD, 5 August 1970.

California college computer centers are having a difficult time getting disaster insurance because of recent campus unrest. A prerequisite for obtaining coverage appears to be twenty-four hour guard protection.

*(2300)*72*ab*cc*da*nm
Countryman, Vern. "Computers and Dossiers - Part II."

COMPUTERS AND AUTOMATION, February 1972.

*(2310)*72*ac*ai*bb*db*hd*if*kf*me*nj*x1
"County Supervisor is Sued Over Use of DP Mail Lists." COMPUTERWORLD, 5 July 1972, p. 1.

An Orange County, California supervisor was charged with misuse of county computer data services in his reelection. He allegedly requisitioned a mailing list of county employees and used the printouts of names and addresses to mail political material.

*(2320)*69*ae*cb*cc*cd*fe*ea*eh*ff*lb*mg*nm
Courtney, R. H. Jr. "Data Security and Privacy." THE 6TH ANNUAL NATIONAL COLLOQUIUM ON INFORMATION RETRIEVAL, Medical Documentation Service, Philadelphia, Pennsylvania, May 1969, pp. 9-14.

This paper is concerned with the security and privacy of data in remote-access, time-shared computer systems. Data security is considered to have the four fundamental components: authorization, identification, system integrity, and auditing.

*(2330)*71*ad*ak*cb*cc*cd*lb
Courtney, R. H. Jr. "Forty Commonly Found Deficiencies in the Security of Data Processing Activities." IBM Data Security and Privacy Systems Development Division, 30 June 1971, 14 pp.

A list of the forty most commonly found security deficiencies is given. The author, who is the head of IBM's Data Security and Privacy Systems Development Division, tries to play down the sensationalism used by some consultants in the computer security consulting business. He suggests that magnetic cards be used to replace passwords for remote terminal access. He doesn't see any significant difference between accidently and intentionally destroyed data.

*(2340)*72*ab*cb*cc*da*db*mc
"The Credit Card Explosion." BUSINESS AUTOMATION, April 1972, p. 26.

*(2350)*67*ab*cc*cd*da*hd
Cross, Richard F. "Safeguarding Classified Information." INDUSTRIAL SECURITY, August 1967.

*(2360)*71*ab*cc*cd
Cross, Richard F. "Tighter Security for Computers." INDUSTRIAL SECURITY, August 1971, pp. 86-89.

*(2370)*68*ad*ak*cb*ed*gh*x1
"CP-67/CMS User's Guide." Report 320-2015, IBM Cambridge Scientific Center, Cambridge, Massachusetts 02139, July

1968.

One of IBM's efforts to provide file access control is described. Files may be released to all other users in one of four modes: read only; read/write; read only and erase after one read; and read/write and erase after one read. However, the manual notes that all modes may not be implemented.

*(2380)*70*ab*ca*da*eq*x1
"Cryptic Computers." SCIENTIFIC AMERICAN, January 1970, p. 52.

This article briefly summarizes a speech by Ralph Skatrud entitled "A Consideration of the Application of Cryptographic Techniques to Data Processing" given at the 1969 Fall Joint Computer Conference. Mr. Skatrud proposed two methods for implementing cryptographic protection systems in computers. One method is a polyalphabetic substitution technique that employees a number of continuously changing cipher alphabets. The other method is a digital matrix transposition technique that reads data into a matrix by rows and out by columns, under the control of random digits stored in the computer. Both methods are theoretically unbreakable since only a one-time code is used.

*(2390)*73*ab*cb*eq
THE CRYPTOGRAM. The American Cryptogram Association, Rogot, E.&E. 9504 Forest Road, Bethesda, Maryland 20014. (Bimonthly).

*(2400)*70*ac*ai*ca*da*eq*gh*hc*hd*lb
"Cryptographic Package May End 360 Program Thefts." COMPUTERWORLD, 24 June 1970.

*(2410)*69*ab*cc*da*ka*mg*nl*nm
Curran, W. J.; Stearns, B.; and Kaplan, H. "Privacy, Confidentiality, and Other Legal Considerations in the Establishment of a Centralized Health-Data System." NEW ENGLAND JOURNAL OF MEDICINE, 31 June 1969.

The authors give specific proposals for the safeguarding of information in a medical databank.

*(2420)*71*ab*cb*dd*eo*ep
Dale, Dixon R. "Controlling Data Transmission Errors." DATA DYNAMICS, July 1971, pp. 18-22.

*(2430)*65*ae*ag*al*cb*eb*ed*fv*gc*ht*hu*lb*na*x3
Daley, R. C.; and Neumann, P. G. "A General Purpose File System for Secondary Storage." AFIPS CONFERENCE PROCEEDINGS, Fall Joint Computer Conference, Vol. 27, 1965, pp. 213-229.

If computer files are to be shared among various users in a way which can be flexibly controlled, safeguards against the following threats should be provided: masquerading; accidents or maliciousness by authorized and unauthorized users; self-inflicted accidents; hardware or system software failures; unauthorized tampering of system safeguards; and excessive use of safeguards. This paper describes a basic formulation of a file system designed to meet these threats. The formulation provides the user with a simple means of addressing an essentially infinite amount of secondary storage in a machine-independent and device-independent fashion. The file system was designed to be independent of machine characteristics. All physical addressing is done by the file system. The user is only aware of symbolic addresses.

Section 2 of this paper presents a hierarchical tree structure of files which permits flexible access control in the file system. File directories exist at every intersection of the tree's branches. Files exist at the tips of all the outer-most branches which do not divide into higher level branches. Each branch contains read, execute, write, append, and trap access controls which may or may not allow a user to access branches, directories, and files further up the tree. The trap control essentially calls a subroutine which can make any checks on the potential user that the file owner desires. A link command is available for providing access links between any nonadjacent branches.

Section 3 discusses a file backup system. This backup system makes secondary storage appear to the user as having infinite storage space. It also provides salvage and catastrophe information-reloads in case of machine breakdown, system failure, or sabotage.

Section 4 describes the basic file and backup systems presented in the preceeding sections as implemented in MIT's MULTICS system. The MULTICS system program modules and their interrelationships are explained. The modular design helps achieve the system's machine independence.

*(2440)*70*ac*ai*cb*dg
"Dangers to Software Security Assessed." COMPUTERWORLD, 26

August 1970, p. S-2.

*(2450)*67*ab*db*hj*kd
Dansiger, Sheldon J. "Embezzling Primer." COMPUTERS AND AUTOMATION, Noverber 1967, pp. 41-43.

*(2460)*68*ab*cc*da*fz*hc*ma
Dansiger, Sheldon J. "Proprietary Protection of Computer Programs." COMPUTERS AND AUTOMATION, February 1968, p. 32.

The author seems to have doubts about the effectiveness of non-disclosure agreements with respect to sold and leased programs. He feels that only by keeping these programs from the premises of the customer, such as through time-sharing, will the necessary protection be obtained.

*(2470)*66*ae*ag*cb*ep
Dantine, D. J. "Communications Needs of the User for Management Information Systems." AFIPS CONFERENCE PROCEEDINGS, Fall Joint Computer Conference, Vol. 29, 1966, pp. 403-411.

*(2480)*70*ae*cb*cc
"Data Base Management System Requirements." JOINT GUIDE-SHARE DATA BASE REQUIREMENTS GROUP, GUIDE International Corporation, 1 Illinois Center, 111 East Wacker Drive, Chicago, Illinois, 60601; or SHARE Inc., 25 Broadway, Suite 750, New York, New York, 10004, 11 November 1970.

Idealized requirements for a database management system are proposed. Security and integrity are important parameters.

*(2490)*72*ad*cb*cc*cd
"Data Center Security Guidelines." GSD 28-070, GUIDE Data Center Security Project, GUIDE International Corporation, 1 Illinois Center, 111 East Wacker Drive, Chicago, Illinois 60601, February 1972.

*(2500)*71*ae*cb*cc
"Data Management System Requirements." Construction Management System Action Group (CMSAG): Data Management Committee, 23 June 1971.

Specific requirements for data security and integrity are discussed.

*(2510)*73*ab*cc*np*x2
DATA PROCESSING DIGEST. Data Processing Digest Inc., 6820 La Tijera Boulevard, Los Angeles, California 90045, 1955-, (Monthly, with annual cumulative index).

Every month this magazine summarizes about twenty current data processing articles found in various magazines and reviews several recently published books. The magazines annually summarizes or reviews about seven or eight articles and books on computer security. The article summaries are not too valuable because they are quite often as long as the original article, which can usually be located quite easily in its original source. However, the book reviews are very useful.

*(2520)*71*ab*cc*dc*dd*de*fy*x2
"Data Processing Errors and Omissions Insurance." BANKING, April 1971, p. 38.

The only known sources for data processing errors and omissions insurance are: Crum and Foster Companies; Fireman's Fund American; Lloyd's of London; Reliance Mutual; and Saint Paul Fire and Marine Insurance Company. The rates and coverage offered by these companies appears to be quite similar. A list of exclusions that apply to this type of insurance is also given.

*(2530)*70*ac*ai*dd*hr*kd*nl
"Data Processing May Receive Scrutiny at FTC Hearing on Credit Card Billing." COMPUTERWORLD, 21 October 1970.

The Federal Trade Commission plans to investigate abuse of customers by computerized billing system errors.

*(2540)*69*ad*ak*cc
"Data Processing Techniques for Management Control of Electronic Data Processing." F20-0006-0, IBM Corporation, White Plains, New York, September 1969.

*(2550)*ac*ai*cc*da*ka*mb*mf*nm*x1
"Data Security and Control Must Go Hand in Hand." COMPUTERWORLD, 19 January 1972, p. 10.

State officials now are attacking an FBI regulation which requires that a computer linked to the National Criminal History System must be used only for law enforcement purposes. These officials insist that adequate hardware and software security can be built into a shared system. This COMPUTERWORLD editorial disagrees. It agrees with J. Edgar Hoover's statement, "If law enforcement or other criminal agencies are to be responsible for the confidentiality of the information in computerized systems, then they must have complete management control of the hardware and the people who use and operate the system".

*(2560)*70*ab*cb*cc*dg*ea*ec*ed*ef*ej*er*fe*ff*fi*gh*ha
*je*kb*lb*nf*x2
"Data Security in the CDB." EDP ANALYZER, May 1970, pp. 1-14.

This article is primarily concerned with security threats and safeguards in a remote-access, time-shared computer environment. It draws heavily on literature from the 1967 Spring and 1969 Fall Joint Computer Conferences, "Computers and Privacy: A Survey" by L. J. Hoffman, and "Considerations of Data Security in a Computer Environment" by IBM. First, security techniques in Continental Airlines' reservation system and experiences of Professor E. L. Glaser, a skilled computer penetrator, are discussed. Then a list of different types of remote-access, time-shared computer threats (developed by H. E. Peterson and R. Turn) and a list of sensitive, common business files are presented. The following countermeasures are briefly discussed: access management (passwords, terminal-identification, Hsiao's user authority items, a brief but quite informative description of the ADEPT-50 system); file design (several levels of access controls, physical separation of files, failure of write operation to completely erase previously recorded data); hardware/software techniques (main memory read and write protection, parity checks, interrupt problems, non-privileged state, certification of systems); communication protection (encryption, dedicated lines, aperiodic check for bugs of the Watergate species); reliability, auditability, integrity (audit trails, validation of program changes); and general security procedures (good security systems shouldn't be weakened by disclosing their techniques, backround checks on employees, assignment of responsibility for every sensitive file). Finally, a list is given of safeguards to implement if highly sensitive data must be stored in a remote-access, time-shared computer.

*(2570)*00*af*cb*da*ep*eq*gh
"DATA SEQUESTOR - Product Description Sheet." Model JJC-3, Ground Data Corporation, 4014 N. E. 5th Terrace, Fort Lauderdale, Florida 33308.

This device provides encrypted communication for remote terminal users. An encoder is provided at the terminal site and a decoder at the computer site. The device can simultaneously handle several different encrypted lines all with different keys. However, the user keys are stored in the computer system and their accessibility will limit the protection available from this device.

*(2580)*00*af*cb*da*ep*eq*gh
"DATACODER - Product Description Sheet." Model DC-110, Datotek Inc., 8220 Westchester, Dallas, Texas 75225.

A device located at the terminal site for protecting transmission and storage of information is described. The device was designed to be used only for encoding "text-only" files. Numeric fields of a record must not be encoded for computation since the device exists only at the terminal and no decoding is possible at the computer site. An example shows a payroll file with the employee names encrypted, and their social security numbers and salaries left uncoded.

*(2590)*69*ab*cb*cc*da*dd*de*gg*hd*ka*mb*md*nm*x2
Davidson, Timothy A. "Computer Information Privacy." THE OFFICE, August 1969, pp. 10-17.

A few advantages and disadvantages are given concerning a proposed federal data bank which will merge all available statistical data now collected by some twenty government departments. Some considerations are: no laws exist on malicious use of personal information; data centralization might produce subjective information on opinions and beliefs; most data on individuals is now collected from unreliable investigators. However, centralized files could tighten the present loose information practices. Some general privacy threats are: securing personal information without the subject's consent; using information without regard to its accuracy or for purposes other than those consented to by the subject; and showing little interest in preventing unauthorized access to data under one's control. The rest of this article briefly summarizes the following security topics discussed at the 1967 Spring Joint Computer Conference: Peterson's and Turn's list of computer threats, software monitoring, and cryptography.

*(2600)*71*ab*cc*cd*dg
Davis, A. G. "Security of the Computer Center." INDUSTRIAL SECURITY, April 1971, p. 20.

*(2610)*68*aa*cc*cd*ff*fq*fp*fv*kb*la*ma*nn*x3
Davis, Gordon B., et al. AUDITING AND EDP. American Institute of Certified Public Accountants Inc., 666 Fifth Avenue, New York, New York 10019, 1968, 344 pp., $12.00.

This book is the result of efforts by a special auditing EDP task force of AICPA members with broad experience in EDP auditing. The book has the following purposes: (1) to guide CPAs in auditing business enterprises which use computers for record keeping; (2) to provide a starting point in building a consensus of expert opinion on auditing practices for examining such companies; (3) to suggest the utility and applicability of different auditing methods where experience is still lacking; and (4) to provide source materials for training and information purposes.

There are fifteen chapters entitled: The Auditor and the Computer, Preferred Practices in Organization and Management of the EDP Function, Documentation of the Data Processing System, Hardware Features for Control Over

Equipment Malfunctions, Control Over Input and Output, Programming Control Over Processing, Safeguarding Records and Files, Evaluating Internal Control, The Audit Trail in an EDP System, Auditing a Computer System Without Using the Computer to Test the Data Processing System, Using the Computer to Test the Records Produced by a Computer System, Auditing Advanced Data Processing Systems, and The Training of the CPA for Auditing EDP.

This is a very important book, especially for auditors, but it has become somewhat obsolete in recent years. Only chapter 7, Safeguarding Records and Files, is directly concerned with computer security.

*(2620)*70*ac*ai*cb*cc*cd*dg*ma

Davis, Morton S. "Service Bureaus Need to Improve Data Security." COMPUTERWORLD, 26 August 1970.

Security problems from both the customer's and the service bureau's viewpoints are discussed.

*(2630)*71*ae*cb*cc*da*db*eh*hd*lb

Dean, Albert Jr. "Data Privacy and Integrity Requirements for On-Line Data Management Systems." ACM Special Interest Group on File Description and Translation (SIGFIDET) Workshop, 11 November 1971.

*(2640)*69*ad*cb*cc*lb*ma

DeLair, W. E. "Security Responsibilities of a Time-Sharing Company." Transdata Corporation, 25 October 1969.

*(2650)*73*ac*ai*cc*db*fi*mk*x2

"Democrats Set Up Guide to Safeguard Elections in 1972." COMPUTERWORLD, 23 May 1973, p. 5.

A workbook passed out by the Democratic Party states that the parties and party workers remain the most important deterrent to election frauds and errors. There have been cases of consistent errors in election results from punch-card ballot counting, but there has not been a case of fraud that has led to a criminal conviction. Several procedural safeguards are given. Two of them are concerned with computerized systems. The source programs should be made available to computer specialists to check for possible areas of fraud. An election night core dump should be made and later compared to the approved source and object code listings.

*(2660)*71*ab*cb*cc

Denning, Peter J. "Third Generation Computer Systems." COMPUTING SURVEYS, December 1971.

Several universal concepts of computer and data protection are presented.

*(2670)*65*ab*cb*hd*hi

Dennis, Jack B. "Segmentation and the Design of Multiprogrammed Computer System." JOURNAL OF THE ACM, Vol 12, October 1965, pp. 589-602.

*(2680)*66*ab*ah*al*ca*ee*x2

Dennis, Jack B.; and Van Horn, E. C. "Programming Semantics for Multiprogrammed Computation." COMMUNICATIONS OF THE ACM, March 1966, pp. 143-155.

The paper is rather technical and requires a good understanding of computer programming. It defines and discusses approximately twenty-five meta-instructions that incorporate powers found mostly absent from contemporary programming languages, but essential to computation processes in multi-programmed computer systems. These powers relate to parallel processing, protection of separate computations, program debugging, and user sharing of memory segments or other computing objects. The meta-instructions form a language whose sophistication is approximately midway between assembly language and advanced algebraic language.

A computation is thought of as proceeding within some "sphere of protection" specified by a "list of capabilities". Each capability list locates by means of a pointer some computing object and indicates the actions that the computation may perform with respect to that object.

*(2690)*66*ad*cb*cc*cd*da*dc*fk*fl*gc*hd*jd*lb

Dennis, Robert L. "Security in the Computer Environment." SP-2440/000/01, System Development Corporation, 2500 Colorado Avenue, Santa Monica, California 90406; or AD-640 648, National Technical Information Service, Springfield, Virginia 22151, August 1966.

This is a digest of presentations made at the Conference of Research Security Administrators. Insuring that information is secure in a time-shared computer; protecting magnetically stored data; avoiding loss of classified information through electronic radiation; and destroying old confidential information are discussed.

*(2700)*62*ab*cc*dc*fy

"Describes Coverage Specially Designed for EDP Equipment." THE NATIONAL UNDERWRITER, 20 July 1962.

*(2710)*70*ac*ai*cc*mk

"Detroit's Canvassers Axe Punch Card Vote." COMPUTERWORLD, 25 November 1970, p. 1.

*(2720)*70*ab*cc*dd*fp*gc*hp

Devitt, R. G. "Cut Expenses by Taking Care of Your Tape." COMPUTER DECISIONS, October 1970, p. 42.

The article describes a tape handling and maintenance program to increase the reliability of magnetic tape.

*(2730)*68*ab*cc*da*db*el*ff*lb
Diamond, T. D.; and Krallinger, J. C. "Controls and Audit Trails for Real-Time Systems." INTERNAL AUDITOR, November 1968.

*(2740)*72*ab*bc*be*cc*cd*dg*fu*gg*x1
Dickey, C. Lewis. "Securing the Computer." JOURNAL OF SYSTEMS MANAGEMENT, February 1972, pp. 8-10.

Causes of losses fall into one of these six categories: accident and natural disasters, environmental problems, EDP equipment malfunction, human error, sabotage, and theft. (The author has not considered fraud.) The following preventive and corrective measures are briefly discussed: site selection and design; physical access regulation; system control (exception reports, input verification, programming halts, backup files, and updating); personnel control (security education and assigning responsibility); testing the security system; and insurance. Each company should first determine the value of its EDP operation and then provide the appropriate safeguards based on this value.

*(2750)*68*ab*ah*cb
Dijkstra, E. W. "The Structure of 'THE' Multi-Programming System." COMMUNICATIONS OF THE ACM, May 1968, pp. 341-346.

*(2760)*66*ab*cc*cd*dc*dd*de*fv*la*x1
Dillon, Gregory M. "How Much Protection for Magnetically Recorded Data?" SYSTEMS AND PROCEDURES JOURNAL, September 1966, pp. 30-33.

The concentration of many businesses records on magnetic media stored in one location, and the concentration of clerical "know-how" in complex computer programs make protection of this compactly and centrally stored information absolutely necessary. The author describes, in detail, steps taken by the treasurer's department of DuPont Company to provide adequate backup without incurring excessive copying and storage expenses. However, a large part of the article is out-of-date and some statements are no longer true.

*(2770)*68*ac*ai*bb*db*mc
"Diners Club Fraud Involved Printout." COMPUTERWORLD, 18 September 1968, p. 1.

*(2780)*70*ac*ai*cb*cc*ne
"Dissatisfaction Expressed with Data Security." COMPUTERWORLD, 11 November 1970, p. 3.

*(2790)*69*ae*cb*eb

Dixon, P. J. "Generalized Data Management Functional Requirements." FILE ORGANIZATION: SELECTED PAPERS FROM FILE 68 - AN I.A.G. CONFERENCE, Amsterdam, 1969, pp. 302-309.

*(2800)*69*af*cb*ei

Dobieski, A. W.; and Wong, R. E. "Optimal Blocking Tactics for Border Security Systems." BULLETIN OPERATIONS RESEARCH SOCIETY OF AMERICA, Vol. 17, Suppl. 1, 1969, p. B109.

*(2810)*71*ab*cb*cc*dd*de

Doll, Dixon R. "Selecting an Error Control Technique." DATA DYNAMICS, August 1971, p. 6.

*(2820)*71*ab*bc*dc*jf*jg

Donati, F. R. "Computers and Catastrophes." DATA MANAGEMENT, December 1971.

*(2830)*72*ab*cb*da*eq*x1

Donn, Edward S. "Secure Your Digital Data." THE ELECTRONIC ENGINEER, May 1972, pp. 5-7.

Extensions in the art and science of pseudorandom binary-sequence generation now make it practical to encrypt information thoroughly before transmission or storage. Diagrams are given on shift registers used for encoding and decoding. Security of the encrypted message increases as the length (in flip-flops) of the pseudorandom bit generating shift register increases.

*(2840)*69*ab*cd*dd*gd

Donnelly, G. J. "Non-Interruptible Electrical Power for a Large Computer System." ELECTRICAL CONSTRUCTION DESIGN, 1969, pp. 31-35.

The rapidly increasing dependence of business decision making and record keeping on data processing systems has created a need for maximum reliability of these systems. System electrical power considerations are discussed.

*(2850)*67*ab*cc*da*f1

Donovan, Robert. "Trade Secrets." SECURITY WORLD, April 1967, pp. 12-18.

*(2860)*65*af*cc*ff*lb*mc

Downs, M. T.; Harlow, W. A.; and Hudson, C. W. "On-Line Banking Auditing." NAA Bulletin, January 1965, p. 57.

*(2870)*73*ac*ai*bb*be*cc*db*de*fj*hk*hp*ka*me*x1

"DP Cited for Drop in Welfare Rolls." COMPUTERWORLD, 25 April 1973, p. 1.

Tighter management and computerization have caused a drop of 17,292 cases in New York's welfare rolls during February. This was a $777,000 monthly savings. The computer reduced agency errors and eliminated many duplicate payments.

*(2880)*71*ac*ai*bb*db
"DP Fraud - Mum's the Word." COMPUTERWORLD, 24 March 1971, p. 6.

*(2890)*72*ac*ai*bc*bf*cd*dc*df*ia*jf*x2
"DP Operator Arrested: Sabotage Was the Problem." COMPUTERWORLD, 2 August 1972, p. 1.

A computer operator was charged with short-circuiting the National Farmers Union Corporation computer system at least fifty-six times in the past two years. But before he was caught, the firm and Burroughs spent $500,000 trying to find the problem which was assumed to be a computer hardware or power line problem. The average down time for the fifty-six instances was eight hours. The operator caused the shorts by putting a metal object between open circuits in the computer's internal disk file.

*(2900)*68*ab*cc*da*el*hn*lb*mc
Drattel, Alan. "Corralling Credit Data." BUSINESS AUTOMATION, February 1968, p. 40.

Credit Bureau Services of Dallas, Texas is automating their processing of credit information. Company management believes the automated system will be more secure than the old manual system, because now only the computer terminal operators will have access to the information (?) whereas before any employee could obtain access. Daily computer-produced reports will be produced on each operator's activities. These operators will also be required to take periodic polygraph tests.

*(2910)*71*ac*ai*da*hd*nm*no
Drattell, Alan. "Survey Shows Privacy Held Less Secure." COMPUTERWORLD, 30 June 1971.

*(2920)*69*ab*cc*da*f1*hc*x1
Duggan, Michael A. "Software Protection." DATAMATION, June 1969, pp. 113-116.

This article briefly discusses the proceedings of a workshop sponsored by Growth/Change Seminars on March 3, 1969 in Chicago. Traditional areas of software protection such as patents, trademarks, copyrights, trade secrets, and contracts are discussed. Most of the article is obsolete, but the following list of safeguard considerations is still useful: will the safeguard prevent or discourage successful theft; will it provide evidence to punish theft after the fact; will it prevent meaningful duplication or imitation; is the safeguard easy or hard to implement; what is to be protected - the idea, the technique, or the expression; is the software self-protecting due to its dynamic nature; and why is the protection sought?

*(2930)*69*ae*ca*ea
Dyche, J. W. "Positive Personnel Authentication by Handwriting." PROCEEDINGS OF CARNAHAN COMFERENCE ON ELECTRONIC CRIME COUNTERMEASURES, University of Kentucky, Lexington, Kentucky, 1969, pp. 114-126.

*(2940)*71*ab*cc*fc*ff*ni
Edds, J. A. "EDP Without Tears." BUSINESS QUARTERLY, (Canada), Spring 1971, pp. 26-34.

*(2950)*70*ac*ai*gg
"EDP Centers Seen Largely Ignorant of Data Protection." COMPUTERWORLD, 19 August 1970, p. 8.

*(2960)*66*ad*al*cb*eq*lb
Edwards, D. J. "On-Line Cryptanalytic Aid System (OCAS)." MAC TR-27, Electrical Engineering Department, MIT, Cambridge, Massachusetts 02139, May 1966.

*(2970)*64*ad*cd*dc*ge*x2
"Electronic Computer Systems 1964." National Fire Protection Association, 60 Batterymarch Street, Boston, Massachusetts 02110, $.60.

This pamphlet provides useful information on fire protection for the computer center.

*(2980)*00*af*cc*dd*de*fp
"Electronic Data Processing and Omissions." Insurance Policy, Chubb and Son Inc., 90 John Street, New York, New York 10038.

*(2990)*70*ab*cd*da*dc*gf*gh*mc*x1
"Electronic Security in the Computer Room." BANKING, May 1970, p. 86.

The importance of computer room security for State Street Bank and Trust Company of Boston is described. A physical access control system utilizing magnetic encoded cards is briefly described. The system is sold by Holobeam Inc., of Paramus, New Jersey.

*(3000)*70*ae*cb*cc*gg*lb
Ellis, Terrance. "Time-Sharing Security." American Management Association Catastrophe Prevention Seminar, 15 April 1970.

*(3010)*68*ad*cb*cc*da*gh*mh*nq
Ellis, William B. "Security Procedures for the RYE System." NSA: C924, National Security Agency, 23 December 1968, (classified).

*(3020)*67*ab*bb*bd*cc*db*dd
"Employees Accused of Illegal Computer Use." DATAMATION, December 1967, p. 78.

Five employees of the Chicago Board of Education were accused of using the Board's computer to operate their own service bureau.

*(3030)*67*ad*cb*fd*gh*mh*ng*x2

Enger, Isadore; Merriman, Guy T.; and Bussemy, Ann L. "Automatic Security Classification Study." RADC-TR-67-472, Rome Air Force Development Center, Griffis Air Force Base, New York, October 1967.

This is a report on the feasibility of using computers to automatically assign security classifications to government documents. Initial results showed computer assigned security levels agreed only 54% of the time with manual assigned security levels. However, the techniques used may still have some future value.

*(3040)*67*aa*cc*da*dc*hb*kb

Engberg, Edward. THE SPY IN THE CORPORATE STRUCTURE AND THE RIGHT TO PRIVACY. World Publishing Company, Cleveland, Ohio, 1967.

Ethical and legal implications of industrial espionage are discussed. Methods and devices used by industrial spies, and countermeasures that can be used against them are described.

*(3050)*70*ac*da*db*dc*hd*hg*jf*ka*mc*nm

Ernest, M. L. "What Else Will Computers Do To Us." WALL STREET JOURNAL, 21 October 1970.

This article mentions several social dangers that can result from companies carelessly using poorly designed computer information systems. Also discussed are: depersonalization, vulnerability, and talent bias; privacy threats of a national information databank; the dangers in monetary transfers using computers; and computer sabotage by industrial spies.

*(3060)*67*ae*ag*cb*da*ed*nc*x2

Evans, David C.; and Leclerc, Jean Yves. "Address Mapping and the Control of Access in an Interactive Computer." AFIPS CONFERENCE PROCEEDINGS, Spring Joint Computer Conference, Vol. 30, 1967, pp. 23-30.

The authors believe that present interactive computing systems are mainly adaptations of conventional computing systems and are far from ideal in many respects. This paper describes a much improved mechanism developed by the authors for protection, address mapping, and subroutine linkage. The particular limitations of present computing systems to which this paper is directed are: the limiting or controlling of access to specified regions of physical memory or to specified units of information; the denying of all direct access to input/output equipment by user programs; the required modification of procedures by program to bind segments together for a computing process; and the lack of a convenient means for handling semi-independent computing processes which should operate concurrently with only limited interaction.

A mapping mechanism is described by which procedures are bound to their parameters at execution time without modification or relocation. Existing address mapping schemes do not provide all of the desired capability. Their most serious defect is that access to a segment of information solely depends on that segment when it should depend on the access path to that segment. The authors' system provides access path control for access of information. This enables strong selective control of access to information, dynamic binding capability at run time, and elimination of arbitrary restrictions on access to I/O equipment. These improvements do not result in substantial cost increases in hardware or software.

Most of the system concepts discussed in this paper were developed by others, but the authors' integrated system design of these concepts is original. Although the paper was very useful in 1967, it is now somewhat obsolete.

*(3070)*71*ad*ak*cb*ec*gh

Evans, J. R.; and Roossien, J. W. "File Protect Circuit and Method." IBM Corporation, White Plains, New York, 15 June 1971.

This article describes a file protection circuit for disk storage control units which prevents users from reading unauthorized information from a disk. Each transfer from a sequentially addressable buffer within the storage control unit is monitored. A blocking mechanism is used to prevent the transfer of data fields when it is determined that the data requested is unauthorized.

*(3080)*72*ad*cb*ei

Fabry, R. S. "Dynamic Verification of Operating System Decisions." Computer System Research, University of California, Berkeley, California, February 1972, 14 pp.

*(3090)*68*ad*ca*ed*ef*el

Fabry, R. S. "Preliminary Description of a Supervisor for a Machine Oriented Around Capabilities." COO-614-64, Institute of Computer Research Quarterly Report No. 18, University of Chicago, Sect. 1, August 1968, pp. 1-97.

*(3100)*72*ab*cc*ff

Fadell, J. F. "The Auditor of the Future." BANKERS MAGAZINE, No. 2, 1972, pp. 76-80.

*(3110)*70*ac*ai*dd*de*ka*mc*nl*nm

"Fair Credit Bill Would Protect Against False Billing." COMPUTERWORLD, 12 August 1970.

*(3120)*68*ad*ak*cb*ed*gh*lb*x1

Falkoff, A. D.; and Iverson, K. E. "APL/360: User's Manual." IBM Thomas J. Watson Research Center, 1968.

One of IBM's efforts to provide file access control is described. The owner of data may specify a password, which is the same for all users, to control access to a work space.

*(3130)*73*ac*ai*be*cc*de*fh*fj*hp*ka*mf*nj*x2

"False Arrests Spark Police Mea Culpa." COMPUTERWORLD, 6 June 1973, p. 6.

After several false arrest suits were filed, the San Francisco police department publicly apologized for inaccuracies in its computer system used to identify wanted persons. The errors appear to be due to human oversight rather than a faulty computer or computer program. One suit is asking for $1,500,00 in damages. The latest suit was brought by a couple who were wrongfully arrested, roughed up, and held for eighteen hours. Their car was stolen two years ago, but it was later returned. The computer system hadn't recorded the return, and the couple was arrested for auto theft.

*(3140)*67*ab*cb*cc*cd*da*gg*nm

Fanwick, Charles. "Computer Safeguards: How Safe Are They?" SDC MAGAZINE, System Development Corporation, 2500 Colorado Avenue, Santa Monica, California 90406, July 1967, pp. 26-28.

This entire issue of SDC MAGAZINE is concerned with computer security and data privacy. The privacy issue is discussed at length. The security issue is given much less coverage.

*(3150)*66*ad*cb*da*gg*hd*ka*mb*nl*nm

Fanwick, Charles. "Maintaining Privacy of Computerized Data." SP-2647, System Development Corporation, 2500 Colorade Avenue, Santa Monica, California 90406, 1 December 1966.

This report discusses the individual's right to privacy, databank threats, and legal and technological safeguards for individual privacy protection.

*(3160)*70*ab*cb*cc*db*ei*el*ff*fi*fk*fx*ia*id*mk*x3

Farmer, James; Springer, Colby; and Strumwasser, Michael J. "Cheating the Vote-Count System." DATAMATION, May 1970, pp. 76-80.

In June of 1969, the authors made public the results of a feasibility study on the vulnerability of computer vote-counting systems to fraudulent software modification. Their conclusions were: the operating system is vulnerable to modification and could permit changes without physical access to the user vote-count program; a vote bias routine would be difficult to detect during the counting process; a valid logic and accuracy test requires a sophisticated computer program or very large amounts of computer time; many vote fraud techniques require only one person's illegal action; and none of the techniques considered would be detected by a casual observer even if he had an extensive EDP background.

The results of this earlier study were unconvincing to some computer professionals because the study did not demonstrate whether such fraud could be performed on systems commonly in use or how much effort would be needed. This paper describes a further investigation by the authors in which they developed a minature vote-counting system and applied fraudulent techniques to it. The results of this second investigstion confirmed conclusions drawn from the initial study. The authors then briefly list several procedural and software safeguards that can be used to minimize the chance of undetected fraud in present vote-counting systems.

*(3170)*72*aa*bg*cb*cc*cd*dg*gg*ha*ja*nb*nc*nf*ni*nn

Farr, M. A. L.; Chadwick, B.; and Wong, K. K. COMPUTERS AND THE PROFESSIONAL - SECURITY FOR COMPUTER SYSTEMS. National Computing Centre Ltd., Manchester, Lancashire, England, 1972, 172 pp.

This book lists threats to computer systems and suggests possible hardware, software, personnel, and computer environment safeguards. It was written to give initial guidance to those concerned with protecting their computer center. The appendix includes a cost effective matrix that briefly summarizes the effects of various techniques as applied with negligible, low, or high cost to different threats.

*(3180)*71*ac*ai*cb*cd*dd*gc*hu*jg*x2
"Fast Circuits May be More Prone to Failure from Everyday Shock." COMPUTERWORLD, 20 January 1971, p. 1.

The faster the circuitry in your computer, the more susceptible it is to errors or failure caused by normal, everyday electric shock. Properly regulated humidity can decrease the likelihood of static problems. It is recommended that computer designers avoid using circuitry faster than what is required for the computer's application. The most common static problem was found to be caused by arcs to ungrounded toggle switches. Several basic grounding rules in installation planning are given.

*(3190)*70*ac*ai*ba*bb*da*db*hd*ii*lb*ma*nj
"FBI Accuses Youth of Tapping T/S Service, Copying Data Files." COMPUTERWORLD, 29 July 1970, p. 1.

A Cincinnati youth faces a five year prison term for unauthorized use of a commercial time-sharing system.

*(3200)*69*ab*ba*cc*da*jc
"FBI Tracks Wandering Wang." BUSINESS AUTOMATION, April 1969, p. 38.

The theft of a $2,500 Wang computer from Argonne National Laboratories is discussed.

*(3210)*71*ad*cb*eb
"Feature Analysis of Generalized Data Base Management Systems." CODASYL Systems Committee Report, Available ACM Headquarters, May 1971.

*(3220)*70*ac*ai*be*cc*db*de*hp*md
"Federal Employee Receives $27,054 Courtesy of Computer Assisted Error." COMPUTERWORLD, 14 October 1970.

A federal government employee received a $27,000 check that was supposed to have been given to a painting contractor. The employee cashed the check and spent $8,000 before the error was detected. The mispayment resulted from a clerical error.

*(3230)*72*ac*bd*be*cc*dd*de*mc*md*x1
"Federal Reserve Computer Error Caused Puzzling Money Mark-Up Steps." WALL STREET JOURNAL, 18 February 1972, p. 19.

The Federal Reserve sold a large amount of treasury bills, causing some money specialists to wonder whether the Fed had changed its easy-money policy in mid-flight. However, the Fed's computer system had given out incorrect information, causing Reserve officials to believe that there were less reserves in the banking system than actually was the case.

*(3240)*71*ad*ak*cb*eq
Feisel, H.; Notz, W. A.; Smith, J. L. "Cryptographic Techniques for Machine to Machine Data Communications." RC 3663, IBM Corporation, White Plains, New York, 27 December 1971.

*(3250)*70*af*cc*da*es*he
Fellegi, I. P. "On the Question of Statistical Confidentiality." ANNUAL MEETING OF THE AMERICAN STATISTICAL ASSOCIATION, 1970, (Unpublished).

*(3260)*72*ab*cc*da*es*he
Fellegi, I. P. "Question of Statistical Confidentiality." JOURNAL OF THE AMERICAN STATISTICAL ASSOCIATION, 1972, pp. 7-18.

*(3270)*71*ae*cc*fy
Felser, G. M. "How Much Longer Will Your Humpty Dumpty Stay on the Wall?" EDP DISASTER PROTECTION WORKSHOP: 18TH INTERNATIONAL CONFERENCE, 1971.

The article discusses EDP insurance matters.

*(3280)*68*ab*cc*fm
Fenske, R. W. "The Full Control of Operations in Data Processing." COMPUTERS AND AUTOMATION, April 1968, p. 16.

*(3290)*71*ab*cc*fz*ma
Fenwick, William A. "Marketing EDP Services: Reviewing the Legal Considerations." COMPUTERS AND AUTOMATION, November 1971.

Several security safeguards to protect the confidentiality of data are discussed.

*(3300)*65*ad*cb*eq
Fiellman, R. W. "Computer Solution of Cryptograms and Ciphers." SRC-82-A-65-32, Case Institute of Technology Systems Research Center, 1965.

*(3310)*70*ad*al*ca*cd*ed
Fillat A. L.; and Kraning, L. A. "Generalized Organization of Large Data-Bases: A Set-Theoretic Approach to Relations." MAC TR-70, MIT, Cambridge, Massachusetts 02139, June 1970.

Some of the limitations of the ring structure for file access control in MIT's MULTICS system are discussed.

*(3320)*68*ab*cb*cc*ek*ff*gh
Findlay, J. C. "Auditing Computer Records." JOURNAL OF INDUSTRIAL ENGINEERING, October 1968, pp. 484-486.

The "auditape" computer audit program is described.

*(3330)*68*ab*cd*dc*ge*jg
"Fire Defenses for Computer Rooms." OCCUPATIONAL HAZARDS, December 1968.
Precautionary steps to guard against heat, fire, smoke, and water damage are described.

*(3340)*72*ab*cd*dc*ge*x1
"Fire Protection for EDP Centers." INFOSYSTEMS, September 1972, pp. 40-41.
This article describes the "Firecycle" water extinguishing system used at Bell Canada's Don Mills Center and a carbon dioxide extinguishing system used at the main EDP center of Owens-Illinois in Toledo, Ohio. Nothing unusual is presented. The superior Halon 1301 extinguishing system is not discussed.

*(3350)*62*ad*cd*dc*ge*jg
Fire Protection for Essential Electronic Equipment." RP-1, Federal Fire Council, Washington, D.C. 20405; or AD-?, National Technical Information Service, Springfield, Virginia 22151, March 1962.
This pamphlet is quite comprehensive and should be a valuable guide for those concerned about fire protection.

*(3360)*70*ab*bc*cd*dc*ga*gf*jf*mj*x1
"Firebombs Damage a Computer Center." THE OFFICE, August 1970, pp. 42-43.
This article describes damage done to the Fresno State College Computer Center when demonstrating students tossed three gasoline bombs through two unprotected windows. A list is presented of fifteen new physical and procedural safeguards taken by the center.

*(3370)*67*ac*ba*bb*da*db
"Fiscal Losses." ELECTRONIC NEWS, 6 December 1967.

*(3380)73*ae*cb
Fletcher, John. "Octopus Software Security." 7TH ANNUAL IEEE COMPUTER CONFERENCE, March 1973.

*(3390)*00*ad*cc*me*nm
Fogarty, Michael S. "Issues of Privacy and Security in the Urban Information System." Northwest Regional Educational Laboratory, Oregon.
The costs and benefits of a large urban computerized data bank are described. Privacy issues are also discussed.

*(3400)*69*ab*cc*cd*da*db*x1
"Foiling the Computer Spy." SUPERVISORY MANAGEMENT, April 1969, pp. 40-42.
This short article superficially discusses several

types of threats and safeguards such as physical access control (guards, alarms), pressurized cables, and some specific auditing techniques.

*(3410)*72*ac*ai*cc*da*hw*mb*nm*x1
"Follow Traditional Security Methods, Canadian Says." COMPUTERWORLD, 22 November 1972, p. 3.

The title of this article only pertains to the article's first sentence where Robert Stanbury, Canadian Minister of Communications, states that traditional precautions such as personnel selection are at least as important as sophisticated lock and password systems. The rest of the article gives some of Stanbury's thoughts on the conclusions reached by a Canadian Task Force studying privacy issues related to computerized databanks. He believes that the privacy issue is under control, although it could develop into a crisis if databank owners don't show some restraint. The task force found that most firms do not store their most sensitive information in computers.

*(3420)*69*ab*cc*cd*da*gf*hb*x2
"Fortifying Your Business Security." THE OFFICE, August 1969, pp. 39-52.

This article is primarily concerned with physical access control for preventing thefts and espionage activities. Computers and data processing are not given any special attention. Some of the items discussed are: closed circuit TV; bugging devices; exterior fencing and lighting; various mechanical and electrical locks; alarms; and alarm monitoring. Advantages and disadvantages were given for the following alarm devices: contact switches, capacity alarms, motion detectors, photoelectric alarms, ultrasonic alarms, audio systems, radar and microwave motion detectors, automatic telephone dialers, and vibration detection system. Unauthorized visitors are probably one of the biggest causes of office thefts. Any firm with over $500,000 in annual gross sales should consider itself a target for industrial espionage.

*(3430)*70*ab*dc*ge*jg
Ford, Charles. "Halon 1301 Fire Extinguishing Agent." FIRE JOURNAL, November 1970.

For information about Fenwal's Halon systems, write Fenwal Inc., 400 Main Street, Ashland, Massachusetts 01721.

*(3440)*71*ab*cc*da*fh*hd*ka*mb*nl*nm*x2
Foster, Caxton C. "Data Banks - A Position Paper." COMPUTERS AND AUTOMATION, March 1971, pp. 28-30.

The author first attempts to show that there are some very real dangers associated with today's personal databanks. Several threats such as machine failure, logical errors, wiretapping, unauthorized access, and bad input data are discussed. The most difficult problem to control will be the overzealous administrator who can, and must, because of his job, have access to the databanks at will. The author proposes twelve legal and regulatory safeguards that must be implemented if an individual's privacy is to be truly protected. Some of these safeguards are: the right not to answer non-pertinent questions; the right to access and challenge data; the right to restrict distribution of one's personal data; government regulation of databanks with periodic testing; approval of all merged databanks; and required notification of all individuals whose personal data is stored in a databank. Maintaining a databank should be made a legal privilege, not a legal right.

*(3450)*68*aa*cb*cd*da*db*hb*nm
Foster, J. E. ELECTRONICS AND PRIVACY: SECURITY ASPECTS. Avco Lycoming Division, Stratford, Connecticut, March 1968.

This article discusses how electronic devices can be used for protecting privacy instead of just invading it. Technology in defensive devices has usually lagged behind that of offensive devices. Privacy and security need to be given more attention when designing electronic devices.

*(3460)*73*ab*cc*ff
Francis, F. A. "An Integrated Approach to Computer Audits." THE INTERNAL AUDITOR, January 1973.

*(3470)*72*ac*ai*cb*da*ep*eq*je*lb*x2
Frank, Ronald A. "Phone Lines Prone to Compromise." COMPUTERWORLD, 6 December 1972, p. 19.

Some AT&T company policies and hardware safeguards pertaining to information security are discussed in this article. The company only allows wiretapping ordered by a court and only if further ironclad documentation and assurances are given. There is little hard proof that unauthorized wiretapping is occurring in any significant amount. A firm named Datotek Inc. supplies encrypting devices for protecting remote communications with computers. These devices can be rented at a price between $150 and $250 per month.

*(3480)*72*ac*ai*cb*dg*ea*lb*ma*x1
Frank, Ronald A. "T/S Vendors Stress Security of Terminal, Net, CPU." COMPUTERWORLD, 6 December 1972, p. 21.

The author states that, "While most users fall short of encrypting all their data, elaborate measures are implemented by all time-sharing vendors to protect their user's information." One should be skeptical about this statement because most literature on service bureaus indicates that their security safeguards are quite inadequate. In fact, the only safeguards discussed in this article are a few applications of simple passwords.

*(3490)*69*ab*bb*cc*db*ff*hj*kb*kd*ne*nj*x1
Freed, Roy N. "Computer Fraud: A Management Trap." BUSINESS HORIZONS, June 1969, pp. 25-30.

This article attempts to alert management to legal and other dangers of continuing to use computers for business accounting without taking adequate precautions against embezzlement. Several examples of computer embezzlement are briefly described. Each corporate officer has a legal duty to his company to exercise the care in performance of his duties that a "reasonably prudent" man would devote to his own business. Moreover, he is legally obligated to reimburse his corporation for all losses resulting from his failure to exercise such care. Coporate officers who sign securities registration statements are liable to stockholders under Section II of the Securities Act of 1933 for misleading omissions of fact. When adequate internal controls are missing and haven't been compensated for in an audit, CPA's must so state this in their opinions or risk legal liability under SEC law. A few simple accounting control procedures for detecting and preventing embezzlement are briefly described.

*(3500)*69*ad*cc*fz
Freed, Roy N. "Get the Computer System You Want." HARVARD BUSINESS REVIEW, November 1969, pp. 99-108.

Guidelines for computer contracting are presented.

*(3510)*69*aa*bg*cc*dg*fy*nj
Freed, Roy N. MATERIALS AND CASES ON COMPUTERS AND LAW. Boston University Bookstore, Boston, Massachusetts, 1969.

*(3520)*70*ae*ag*cc*df*dg*fz*ma*nk*x3
Freed, Roy N. "The Role of Computer Specialists in Contracting for Computers - An Interdisciplinary Effort." AFIPS CONFERENCE PROCEEDINGS, Fall Joint Computer Conference, Vol. 37, 1970.

The complexity of computer-communications technology requires computer specialist involvement in the negotiation and structuring of legal contracts relating to computer systems. This paper suggests means for making such involvement as fruitful as possible for all parties concerned.

Computer specialists must be called upon to identify the pertinent facts in contractual transactions, which might include: the nature of the customer's needs; technical aspects of the products or services considered to fill their needs; and types of business approaches available to secure those products or services. They must also: prepare specifications covering the supplier's performance; select ways for determining whether performance is satisfactory (acceptance tests); identify possible needs for maintenance; determine the likelihood that a particular program will be enhanced; determine items that could comprise a specific software package; evaluate the risk that a particular proprietary package will be stolen; point out jeopardies to file information in time-sharing applications; propose means for preventing unauthorized access; and identify any other needs for legal protection. The lawyers' responsibilities include: verbalizing the details of relationships; reducing complicated arrangements to writing; and prodding the parties for an identification of potential circumstances that require advanced treatment.

A critical factor is the need to make the customer truly independent from the supplier after a sound committment period of a reasonable length of time and even during that period if the supplier falls down on his contractual obligations. It is also essential that substantially all of the written agreement, if not the entire agreement, be readily understandable by non-technical individuals.

*(3530)*72*ab*cc*df*dg*fb*fc*ff*fg*fk*fn*fp*fs*fu*fw*fx *kd*mc*nb*nc*nf*nj*nn*x4

Freiser, J.; and Snelling H. T. "Bank Management's Role in EDP Security." THE BANKERS MAGAZINE, Winter 1972, pp. 78-83.

The advice given in this article can be useful to any organization making use of computers, not just the banking industry. The authors state that total security responsibility cannot be incumbent on the EDP manager because he serves as intermediary or caretaker of vital data at only one stage in a complex process. They believe that the responsibility for security should ideally be shared at five levels, each with a differing involvement, level of sophistication or technical expertise, and point of view. The user (level 1) should be primarily responsible for advising the EDP security coordinator (level 5) of: the value of the file; its sensitivity; probable consequences if the file is destroyed, modified, or exposed; and consequences if it cannot be processed. The user should be aware that the reconstruction cost of the file is often smaller or larger than the value of the file to the firm! EDP management (level 2) should be responsible for: all aspects of physical security; reliability (e.g. air conditioning and power supply); EDP personnel including training and supervision; low-level backup decisions such as additional peripheral equipment needs; tape, disk, and other storage media; and operating procedures. A records retention group (level 3) should be responsible for developing standards based on the firm's specific needs as well as legal requirements, the most important being the Internal Revenue Service. This group should also: examine the firm's on-site and off-site file backup needs; develop emergency, contingency, and disaster recovery plans; and aperiodically test these plans. The audit team (level 4) should be responsible for determining the integrity of all important files. This is normally an after-the-fact, detection-oriented safeguard. The audit team should also examine and give opinions on any possible weaknesses they feel exist in the security program. Computer security personnel (level 5) should be responsible for most of the planning, coordinating, and implementing of the EDP security program. They should have expertise in EDP technology and financial audit techniques, and have legal council available on an "as needed" basis.

The authors list the following twelve "instant security-audit" techniques which a non-technical executive can examine, even on a walk-through basis, to determine the need to allocate more resources to improving security: showcase data center, the open shop, bad housekeeping, inadequate physical and environmental precautions, low employee morale, supervision and training, rotation of duties, lack of adequate file and documentation control, lack of file and site backup, absence of comprehensive operating procedures, absence of security audits, and a mechanical gadgets approach to data security. A few suggestions are given for improving the cost/effectiveness of EDP security. It should be realized that not all security safeguards are pure financial drains. Many result in effectiveness and efficiency improvements that alone may justify their cost.

*(3540)*72*ab*bd*cc*df*dg*fz*ma*nj*nk*x3
Friedman, R. C. "EDP and the Law." DATA MANAGEMENT, August 1972, pp. 14-15.

During the next few years the EDP industry could be involved in numerous lawsuits arising from increased liability within the vendor-user-public relationship. This article investigates two recent and important legal actions. One of these indicates that vendor liability will soon extend beyond pure hardware/software performance to include damages resulting from a malfunction of their hardware or software. This liability may also extend one step further to make the vendor responsible for damages sustained by clients of the computer user as a result of vendor hardware/software errors. The above liabilities now exist for other manufactured products and may soon be extended to the EDP industry. In the other recent legal action, a Colorado court established an important legal precedent in ruling that a company is legally responsible for actions of its computer, as if those actions were that of humans. The author suggests that vendor-user written contracts be reviewed and that very explicit enumeration of responsibility for consequential damages be made. Performance standards should also be made part of this contract. Users who deal with the public are faced with a greater chance of a lawsuit, and they need even more careful examination of their liabilities.

*(3550)*70*ad*ak*ca*cb*ed*ee*ef*ei*ej*fe*lb*nc*ng*x3
Friedman, T. D. "The Authorization Problem in Shared Files." IBM SYSTEMS JOURNAL, Vol. 9, No. 4, 1970, pp. 258-280.

The author defines "authorization" as determining whether a user who is correctly recognized by the computer system should be allowed to access information he desires. In most of the literature on computer security, Friedman's "authorization" is referred to as "computer access control", and authorization refers to granting access rights through human interaction outside the computer system. However, Friedman's definition will be used in this annotation. This paper considers authorization (Friedman's definition), as far as possible, apart from specific access mechanisms or operating systems. It also suggests directions for future study and research. Information protection is considered only with regard to secondary storage in general-purpose, time-sharing systems. The authorization problem within main storage is not considered.

The authorization problem can be viewed as a matrix where the columns of the matrix represent particular data items in the system, the rows represent users of the system, and each element, d(i,j), in the matrix represents a decision rule specifying the conditions under which user "i" is entitled to access the data item "j" and the actions that "i" is permitted to perform upon "j". Authorization is not so much a theoretical problem as one of implementation efficiency. A matrix mapping function, easily implemented in specialized applications, may be unmanageable in most general-purpose, time-sharing systems.

Unauthorized access may be disabled during log-on when the user requests information, when the system selects the information, or when the system transmits the information. Each disable period allows different protection capabilities. A program can, in common situations, require more or less access privileges than the person who invoked it. An ideal authorization mechanism should: not disclose information to unauthorized parties; not be "breakable" by persons understanding its operation; allow data owners to easily specify allowed access; allow all common file processing operations; not significantly increase response time; place few restrictions on the operating system; not require users to remember long lists of passwords; and not depend upon continuous attention of a security officer.

The author then proposes a hypothetical authorization system which considers the above ideal characteristics. The system includes: isolation of the authorization mechanism from the operating system; access limitation where files can only be accessed by means of the authorization system; adjacent tagging where access control tags are kept adjacent to the data itself; a single-tag rule where a new tag replaces an old one instead of adding a second tag; and compartmentalization where all data similarly restricted to certain users are assigned a common protection tag. The above characteristics are then expanded in an illustrative authorization model. A possible drawback of this system is that the protection information is stored with the data. Hoffman, Hsiao, and Manola believe that protection information should be separated from the data.

*(3560)*67*af*cb*da*eq
Friedman, W. F. "Cryptology." ENCYCLOPEDIA BRITANNICA, Chicago, Illinois, Vol. 6, 1967, pp. 844-851.

*(3570)*70*ab*cc*ff
Fritzemeyer, J. R.; and Spinelli, C. C. "Auditing Accounts Receivable by Computer - A Case History." JOURNAL OF ACCOUNTANCY, April 1970.

*(3580)*73*af*cc*np*x1
FUNK AND SCOTT INDEX OF CORPORATIONS AND INDUSTRIES: SECTION 1 - INDUSTRIES AND PRODUCTS. Predicasts Inc., 200 University Circle Research Center, 11001 Cedar Avenue, Cleveland, Ohio, 1962-, (Annually).

This index covers company, product, and industry information from over 750 financial publications, business-oriented newspapers, trade magazines, and special reports. Computer security articles can be found under the index "computer services" (numbered 73991 or more recently 73700) and sub-indicies "computer service bureaus", "computer software", "sociological factors", and "information services". Each annual publication contains about fifteen references to computer security articles. Most of these articles come from DATAMATION, INDUSTRY WEEK, and COMPUTERWORLD.

*(3590)*70*ab*cb*cc*fe*hd*ka*mg*nm*x2
Gabrieli, Dr. E. R. "Right of Privacy and Medical Computing." DATAMATION, April 1970, p. 173.

This article summarizes the proceedings of a four day conference (October 2-5, 1969) on "The Use of Computers in Clinical Medicine". The conference was sponsored by Continuing Medical Education, State University of New York at Buffalo. The purpose of the meeting was to formulate some privacy related recommendations, rather than to reiterate already known arguments. A 200 to 400 word summary is given on each of twelve speeches presented at the conference. Some of the more interesting comments are presented below.

The release of medical information should be based on: the purpose of the request, the nature of the information requested, who is requesting the information, and the need for the patient's written consent. Adding privacy safeguards to present computer systems should cost about $15,000 in one-time storage costs and about two to ten percent in additional operating time. The crux of objections to health databanks is that inevitably there will be pressure for the release of this information. The pressure could be from employers, credit agencies, police, private investigators, etc.. Would the databank administrator be sufficiently independent to withstand such pressures? Legal justice and scientific progress frequently demand use of medical data at the expense of personal privacy. In some states, private communication between the patient and doctor is not considered privileged in court. Until these problems are solved, it is ridiculous to try to build a basis for privacy in massive databanks.

*(3600)*70*ab*cc*fc*ff
Gage, R. W. "A Leadership Opportunity for the Internal Auditor." THE INTERNAL AUDITOR, July 1970.

*(3610)*56*aa*cb*da*eq
Gaines, H. F. CRYPTANALYSIS. Dover Press, New York, 1956.

This book describes in great detail cryptanalytic techniques that can be used to break ciphers.

*(3620)*72*ab*ah*cb*ed*el
Gaines, R. Stockton. "An Operating System Bases on the Concept of a Supervisory Computer." COMMUNICATIONS OF THE ACM, March 1972.

*(3630)*67*ab*cc*da*fe*fs*hd*ka*mf*nl*nm
Gallati, Robert R. J. "Criminal Justice Systems and the Right to Privacy." PUBLIC AUTOMATION - OUTPUT, July 1967.

Some limitations for criminal justice databanks, and a six-point policy program for providing data security and protecting individual privacy are discussed.

*(3640)*70*ad*cc*da*ka*lb*mf*nm
Gallati, Robert R. J. "Security and Privacy Consideration in Criminal History Information Systems." Technical Report 2, Project SEARCH, California Crime Technological Research Foundation, 1108 14th Street, Sacramento, California 95814, July 1970.

This report was written to serve as a reference on privacy and security matters dealing with criminal history information systems (especially Project SEARCH).

*(3650)*67*ae*ag*cb*cc*da*gg*hd*ka*lb*mf*nm
Gallati, Robert R. J. "Security and Privacy Policy." Speech Presented at AFIPS CONFERENCE PROCEEDINGS, Spring Joint Computer Conference, 1967.

The results of studies by the New York State Identification and Intelligence System (NYSIIS) are presented. The studies analyzed problems of security and privacy relating to New York's state-wide computerized criminal information system. This system serves over 3600 agencies in six different areas of criminal justice administration. Solutions are offered for consideration, with a view of aiding others in finding insights into similar problems.

*(3660)*72*ab*bc*cd*dc*gc*hi*jd*jg*x2
Gans, Rudolph, F. "Magnetic Pollution: Is it for Reel?" INFOSYSTEMS, December 1972, p. 52.

Although it takes a relatively strong magnetic signal to erase or degrade a magnetic tape, there are many documented cases which show that the accidental loss of magnetic tape data is a common problem. Lighting, magnets, radar, and power generating equipment all present problems to magnetically stored data. The author states that tape transports are available for partially protecting magnetic tapes. Only containers made of special magnetic alloys can offer protection, and no containers can offer 100% protection. Plastic or other fiber material transports offer no protection. However, even if protective containers are used, good housekeeping procedures must be enforced if protection is to be achieved.

*(3670)*66*ab*cb*cc*da*db*dc*fi*hc*kb
Garland, Robert F. "Computer Programs - Control and Security." MANAGEMENT ACCOUNTING, December 1966.

Some good techniques to protect computer programs are given.

*(3680)*71*ae*cb*dd*de*el*ke*mh
Garrett, J. W. "Security Considerations in Process Computer

Interface Design." PROCEEDINGS OF THE 6TH ANNUAL CONFERENCE ON THE USE OF DIGITAL COMPUTERS IN PROCESS CONTROL, Louisiana State University, Baton Rouge, Louisiana, February 1971, pp. 24-29.

The architecture of a computer-process interface and its relation to system security are discussed. Good architecture can be achieved by defining failure modes and designing the interface to detect and minimize the effect of these failures. This improved architecture need not increase the price of the system. Many validity checks and error traps should be performed by the software, but adequate hardware inputs must be present to give software the ability to recognize all serious errors and failures.

*(3690)*70*ad*cb*ea*ec*ed*ej*el*ep*eq*ff*gg*gh*ng*nh*nl *nn*x2

Garrison, William A.; and Ramamoorthy, C. V. "Privacy and Security in Data Banks." AD-718 406, National Technical Information Service, Springfield, Virginia 22151, November 1970, 120 pp.

This paper is primarily concerned with presenting and comparing hardware and software techniques for preventing illegal access to information stored within the computer. The paper is a good summary of about twenty other papers, but it doesn't appear to contain any original or uncommon ideas. Four of seven chapters require some technical knowledge of computers to be adequately understood. A large number of data access safeguard techniques are presented. However, none are discussed in any depth. Throughout the paper the authors have attempted to list or classify the different: advantages to pooling information; types of legal and administrative safeguards; data access threats; types of information stored; types of databank users; functions of a secure databank; identification techniques; types of information activities; file processing restrictions; memory protection techniques; surveillance functions; and cryptography techniques. Four cryptography techniques are compared on a cost, coding efficiency, memory requirement, and security level basis. The current status of the Cambridge University File Protection System, the Berkeley Computer Corporation - Model 1 System, the RUSH Time-Sharing System, and the ADEPT-50 Time-Sharing System are described and compared. Some possible areas of future research are also suggested.

*(3700)*71*ae*cb*da*ed*ef*hc*ka*mg*nm

Geblat, M.; and Hsiao, David. "Privacy Measures and Data Accessibility in a Medical System." FOURTH ANNUAL MEETING OF THE SOCIETY FOR EPIDEMIOLOGIC RESEARCH, 21 May 1971.

This article describes the Cardiovascular Research

Databank System designed by the Moore School of Electrical Engineering, University of Pennsylvania. Users of the system are given access control authority items. Protection can be implemented down to the field and record level. A file owner can also write a special access control program to screen all persons who attempt to use his file.

*(3710)*73*ab*cb*da*eq
Geffe, P. R. "How to Protect Data With Ciphers That are Really Hard to Break." ELECTRONICS, 4 January 1973, pp. 99-101.

Many ciphers in use today are based on encoding techniques that are vulnerable to solution by linear equations. A non-linear encoding scheme will provide a much more secure cipher.

*(3720)*70*ab*ba*bb*cc*cd*dg*ha*ne*x1
Gellman, Harvay S. "Crime in Industry: Using the Computer to Steal." VITAL SPEECHES OF THE DAY, 15 December 1970, pp. 152-155.

This article attempts to briefly point out many different types of threats to computers and computerized data. It tries to convince the reader that more than superficial security measures are necessary for adequate protection. Sixteen examples of computer fraud, theft, and destruction are given. The article is directed to those people who are unaware of the importance of computer security. It is exactly the same as two other articles by Gellman entitled "How the Computer can be Used to Rob You Blind" in RISK MANAGEMENT and "Using the Computer to Steal" in COMPUTERS AND AUTOMATION. Nothing new or unusual is presented.

*(3730)*71*ab*ba*bb*cc*cd*dg*ha*ne*x1
Gellman, Harvey S. "How the Computer can be Used to Rob You Blind." RISK MANAGEMENT, August 1971.

This article attempts to briefly point out many different types of threats to computers and computerized data. It tries to convince the reader that more than superficial security measures are necessary for adequate protection. Sixteen examples of computer fraud, theft, and destruction are given. The article is directed to those people who are unaware of the importance of computer security. It is exactly the same as two other articles by Gellman entitled "Using the Computer to Steal" in COMPUTERS AND AUTOMATION and "Crime in Industry: Using the Computer to Steal" in VITAL SPEECHES OF THE DAY. Nothing new or unusual is presented.

*(3740)*71*ab*ba*bb*cc*cd*dg*ha*ne*x1
Gellman, Harvey S. "Using the Computer to Steal." COMPUTERS

AND AUTOMATION, April 1971, pp. 16-19.

This article attempts to briefly point out many different types of threats to computers and computerized data. It tries to convince the reader that more than superficial security measures are necessary for adequate protection. Sixteen examples of computer fraud, theft, and destruction are given. The article is directed to those people who are unaware of the importance of computer security. It is exactly the same as two other articles by Gellman entitled "How the Computer can be Used to Rob You Blind" in RISK MANAGEMENT and "Crime in Industry: Using the Computer to Steal" in VITAL SPEECHES OF THE DAY. Nothing new or unusual is presented.

*(3750)*00*ad*cc*db*f1

"General Information on Copyright." Copyright Office, Washington, D.C. 20540.

This circular gives introductory information for obtaining a copyright. Another circular on obtaining computer program copyrights is also available upon request.

*(3760)*00*aa*cb*cc*cd*da*hb*lb

Gerhard, William D. NETWORK OF COMPUTERS. National Security Agency, Fort George G. Meade, Maryland 20755.

Thirty pages of this book are devoted to computer security. Nothing really new or unique is discussed.

*(3770)*72*ac*ai*bb*cc*db*hm*mj*x2

"Ghosted Programs for Sale." COMPUTERWORLD, 22 March 1972, p. 1.

The practice of hiring outsiders to write term papers has spread into the computer science department at the University of Michigan. At least one firm, Creative Research, performs programming services for students. For a relatively small and simple program the fee is from $10 to $15. Creative Research acts as a middleman operation by contracting advanced computer students and local business programmers to do the programming. These programmers usually use the university computer for program testing and debugging. Since they can implement working programs more efficiently, they are able to use the student's unused allotted programming time for their own purposes.

*(3780)*73*ab*bb*cc*db*hj*mc*x1

"Ghostly Insurance." TIME, 16 April 1973, p. 90.

The Equity Funding Corporation scandal, one of the largest scandals in U.S. history, is briefly described. The firm created fictitious insurance policyholders, put them on their books, and sold the phoney policies to other companies in the business of reinsurance. Under this arrangement the reinsurer pays the company that sold the policy $1.80 for every $1.00 it gets in premiums the first year. The buyer hopes to make a profit on premiums of later years, while the seller continues to service the policy. Up to $1 billion of Equity's $6.5 billion in insurance is expected to be fake. At later stages of the scandal, large groups of Equity Funding employees knew of and participated in the scandal. The computer played a major role in deceiving outside auditors.

*(3790)*72*ab*cb*da*eq*gh*nk*x4

Girsdansky, M. B. "Cryptology, the Computer, and Data Privacy." COMPUTERS AND AUTOMATION, April 1972, pp. 12-19.

This article first presents a description of the Vigenere and Vernam encipherment techniques, and a loop system for producing extra long keys for these two techniques. This is followed by an excellent very detailed discussion of how and under what circumstances these ciphers can be broken. Bryant Tuckerman, an IBM researcher whose work is the basis for much of this article, found that most Vigenre and Vernam techniques can be broken with surprisingly little effort. The multiple-loop system provides surprisingly little additional security to these two techniques. Methods used to break these ciphers are also explained in some detail. The first part of this article should definitely be read by those seriously interested in cryptography.

The author states that surprisingly secure ciphers can be produced with the successive application of relatively simple substitution and transposition methods. An IBM cryptographic system named "LUCIFER" is then explained in some detail. This system is based on successive application of substitution and transposition methods developed by IBM's Horst Feistel. The system was implemented using a combination of hardware and software developed by William A. Notz and J. Lynn Smith. It encodes and transmits data in 128 bit blocks, can be attached to any terminal, and is compatible with all System 360 equipment.

*(3800)*71*ad*ak*cb*da*eq*gh*ng

Girsdansky, M. B. "Data Privacy: Cryptology and the Computer at IBM Research." IBM RESEARCH REPORTS, Vol. 7, No. 4, IBM Corporation, White Plains, New York, 1971.

This report describes research being done by IBM to devise unbreakable ciphers. Most conventional encipherment schemes are easily broken with the aid of a computer. The LUCIFER hardware encryption device is also described.

*(3810)*67*ae*ag*cb*da*ed*gh*lb*x2

Glaser, Edward L. "A Brief Description of Privacy Measures in the MULTICS Operating System." AFIPS CONFERENCE PROCEEDINGS, Spring Joint Computer Conference, Vol. 30, 1967, pp. 303-304.

All references to data are made by symbolic name and never by physical address. Each file has an associated access-control list defining authorized users. The log-in routine not only includes passwords, but can also include special log-in algorithms. A combination of hardware and software safeguards is used to prevent the user from gaining access to privileged instructions. The operating system activities are separated in program modules which help to minimize illegal disclosure of the entire system. The system can record extensive audit trails on any specified user or program.

*(3820)*68*ae*cb*cc*dg*gg

Glaser, Edward L. "The Safeguarding of Information: A User's View." PROCEEDINGS OF THE FOURTH INTERNATIONAL FEDERATION FOR INFORMATION PROCESSING (IFIP) CONGRESS: Supplement Booklet 1, (Amsterdam: North Holland), August 1968, pp.13-16.

*(3830)*65*ae*ag*cb*el*gh*lb*x1

Glaser, Edward L. "Systems Design of a Computer for Time-Sharing Applications." AFIPS CONFERENCE PROCEEDINGS, Fall Joint Computer Conference, Vol. 27, 1965, pp. 197-202.

The modifications of a General Electric 635 computer for MIT's MULTICS System are described in this article. A totally new I/O control unit was designed, as well as a new high speed drum system for secondary storage. But by far the most significant change was the introduction of a new form of addressing logic incorporating segments and pages. The system also utilizes three distinct modes of execution. Most of the paper is devoted to discussing, memory allocations and addressing schemes. The paper is quite technical and only indirectly concerned with computer security.

*(3840)*71*ab*ba*da*hd*lb

Godbout, W. "Computer Theft by Computer." SECURITY WORLD, May 1971.

*(3850)*72*ab*cc*da*f1*nc*ng*x4

Goldberg, David. "Legal Protection of EDP Software." DATAMATION, May 1972, pp. 66-70.

The author, a lawyer, describes various advantages and disadvantages of using patents, statutory copyrights, common law copyrights, and trade secrets for protecting computer software. He concludes that none of these provide adequate protection, although a combination of common law copyright and trade secret protection appears to offer the best alternative under current law. Pending legislative and non-legislative developments are also analyzed. The author feels that a proposal by IBM, although not pleasing in every detail, offers a highly desirable form of protection. IBM's proposal is for a registration system. Protection duration would be for a relatively short period, and liability would be incurred for unauthorized duplication, translation, or use. Although the author's discussion on patents is obsolete, the remaining 95% of this article is still quite relevant. Because of the quickly changing nature of the subject, there are few, if any, other articles that are both more comprehensive and more up-to-date (as of May 1973).

*(3860)*72*ad*ak*cb*da*dc*dd*eb*ed*ht*hu*na
Goldberg, S. L.; and Woodrum, L. J. "Data Security and Recovery Techniques." IBM TECHNICAL DISCLOSURE BULLETIN, Vol. 14, No. 11, April 1972, pp. 3286-3287.

Most existing computer error detection and correction techniques are only capable of correcting a single bit or byte. The author describes a storage method that can recover an entire disk track of destroyed data. This storage method can also protect against unauthorized access of the data.

*(3870)*70*ae*cb*da*eb*gh
Goldstein, Robert C.; and Strnad, Alois J. "The MacAIMS Data Management System." ACM Special Interest Group on File Description and Translation (SIGFIDET) Workshop, 1970.

*(3880)*73*ab*cc*fb*fm*nc
"Good Management of Computer Operations." COMPUTERS AND AUTOMATION, February 1973, pp. 20-24.

*(3890)*73*ab*ba*bd*cb*da*ep*eq*hb*kb*x1
Goode, George E. "Security for Teleprinters and Data Communications." DATA MANAGEMENT, January 1973, pp. 21-26.

There is a greater need for data security for the following reasons: growth in communications, increased competition, increasing pressure applied by governments, growth of crime, and easier availability of electronic snooping devices. Sales information, financial information, legal negotiations, plans for expansion, production data and problems, geographical exploration, personnel data, and payroll data are targets of industrial espionage. Examples are given of sensitive information getting into the wrong hands either by accident or by fraud. These examples appear to be unique to this article. However, the firms involved were not revealed.

The author, president of Datotek Inc. (a seller of cryptographic equiptment), uses the remaining two-thirds of this article to describe a device his firm markets, which encodes and decodes data transmitted between teleprinters. The device is described only in very general non-technical terms. Its true security and efficiency can not be determined from this article.

*(3900)*70*ae*cb*da*gg*hd*lb*mb*nm
Goodfellow, B. B. "Projections of the Impact of Technology on the Development of Large Data Base Information Systems." CONFERENCE ON COMPUTERS: PRIVACY AND FREEDOM OF INFORMATION, Queen's University, Kingston, Ontario, Canada, May 1970.

*(3910)*64*ab*cc*db*ff*kb*kd*x1
Goodman, John V. "Auditing Magnetic Tape Systems." THE COMPUTER JOURNAL, July 1964.

Very little of the article is applicable to systems other than fully magnetic tape systems.

*(3920)*70*ab*cc*da*fd*hd*ka*mb*nl
Gotlieb, C. C. "Regulations for Information Systems." COMPUTERS AND AUTOMATION, September 1970, pp. 14-17.

The author suggests that information systems be classified. He also examines the goals, methods, and costs of information system regulation.

*(3930)*70*ab*ba*cc*da*jc*md*me
"Government Offices Lose Things Too." THE OFFICE, August 1970.

*(3940)*71*ad*cb*dg*ed*ei
Graham, G. Scott. "Protection Structures in Operating Systems." Master's Thesis, Department of Computer Science, University of Toronto, Canada, August 1971.

*(3950)*72*ae*ag*ca*dg*ee*ei*ej*el*gh*nc*nh*x4
Graham, G. Scott; and Denning, Peter J. "Protection - Principles and Practice." AFIPS CONFERENCE PROCEEDINGS, Spring Joint Computer Conference, Vol. 40, 1972, pp. 417-429.

An abstract access control model is developed which provides a basis for comparing and evaluating quite different access control systems. It can also be used to: isolate the elements of protection; formulate methods for proving the correctness of a protection system; and identify nontechnical issues required to complement the technical ones.

The model is based on a security matrix where the columns of the matrix correspond to particular objects, "X", to which access must be controlled (files, devices, subjects), and the rows correspond to particular subjects, "S", which are active entities whose access to objects must be controlled. Each element of the matrix, A(S,X), corresponds to a particular set of rules in which subject "S" is permitted access to object "X" and the actions that "S" is permitted to perform upon "X". The authors present a set of eight commands which the access control monitor uses to modify the security matrix. The entire protection system is viewed as a set of subjects, monitors, and objects. The subjects can access the objects only through the monitors. All monitors (file system, memory addressing hardware, terminal manager) can read the security matrix, but only the access control monitor can modify it. Beside the very common subject-object attributes of read, write, and execute, several other very interesting attributes such as: copy flag, transfer only, limited use, and indirect use are described. Dennis and Van Horn's capability list, Lampson's domains of capability, the MULTICS system's access control list, and IBM's system of locks and keys are all discussed in the context of this abstract model. The model clearly shows where technical access control safeguards can provide no protection and where legal and procedural safeguards must be implemented.

This article is required reading for anyone concerned with designing access control systems. It can also be quite educational for other readers. However, it is somewhat technical and requires a fair understanding of internal computer operations.

*(3960)*68*ab*ah*al*cb*dg*ec*ed*ei*gh*x2

Graham, Robert M. "Protection in an Information Processing Utility." COMMUNICATIONS OF THE ACM, May 1968, pp. 365-369.

The problems of protecting both user and system information during the execution of a process are the primary concern of this article. The author feels that a satisfactory protection mechanism should have the following properties: any user should be able to deny access by other users to all of his memory segments; it should be easy for a user to control access privileges of other users; layers of protection should be available to apply a "need to know" philosophy to any degree; and procedures should be able to be called across layers of protection without any special programming on the part of the calling procedure. Graham's concentric model for access control is described along with the necessary hardware and software properties needed to implement his model. This model is the basis for access control in MIT's MULTICS system. However, much has been done since this article was written and several better access control concepts now exist.

*(3970)*69*ab*bc*cc*cd*dc*jf*mj*x1
Grant, C. B. "Will Students Wreck Your Computer Center?" DATA PROCESSING MAGAZINE, May 1969, pp. 62-63.

This article describes the destruction of the Sir George Williams University computer center by rioting students. Several reasons why computer centers need more protection are briefly discussed. The author then goes into a rather emotional discussion on why all rioters are the scum of the earth, and how we should revolutionize our school admissions policies to admit anyone who wants to attend.

*(3980)*68*ab*cc*db*de*ff*hk*hp
Greco, J. A. "Comments on the Structural Check of Input Data in a Computer System." JOURNAL OF ACCOUNTANCY, June 1968, pp. 46-52.

*(3990)*66*aa*cc*da*db*dc*hb
Greene, Richard M. Jr. BUSINESS INTELLIGENCE AND ESPIONAGE. Dow Jones-Irwin Inc., 1966.

*(4000)*71*ae*cb*cc*da*ha
Greenlee, Malcom B. "Privacy Considerations for Computer Systems." ADVANCED MANAGEMENT RESEARCH SEMINAR ON COMPUTER SECURITY, 1971.

*(4010)*69*ae*cc*da*fb*ka*mb*nj*nk*nl*nm
Greenier, E. J. Jr. "Computers and Privacy: A Proposal for Self-Regulation." PROCEEDINGS OF THE ACM, October 1969, pp. 231-269.

Some legal problems in assuring the privacy and security of computerized data are discussed. Recent trends in the law of privacy are analyzed, and a theoretical projection of possible future developments is made. The author concludes that the computer industry must start a program of self-regulation if it is to continue to operate in the public interest. He suggests that this program be modeled after the highly successful National Association of Securities Dealers.

*(4020)*68*ad*cb*dg
Grochow, J. M, "The Graphic Display as an Aid in the Monitoring of a Time-Shared Computer System." MAC-TR-54, MIT, Cambridge, Massachusetts 02139; or AD-689 468, National Technical Information Service, Springfield, Virginia 22151, October 1968, 82 pp.

This article is primarily concerned with explaining the use and advantages of a graphic display as a medium for dynamic observation of the processor state of a time-shared system. The problem of data security is only briefly discussed.

*(4030)*68*ab*cc*db*dd*de*fi*hr
Gruenberger, Fred. "Program Testing and Validating." DATAMATION, July 1968.

Some testing methods are described as well as some of the most frequently made testing mistakes.

*(4040)*71*ab*ba*cc*cd*da
"GSA Tightens Office Building Security." THE OFFICE, February 1971, p. 32.

*(4050)*71*ad*cb*cc*lb*md*nd
"GSA Time-Sharing RFP (Protection Requirements)." General Services Administration: Federal Supply Service, Washington, D.C., November 1971.

*(4060)*71*ab*bc*bd*be*cc*cd*dc*dd*de*jf*x1
"Guard that Computer." NATIONS BUSINESS, April 1971, pp. 84-86.

The purpose of this article is to convince the reader that more than superficial safeguards are necessary to provide adequate protection for the computer and its magnetically stored data. Several examples of computer and data destruction by sabotage or accident are briefly described. Building location, fire protection, air conditioning, access control, disaster plans, record backup, and good housekeeping are some of the main points that must be checked.

*(4070)*71*ad*ak*cb*cc*cd*dg*gg*nb*nf
"Guidelines for Protection and Control in a Computer Environment." Report No. ?, IBM Corporation, Data Processing Headquarters, Field Systems Center, Poughkeepsie, New York, 1971.

This is a very useful manual on the subject of how to develop and implement a comprehensive computer security program.

*(4080)*70*af*cc*dg*fb*nj*x2
"The Guilt-Edged Computers. Part 1: The Plight of the Insiders." ADP NEWSLETTER, The Diebold Group Inc., 430 Park Avenue, New York, New York, 29 April 1970.

This article is meant to be a warning to management about establishing adequate controls and safeguards for protecting their computer and essential, magnetically-stored, business data. Reports of data losses are increasing and so are cases of stockholder suits on the grounds of mismanagement. Executives can be personally liable for not establishing adequate internal controls, and CPA's can be liable for not verifying that adequate internal controls don't exist.

*(4090)*68*ab*cc*fc*ff
Guiltinan, R. J. "EDP and the Auditor." CPA JOURNAL, September 1968, pp. 639-641.

*(4100)*69*ab*cb*cc*dg*lb
Guise, Robert F. Jr.. "File Security." DATA SYSTEMS NEWS, November 1969, p. 30.

File security in a time-sharing environment is briefly discussed.

*(4110)*00*ad*cc*da*mb*nm
Guise, Robert F. Jr. "Security and Privacy." CTSS Position Paper, Com-Share Inc., Ann Arbor, Michigan.

The databank and privacy problem is discussed in quite general terms. The author suggests that the computer industry regulate itself.

*(4120)*69*ab*ah*dd*ht*hu
Habermann, A. N. "Prevention of System Deadlocks." COMMUNICATIONS OF THE ACM, June 1969, p. 373.

*(4130)*70*ab*cc*dc*fw
Hallinan, Arthur J. "Internal Audit of a Computer Disaster Plan." THE INTERNAL AUDITOR, November 1970.

*(4140)*71*ac*cc*da*fe*hd*ka*lb*mf*nm*x2
Halloran, Richard. "Inquiry on Surveillance Hears State Aide." NEW YORK TIMES, 11 March 1971, p. 26.

Robert Gallati, director of the New York State Identification and Intelligence System, stated before Congress that he believes personal information systems can be properly safeguarded to protect the privacy of individual citizens. Earlier testimony was in sharp contrast to this. The rest of this short article describes certain features of the New York system. It employs 800 people and can be accessed through any of 3,600 terminals located in various criminal justice agencies throughout New York. Privacy was protected by limiting users of the system, restricting the information programmed into the system, forbidding unauthorized disclosure, permitting individuals to see their own files, and only recording records of individuals considered likely to be criminal repeaters. Certain hardware and software safeguards were also developed.

*(4150)*70*ab*cc*da*ka*nl*nm*x1
Halsbury, The Earl of. "Lord Halsbury Speaks on Computer Privacy." COMPUTERS AND AUTOMATION, July 1970, pp. 42-43; or THE COMPUTER BULLETIN, February 1970.

The author warns that all existing computer security systems can be beaten. He urges that the individual be given the right to see any information stored on him and that the keeping of secret computerized files on individuals be made illegal.

*(4160)*68*ab*cb*cc*db*kd*ni
"Halting the Electronic Hijacker." MODERN OFFICE PROCEDURES, September 1968.

This article discusses computer fraud and gives a checklist of controls.

*(4170)*73*aa*bg*cc*cd*dg*fy*gf*gg*ha*ja*ni
Hamilton, Peter. COMPUTER SECURITY. Auerbach Publishers, 121 North Broad Street, Philadelphia, Pennsylvania 19107, 1973, 384 pp., $9.95.

This book emphasizes the protection of innocent people from computer abuse and misuse. It is divided into nine chapters with the following titles: Computers and Trends in Crime and Fire; The Vulnerability of

Computers; Relating Security Theory to Computer Vulnerability; Physical Security and Control of Access; Security of Computer Personnel; Surveillance of People and Property, Computer Security and Risk Management; Checklist for the Security of a Company and Its Computer Complex; and Subversion by Computer. Also discussed are a variety of power ploys involving both operations abuses and system destruction which could disrupt and render helpless a computer-dependent society.

*(4180)*72*ac*ai*cc*da*ka*nj*no
Hanlon, Joseph. "British Study Discounts Computer Privacy Threats." COMPUTERWORLD, 26 July 1972, p. 4.

The Younger Committee on Privacy found little hard evidence that the computer was a threat to individual privacy. A set of ten principles for handling personal information is given. Criticisms of the report are also included.

*(4190)*71*ac*ai*ba*cb*cc*da*ka*mg*x1
Hanlon, Joseph. "Diagnostic DP Impractical: M.D. Hits Privacy Safeguards." COMPUTERWORLD, 30 June 1971, p. 2.

Dr. Leonard Cronkhite, General Director of Children's Hospital Medical Center, stated in a wide-ranging interview on "computers in health care" that privacy safeguards for medical records are inadequate and computerization will make the problem worse. He states that a $20 bill will buy anything at Children's Hospital. Most hospitals provide little or no safeguards for personal data. Also, manufacturers have not made available any reasonable safeguards.

*(4200)*69*ac*ai*nm
Hanlon, Joseph. "Need Seen for Ombudsman to Regulate All Data Banks." COMPUTERWORLD, 13 August 1969.

Jerry Rosenberg's book THE DEATH OF PRIVACY is reviewed in this article.

*(4210)*71*ac*ai*ba*cc*da*fl*ft*ka*mf*nm*x2
Hanlon, Joseph. "Security Breach Leads to Police Data Theft." COMPUTERWORLD, 10 February 1971, p. 1.

Two policemen and several others have been charged with selling confidential information, including data from New York State's computerized criminal history file, to eight detective agencies and two airlines. The policemen did not tap the computer directly, but stole data from manual files which contained data taken legitimately from the computer. The companies paid $1 to $4 for each name check. One detective has been accused of making over $10,000 a year selling information. Much of the data in the computer is transferred to paper files in New York City, and security for these paper files is quite weak.

*(4220)*70*ac*ai*bc*dc*jf*mj*nj
Hanlon, Joseph. "Ten Students Convicted in 1969 Computer Center Burning." COMPUTERWORLD, 29 April 1970.

The events leading up to the computer disaster at Sir George Williams University are discussed. Certain aspects of the trial are also covered.

*(4230)*71*ae*ag*cb*cc*er*es*fd*he*ka*mb*ng*nm*x4
Hansen, Morris H. "Insuring Confidentiality of Individual Records in Data Storage and Retrieval for Statistical Purposes." AFIPS CONFERENCE PROCEEDINGS, Fall Joint Computer Conference, Vol. 39, 1971, pp. 579-585.

The goal of this paper is to summarize some aspects and principles of confidentiality, and some implications of these principles for computer-based storage systems. The remarks will have special relevance for open retrieval systems in which customers (the general public) can retrieve any desired statistics, subject to a review to insure that the output conforms to prescribed rules designed to avoid individual disclosure. Much of this paper draws on Census Bureau experience. This experience shows that serious unresolved problems exist, which are especially difficult for a system such as the proposed federal data center.

Some resolved and unresolved questions concerning rules for protecting confidentiality of individual records are briefly presented below. Should disclosure rules take into account information sensitivity? Some information changes sensitivity with time and some does not. Presumably it is not feasible to protect against disclosure by collusion. It is difficult but possible for a person with enough supplemental knowledge about an individual to identify additional information about him. Errors and differences in time reference increase statistical confidentiality. Indirect disclosures are a major source of difficulty, and they require that priorities be made in determining which statistics will be made available and which will not. This priority problem is alone sufficiently serious enough to foreclose development of a federal data center. Random modification of data to avoid approximate disclosure often reduces the usefulness of the data. Disclosure of statistical information from samples of a much larger database has proven highly successful in reducing the probabiltiy of individual disclosures while not reducing the data usefulness. The issue of disclosing disclosure rules is unresolved. There is no basis for assuming an all-powerful software system can preserve confidentiality in a national statistical data center.

*(4240)*70*ae*cc*da*me*nm
Hansen, Morris H. "Some Aspects of Confidentiality in Information Systems." EIGHTH ANNUAL CONFERENCE OF THE URBAN REGIONAL INFORMATION SYSTEMS ASSOCIATION, September 1970.

*(4250)*70*ab*ah*cb*cc*dg
Hansen, P. B. "The Nucleus of a Multiprogrammed System." COMMUNICATIONS OF THE ACM, April 1970, p. 238.

*(4260)*71*ab*cc*ff
Harris, R. D. "EDP Systems Audits." DATA MANAGEMENT, September 1971, pp. 64-71.

*(4270)*67*ad*aj*nm*np*x4
Harrison, Annette. "The Problem of Privacy in the Computer Age: An Annotated Bibliography." RM-5495-PR/RC, RAND Corporation, Santa Monica, California 90406, December 1967, 125 pp.

This is an excellent selected bibliography which has annotations on more than 300 articles pertaining to all aspects of the problem of privacy in the computer age. Most of the entries are from the years 1965-1967. The annotations are very well written and average about 100 words in length. Entries are categorized under sixteen subject headings entitled: Business and Industry View of Privacy; Cashless-Checkless Society and Privacy; Computer Utilities, Time Sharing, and Privacy; Congressional View of Privacy; Data Banks; Electronic Eavesdropping and Wiretapping; Federal Statistical Data Center; Government Agencies and Privacy; Legal and Law Enforcement View of Privacy; Mailing Lists and Privacy; Miscellaneous News Media Reporting on Privacy; Privacy Concern in Foreign Countries; Religious Concern and Privacy; Social Scientists' View of Privacy; System Security; and Technologists' Views of Privacy. The sixteen page introduction gives a very good overview of current (1967) problems in the field of computers and privacy. Only 24 of the 300 entries dealt with computer security issues. This bibliography is a must for anyone interested in the privacy-computer relationship.

*(4280)*69*ad*aj*nm*np*x4
Harrison, Annette. "The Problem of Privacy in the Computer Age: An Annotated Bibliography -Volume 2." RM-5495/1-PR/RC, RAND Corporation, Santa Monica, California 90406, December 1969, 148 pp.

This is the second part of an excellent selected bibloigraphy on the problem of privacy in the computer age. See the Volume 1 annotation for additional information. Most of the over 300 entries in this volume cover the period 1967-1969. There is no overlap of entries in these two volumes. The entries are again categorized under sixteen subject headings. An eight page introduction gives a very good overview of current (1969) privacy problems. Only 20 of the 300 entries in this volume dealt with computer security issues. Again, this bibliography is a must for those interested in how computers are affecting individual privacy. The author believes it is critically important that a balance be struck between an individual's right to privacy and society's right to know, before society's right is the only one recognized.

*(4290)*68*ab*cc*ff
Harrison, J. P. "An Auditor's View of Data Processing." DATA MANAGEMENT, September 1968, pp. 32-36.

*(4300)*68*ab*ah*cb*ec
Harrison, M. C. "Implementation of the SHARER 2 Time-Sharing System." COMMUNICATIONS OF THE ACM. December 1968, p. 845.

This article describes a mechanism which allows the execution of part of a program with its own memory protection. The SHARER time-sharing system which uses this feature is described.

*(4310)*69*ab*cc*dd*fi*hr
Harrison, William L. "Program Testing." DATA MANAGEMENT, December 1969.

The author recommends that an independent testing and evaluation group be formed for program testing purposes.

*(4320)*68*ac*ai*db*mf
"Has the Mafia Permeated the Computer Community?" COMPUTERWORLD, 28 August 1968, 11 September 1968.

Ways in which organized crime could benefit from using the computer are discussed.

*(4330)*72*ab*cb*cc*dg*ff*fi*fp*nf*ni*x2
Hawkins, David H. "How Safe is Your Software?" COMPUTER DECISIONS, June 1972, pp. 18-20.

This article was written for a reader with little knowledge of computers and/or software security. The author very briefly describes several common types and levels of access control such as: passwords, classifying users into security levels, read/write/execute control, maintaining security tables, and threat monitoring. Software security is no more safe than the operating system, which is of questionable secureness for almost all manufacturers. The author makes a few more suggestions and then presents the following checklist: are integrity checks made on system programmers and operations personnel; is access restricted according to the level of employee; are key words frequently changed; do procedures for monitoring security violations exist; is the operating system secure; are restart and recovery procedures used; are backup files kept; are changes well documented; are periodic security effectiveness checks made; and is cryptography used for data transmission?

*(4340)*72*ab*cb*dg*ff*fi*fp*nf*x2
Hawkins, David H. "Protecting EDP Systems from Fifth-Column Attacks." MANAGEMENT REVIEW, October 1972, pp. 51-53.

This article is a condensed version of another article by Hawkins entitled "How Safe is Your Software?" in COMPUTER DECISIONS.

*(4350)*68*aa*cd*nb*x3
Healy, Richard J. DESIGN FOR SECURITY. John Wiley and Sons Inc., New York, New York, 1968, 309 pp.

This book deals only with the physical aspects of security and no particular attention is given to computers. The material was designed to demonstrate how the use of proper planning and design, as well as the use of modern techniques and devices, can significantly reduce costs and, at the same time, improve the protection program. The book was intended to be of use to security administrators, architects, plant engineers, personnel managers, and anyone else concerned with the protection of a firm's facilities.

*(4360)*69*aa*bc*cc*cd*dc*fw*gd*jf*jg*nf*nn*x2
Healy, Richard J. EMERGENCY AND DISASTER PLANNING. John Wiley and Sons Inc., New York, New York, 1969, 290 pp.

All key aspects to be considered in a plan to cope with disaster are discussed. This book is complete as a general planning guide. It can also be used as a reference document because it contains a wealth of detail on many subjects. However, there are no explicit discussions on computer disasters. The author has a distinguished international reputation in the field of emergency planning and industrial security. The book is divided into twelve chapters with the following titles: General Disaster Considerations; Emergency Plan Factors - Peacetime Disasters; Emergency Plan Factors - Enemy Attack; Nuclear Attack Effects; Nuclear Accidents; Accidents Involving Hazardous Chemicals; Winds, Cyclones, Hurricanes, and Tornados; Earthquakes; Floods; Homemade Bombs - Bomb Hoaxes; Riots, Civil Disturbances, and Demonstrations; and Psychological Reaction on People.

*(4370)*73*aa*cc*da*db*dc*hb
Healy, Richard J. PROTECTING YOUR BUSINESS AGAINST ESPIONAGE. American Management Association Inc., 135 West

50th Street, New York, New York 10020, 1973, $9.00.

*(4380)*71*aa*bg*cc*cd*dg*el*en*fb*fi*fy*gg*hb*hd*jd*je *jf*jg*ka*lb*nf*nn*x2

Healy, Richard J.; and Walsh, Timothy J. INDUSTRIAL SECURITY MANAGEMENT. American Management Association Inc., 135 West 50th Street, New York, New York 10020, 1971, 274 pp., $15.75.

This book discusses the size, trend, and character of security loss risks. Explicit descriptions of the ways in which losses actually occur and specific countermeasure recommendations are given. The book is divided into twelve chapters with the following titles: The Security Gap, Organizing a Security Operation, Essentials of a Security Program, Prevention of Industrial Espionage, Riots and Civil Disturbances, Computer Security, Prevention of Thefts and Frauds, Guard Operations, Bombs and Bomb Hoaxes, The Systems Approach to Security, Screening and Investigation of Applicants, Effects of Changing and Social Environment on Security. The twenty page chapter on computer security discusses: fire, storage, industrial accident, natural disaster and contingency plans, system malfunction, electronic data theft, time-sharing system dangers, fraud and embezzlement, espionage, physical access control, operating procedure controls, program control, and insurance. However, this chapter on computer security is quite basic, and only the most common safeguards are presented.

*(4390)*72*ab*cc*fm

Heeschen, P. E. "Auditing Data Processing Administrative Activities." THE INTERNAL AUDITOR, November 1970, pp. 55-62.

*(4400)*70*ad*aj*cb*cc*da*gg*hd*ka*mg*nm

Hellman, John Jay. "Privacy and Information Systems: An Argument and an Implementation." Master's Thesis, Department of Electrical Engineering, MIT, Cambridge, Massachusetts 02139; or P-4298, RAND Corporation, Santa Monica, California 90406, 77 pp.; or AD-706 963, National Technical Information Service, Springfield, Virginia 22151, May 1970.

The first part of this paper examines the social and technical implications of information systems. The author believes that information systems must incorporate certain properties in their initial design in order to safeguard man's privacy while still providing society with the information it needs. For a secure system, the cost of violating the system safeguards must be considerably greater than the value of the information to the violator. The second part of this paper applies safeguards derived in Part 1 to problems in medical information systems. A drug information system, a toxicological information system, and a patient medical record system are each analyzed in relation to the individual's right of privacy and society's right to know.

*(4410)*69*ab*cc*cd*dg*x1
Hemphill, Charles F. Jr. "Preventing Damage to EDP Systems." ADMINISTRATIVE MANAGEMENT, April 1969, p. 14.

This article tries to convince the reader that more than superficial safeguards are necessary for adequate protection of computers and magnetically stored data. A few hazards and some basic suggestions (backup files, physical access control, separation of duties) are given.

*(4420)*71*aa*cd*da*dc*ga*gf*hb*jc*jf*jg
Hemphill, Charles F. Jr. SECURITY FOR BUSINESS AND INDUSTRY. Dow Jones, Irwin Inc., Homewood, Illinois, 1971.

Only one chapter of this book is devoted to computer security issues. However, the remainder of the book does have some good ideas on physical security.

*(4430)*70*ab*cc*da*db*ff
Henderson, Reid. "Internal Control Safeguards for EDP." DATA MANAGEMENT, September 1970.

*(4440)*71*ab*cb*cc*da*de*ka*nj*nk*nl*x2
Henderson, Robert P. "Computers and Privacy." ADVANCED MANAGEMENT JOURNAL, July 1971, pp. 8-12.

The author, associate group vice-president of Honeywell, shows that there is a large difference in the meanings of the words "privacy" and "security". The prime responsibility of computer manufacturers is to provide computer hardware and software safeguards that will enable the user to achieve the degree of security he needs or desires. The manufacturer can also help educate the user, but can't impose its technology or ethics on the user. The author describes what is available today and what will be available in the near future in the area of security hardware devices and operating systems for computers. In describing these available security techniques, he presents in very general terms several concepts used in MIT's MULTICS system.

In turning to privacy considerations, the author believes that laws should be developed which give every individual the right: to examine his own file and challenge its contents; to know to whom and under what circumstances this data can be released; and in some cases to control the dissemination of his personal data. Strict controls on the technology of databanks are not wise because the technology is changing very rapidly and controls would soon be obsolete and hinder developments. The author recommends that users conduct periodic audits of their personal data files to erase obsolete and irrelevant information. This article is very similar but not identical to another article by Henderson entitled "Controlling the Computer Threat to Privacy".

*(4450)*71*ab*cc*da*de*fs*ka*nj*nk*nl*x2
Henderson, Robert P. "Controlling the Computer's Threat to Privacy." MICHIGAN BUSINESS REVIEW, November 1971, pp. 9-14.

The author associate group vice-president of Honeywell, shows that there is a great deal of difference between the words "privacy" and "security" as they relate to computers. The prime responsibility of computer manufacturers is to provide computer hardware and software safeguards that will enable the user to achieve the degree of security he needs or desires. Computer room physical security, remote terminal access controls, database access control, and audit-monitors are very briefly discussed in simple language. Maintaining the privacy of personal databanks is the responsibility of the computer user. The user's responsibility is to use adequate manufacturer provided hardware and software safeguards, as well as adequate procedural and physical safeguards. The staff of a computer center is almost always the weakest link in a total security system. The author believes that government certification of computer operators, systems designers, and computer systems is desirable.

Since there is currently almost no legal protection against privacy invasion, the author suggests that federal laws be passed to give all individuals the right: to be informed of all files kept on them; to read their file and challenge its contents (by legal means if necessary); and to know who supplied any bit of information on them. This article is similar but not identical to another article by Henderson entitled "Computers and Privacy".

*(4460)*69*ab*cc*cd*da*db*dc
"Highlights of a Security Plan Devised by Experts." OCCUPATIONAL HAZARDS, March 1969.

*(4470)*63*ab*cc*cd*da*fl*jc
Hiles, Richard A. "Paper Shredders." MODERN OFFICE PROCEDURES, February 1963.

*(4480)*68*ab*cc*da*db*ff*kd
Hill, O. A. Jr. "The Role of the Auditor With Respect to Internal Control and Fraud." THE INTERNAL AUDITOR, May 1968.

*(4490)*71*ad*cb*dc*dd*gc*jg
Hill R. D. "Note on Vulnerablility of Computers to Lightning." General Research Corporation, 5383 Hollister Avenue, Santa Barbara, California 93105, April 1971, 18 pp.

*(4500)*69*ab*cc*dc*fy
Hines, Harold H. Jr. Letter to the Editor. HARVARD BUSINESS REVIEW, May 1969.

Insurance protection available for computers is discussed.

*(4510)*71*ad*cb*ed*ef*gh
Hirsch, J. "Access Control and Retrieval Optimization Functions of the Supervisor for an Extended Data Management Facility (EDMF)." Report 71-21, Moore School of Electrical Engineering, University of Pennsylvania, Philadelphia, Pennsylvania, April 1971.

Access control information is associated with each user, in the form of authority items, instead of being stored with each file. This enables the access control information to be stored together in a system file instead of being scattered throughout user files. Centralized storage of access control information makes updating much easier and probably provides for better security. Data in the EDMF can be protected below the file level. A "service status block" and a "file status block" are used to reduce unnecessary access control information. Manola's Master's thesis includes a more current discussion of access control techniques for the Extended Data Management Facility.

*(4520)872*ab*cc*da*db*hd*ka*ng*nl*nm*x3
Hirsch, Phil. "Computer Systems and the Issue of Privacy: How Far Away is 1984?" DATAMATION, December 1972, pp. 90-93.

This article first discusses a report entitled "Communications for Social Needs". Although the report was reluctantly rejected by President Nixon, projects described in the report are still under consideration. The report proposed federal support for several new applications of communications and computer technology. One system would enable the Feds to turn on every radio and TV in the country, supposedly to warn people of impending disasters. Another system is for electronic transmission of mail between cities. The report said that all handling of the mail will be mechanized so letters will not be read. However, it didn't say that only a very simple computer program could detect and print all mail to and from any individual. Recently, control of the National Criminal History System was removed from the states and given to the FBI. Such a highly centralized system is now considerably more vulnerable to "executive manipulation" (i.e. Watergate).

The use of social security numbers as universal individual identifiers is also discussed. Many organizations have started using social security numbers as identifiers anticipating that they will become universal. Many feel this trend may have gone too far to stop. The problem of a universal identifier is that it enables computer files to be merged (legally or illegally) with considerably less effort.

A three year privacy study, directed by Dr Alan F. Westin, has just been completed. It concludes that central databank developments are not as advanced as many people believe. However, privacy laws must be developed in the mid 1970's. Another study suggests there will be nothing left to save if laws are not developed until the mid 1970's.

*(4530)*70*ab*cb*cc*da*fe*fh*gh*ka*md*nl*nm*x2

Hirsch, Phil. "The World's Biggest Data Bank." DATAMATION, May 1970, pp. 66-73.

This article traces the history of the U.S. Census Bureau. The 1970 census is the first one that will be able to separate statistics into very small areas such as city blocks. Therefore, the issue of individual privacy deserves important consideration. The article discusses steps taken to safeguard this information. The bureau's physical and software security safeguards are shown to be quite inadequate. Nevertheless, the bureau is probably physically secure due to its rather complex and awkward operation. A few typical examples of census data being legitimately used to the detriment of those who supplied the data are discussed at length. The author feels that the most effective method of halting undesirable use of census statistics is to establish an independent federal commission with the power to review all data tabulated from census statistics.

*(4540)*71*ab*cb*cc*cd*dg*nb*x2

Hirschfield, Richard A. "Security in On-Line Systems - A Primer for Management." COMPUTERS AND MANAGEMENT, Septmeber 1971, pp. 15-17.

The purpose of this article is to point out some problems in securing on-line systems and some potential avenues of solution. The article is written for readers who have little knowledge of computers and/or security techniques. It is divided into four sections concerned with: access control (physical security, passwords, file access); data transfer control (computer logs of all accesses, closed-loop verification of data transmission, data encrypting); backup and recovery of files and programs; and systems auditability (publishing security procedures, testing the security system, auditor involvement in system design). Nothing really new or unusual is presented.

*(4550)*71*ac*ai*cb*cc*da*db*ff*lb*x1
Hirschfield, Richard A. "True Jeopardy 'Inside', Auditor Says." COMPUTERWORLD, 30 June 1971, p. S1.

The greatest exposure in on-line systems is unauthorized access through remote terminals. Computer logs, encrypting of data, closed-loop verification to ensure error free transmission, and sufficient audit controls and checks are recommended.

*(4560)*69*ab*ca*ee*ef*el*lb*ng*nl*nm*nn*x3
Hoffman, Lance J. "Computers and Privacy: A Survey." COMPUTING SURVEYS, June 1969, pp. 85-103.

This classic article is a good survey of what has been done in the area of computer system access control. The article is divided into four sections entitled: the privacy problem; legal and administrative safeguards; technical methods proposed to date; and promising research problems. The bulk of this article is concerned with technical methods proposed to date.

The author believes that the most serious technical problem, yet to be solved, is to find an economical method of providing access control below the file level. Hsiao's method is the first to do this, but the author doubts the method is economical. Several other methods of providing access control to users of shared data are briefly described, and the limitations of each method are stated. Also briefly discussed are: methods to identify remote users; privacy transformations (cryptography); threat monitoring; and processing restrictions.

An annotated bibliography of 69 articles is included. Most of the articles are annotated quite well in one or more paragraphs. However, only 15 of the 69 articles deal with computer security issues, and these 15 can easily be found in other references. The other 54 articles are concerned solely with privacy issues.

*(4570)*70*ad*ca*da*db*dc*ee*ef*nc*x2
Hoffman, Lance J. "The Formulary Model for Access Control and Privacy in Computer Systems." Ph.D. Dissertation, Report No. 117, Stanford Linear Accelerator Center, Stanford, California; or AD-(?), National Technical Information Service, Springfield, Virginia 22151, May 1970, 88 pp.

The author believes that data access control can be performed more easily with real-time, access-control computer programs written by the file owner than by look-up tables or access-control bits stored with each word. In his formulary model, data access is controlled by a set of procedures called formularies. The model enables a file owner to control access to any level, including the bit level. However, Hoffman's model excludes the use of any tables and requires the user to describe all his field, record, and file structures in procedures. Other authors feel that the effort needed to do this may be quite substantial, and implementation of the model could be very costly.

*(4580)*71*ae*ag*ca*da*db*dc*ee*ef*nc*x2
Hoffman, Lance J. "The Formulary Model for Flexible Privacy and Access Control." AFIPS CONFERENCE PROCEEDINGS, Fall Joint Computer Conference, Vol. 39, pp. 587-601.

This article is a condensed version of Hoffman's Ph.D. dissertation entitled "The Formulary Model for Access Control and Privacy in Computer Systems".

*(4590)*70*ab*cb*da*es*he*x3
Hoffman, Lance J.;and Miller, W. F. "Getting a Personal Dossier from a Statistical Data Bank." DATAMATION, May 1970, pp. 74-75.

A "statistical" databank is defined as one which returns only summary tables on a group of persons which have a given set of requested characteristics. Suppose one wants to know whether Joe Doe earns over $50,000 per year, and it is known personal information on him is in a statistical databank. It is also known that he is 50 years old, has a Ph.D. degree, and lives in Boston. Suppose the computer states that there are 45 people in the databank that are 50 years old, with Ph.D. degrees, and living in Boston. Now ask - how many of these 45 people earn over $50,000. If the computer returns the answer "45", the desired information on Joe is obtained.

The author presents a simple algorithm which, with enough work and sufficient information, can be used to identify individuals in a statistical databank. They recommend the use of threat monitoring to limit such abuses though realizing that it is not an extremely effective safeguard.

*(4600)*72*ab*cc*cd*dg*ff*nb*x2
Holland, Geoffrey. "Computer Security." ACCOUNTANCY (England), March 1972, pp. 43-45.

This article attempts to draw attention to the serious risks of deliberate and accidental security violations. Some of the more interesting statements are briefly summarized below. The resources of a computer center can be divided into the following categories: plant (physical hardware, building); consumable supplies (cards, paper); data; software; and people. In addition, security can be looked at from the following viewpoints: prevention, detection, recovery, rectification, and compensation. In developing a good security program one must first establish the potential losses in financial terms and examine the exposure to risks. The user, the systems and programming development staff, and the operations staff all must play an active role in the security program. Periodic security system testing is vital because the computer environment is constantly changing and because people soon become lax in their security related behavior.

*(4610)*70*ae*cc*dg*ff*fv*hc*kb
Homes, F. W. "Software Security." 6373-60, American Management Association Briefing Session, 15 April 1970.

Software security, proprietary programs, program documentation, checkpoint recovery procedures, and audit trails are all discussed.

*(4620)*69*ae*cb*cc*da*hd*ka*mb*mg
Holmes, W. S. "Privacy Techniques for Computerized Medical Data Systems." USE OF COMPUTERS IN CLINICAL MEDICINE SYMPOSIUM, School of Medicine, State University of New York, Buffalo, New York, 2 October 1969.

Some security and privacy problems unique to the medical environment are discussed, and a few general computer safeguard techniques are presented.

*(4630)*70*ab*cc*da*ka*nl*nm
Horton, Frank. "Privacy Safeguards Urged." EDP WEEKLY, 21 September 1970, p. 3.

The author, a New York Congressman, feels that the growth of large databanks presents a threat to individual privacy. He urges legislation to prevent abuses by databank owners.

*(4640)*71*ad*cb*dg*eb*ee*ef*eh*ha
Horton, M. "Reading, Writing, Creating, and Updating Records and Files in a Generalized File Structure." Master's Thesis, Moore School of Electrical Engineering, University of Pennsylvania, Philadelphia, Pennsylvania, 1971.

*(4650)*70*ab*cc*ff
Horwitz, G. B. "EDP Auditing - The Coming of Age." JOURNAL OF ACCOUNTANCY, August 1970, pp. 48-56.

*(4660)*70*ab*bb*cc*db*fq*hk*hl*md*x1
"How Bad Guys Thwart Computers." THE OFFICE, September 1970, p. 32.

This article discusses several threats by dishonest employees and saboteurs. Most of the discussion focuses on the federal government. The government's biggest computer problems have occurred in the Internal Revenue

Service. Tax officials have discovered a minor flurry of fraud among their employees. So far all the discovered frauds have been committed by operators and clerks, not programmers or analysts. The IRS now uses different personnel for each of the following steps: systems analysis, program preparation, original run testing, and operating the computer.

*(4670)*65*ab*ba*da*hb
"How I Steal Company Secrets." BUSINESS MANAGEMENT, October 1965.

Methods supposedly used by an industrial spy are the subject of this article.

*(4680)*68*ab*cc*da*hb
"How Safe are Your Business Secrets?" BUSINESS MANAGEMENT, March 1968.

Several precautions are presented for protecting business secrets.

*(4690)*71*ab*bc*cd*dc*gf*jf*mj*x1
"How Security Does Pay Off." THE OFFICE, September 1971, p. 22.

Sometimes minimal security measures can prevent maximum losses. This is what happened at the University of Kansas. The University decided to limit access to its computer room by locking doors after certain hours and restricting traffic in an adjacent hallway by locking the door at one end. One night a bomb exploded and blew an eight foot hole in one wall of the computer room. The saboteur was apparently unable to obtain access to the computer room. Three operators were slightly injured because they thought the saboteur's anonymous phone call was a hoax.

*(4700)*67*ad*cc*cd*da*hb
"How to Avoid Electronic Eavesdropping and Privacy Invasion." Investigator's Information Service, 806 South Robertson Boulevard, Los Angeles, California, 1967.

*(4710)*70*ab*cc*cd*da*hb
"How to Make Sure Nobody Knows Your Business." MODERN OFFICE PROCEDURES, July 1970.

A survey on paper shredders is presented.

*(4720)*68*ab*cc*da*db*ff*hj
"How to Protect Against the Million Dollar Racket." MODERN OFFICE PROCEDURES, March 1968.

A list of danger signals and safeguards, intended to help detect and prevent embezzlement, is the subject of this article.

*(4730)*72*ab*cb*cc*cd*da*db*dc*ff*ge*gf*jc*jg
"How to Protect Your Computer from Theft, Fraud, Fire." CHAIN STORE AGE: Executive Edition, August 1972, pp. 17-19.

*(4740)*71*af*cb*cc*cd*dg*fb*nb*nf*ni*x3
"How Vulnerable is the Computer System?" ADP NEWSLETTER, The Diebold Group Inc., 430 Park Avenue, New York, New York, 8 March 1971.

Guarding against program errors, machine malfunctions, and lack of clear cut audit trails is just as important as guarding against theft, fraud, and riots. Six steps are described which management must take to properly address the computer security problem. Management must: (1) be convinced that there is a problem; (2) organize personnel to handle the problem, fix responsibilities, provide authority, and back up actions taken on behalf of security; (3) acquaint itself with the security procedures that have been planned by auditors and computer professionals to be competent to ask them the "right" questions; (4) make the policy decisions and assure that safeguard expenses are not out of line with the risks involved; (5) get agreement on the time table and costs of implementation, and establish checkpoints and performance yardsticks; and (6) decide on the insurance necessary to cover the remaining risks. This article also contains a checklist of questions that need to be asked and answered for each of several types of security risks.

*(4750)*65*ab*cc*da*hb
"How Your Company Can Thwart a Spy." BUSINESS MANAGEMENT, October 1965.

Methods of defense against professional industrial spies are discussed.

*(4760)*71*ab*cc*cd*dg*fg*ni*x2
Howes, Paul R. "EDP Security: Is Your Guard Up?" MANAGEMENT REVIEW, July 1971, pp. 29-32.

This article is divided into the following three sections: physical security, file and program security, and internal control systems. For each section, the author briefly presents some examples and arguments to show that security safeguards are essential. He presents a checklist for each section which includes specific safeguards that should, in most circumstances, be implemented. The checklists are fairly complete, but they don't include anything uncommon.

*(4770)*69*ae*cb*da*ea*ed*ef*ei*el*gh*ng
Hsiao, David K. "Access Control in an On-Line File System." FILE ORGANIZATION: SELECTED PAPERS FROM FILE 68 - AN

I.A.G. CONFERENCE, 1969, pp. 246-257.

The access control system of a Problem Solving Facility (PSF) designed by the University of Pennsylvania's Moore School of Electrical Engineering is described. Some of the system's capabilities are: records of files can be protected by specifying a logical expression of index words and file names; file users can be authenticated by providing inputs to an access control program written by the file owner; control is available for simultaneous multiple user access to shared files; and capabilities in using a file can be stored with the user rather than the file. The access control system is protected by storing it with the operating system. Two other articles by M. Gelblat and K. Nakaniski discuss the use of this system for medical applications.

*(4780)*68*ad*cb*da*ea*ee*ef*el*gh*ha*ng

Hsiao, David K. "A File System for a Problem Solving Facility." Ph.D. Dissertation, Moore School of Electrical Engineering, University of Pennsylvania, Philadelphia, Pennsylvania, 1968, 175 pp.; or AD-671 826, National Technical Information Service, Springfield, Virginia 22151.

This paper discusses in detail the file access control system of the Problem Solving Facility (PSF) designed by the Moore School. This was the first working system to provide access control below the file level. The design objectives of the system were: to have the capability to grow in terms of data, programs, and file management functions; to protect the privacy of a user's files; and to enable a file owner to gradually share his information with others. The result was a system which uses "authority items". These "authority items": provide access control below the file level; allow storage of access control information with the user not the files; enable the file owner to write his own access control program for authenticating users of his file; and keep data records from having to be reprocessed when a user's or file's access status changes.

Two later papers by Hsiao entitled "Access Control in an On-Line File System" and "A Formal System for Information Retrieval from Files" give a considerably less detailed description of the same system.

*(4790)*71*ab*cb*eb*ee*x2

Hsiao, David K. "A Generalized Record Organization." IEEE TRANSACTIONS, December 1971, pp. 1490-1495.

A generalized record organization is proposed from which many fixed and variable length records of hierarchical and network formats can be derived. In developing the generalization, attempts are made to characterize the record organization. By identifying the characteristics of the record organization, it is possible to segregate, for storage, the global record structural information from the local and nonstructural information. Such a segregation can lead to more efficient use of storage, ease of reorganizing the records, and the possibility of multiple organizations for the same set of records. A scheme for specifying the generalized record organization is illustrated. The implication for data security is that access control information can be separated from the data. Therefore, it is possible to determine the validity of a request without bringing the data requested into main memory.

*(4800)*70*ab*ah*cb*da*ea*ee*ef*el*gh*ng
Hsiao, David K.; and Haravy, F. "A Formal System for Information Retrieval from Files." COMMUNICATIONS OF THE ACM, February 1970, pp. 67-73; (also correction to this article), ibid., April 1970, p. 266.

*(4810)*70*ac*ai*bb*cb*cc*db*ft*hj*hm*kd*me
Huggins, Phyllis. "Computer Plays Big Role in Defrauding Welfare Unit." COMPUTERWORLD, 7 October 1970.

Los Angeles County was defrauded of $50,000 in a welfare check scheme that involved the Data Processing Department of Public Services. Three employees and eight others were indicted. The control system was unfortunately designed on the assumption that EDP personnel are honest.

*(4820)*71*ac*ai*bc*cd*dc*ga*jg*na*x2
Huggins, Phyllis. "Computers Show Resiliency After Earthquake." COMPUTERWORLD, 17 February 1971, p. 1.

EDP centers withstood the 1971 Los Angeles-San Fernando Valley earthquake with remarkably little permanent damage. About half the EDP centers in the area were back in operation by noon (the earthquake occurred in the early morning), and almost all were in operation by the next morning. This article very briefly describes what happened at seventeen computer centers located in the L.A. area. In one center the operator, for security reasons, could only be let out by a guard. When the quake struck, the frightened guard ran, leaving the operator trapped. Luckily, the operator wasn't injured.

*(4830)*71*ac*ai*ba*cb*cc*da*hc*ii*kc*lb*ma*x1
Huggins, Phyllis. "Employee Charged in Program 'Theft'." COMPUTERWORLD, 10 March 1971, p. 1.

Police armed with a search warrant raided a University Computing Company service bureau in Palo Alto, forcing the company to duplicate all its tapes and punched cards, and to dump disk packs and core. A UCC employee was then charged with grand theft. He was said to have illegally tapped an Information Systems Design computer and stole a proprietary program valued at $15,000 to $25,000. IDS first suspected the alleged theft when unrelated punched cards appeared in the output of one of its jobs. A search of telephone company charges revealed that a call to IDS's computer had come from UCC. The data lines between the two companies were tapped, and this led police to the suspect.

*(4840)*70*ac*ai*bc*cd*dc*jf*mj
Huggins, Phyllis. "Programmer Thankful for 'Bug' During Computer Center Bombing." COMPUTERWORLD, 27 May 1970, p. 1.

Protesting students threw three molotov cocktails through a plate-glass window at Fresno State College and destroyed its CDC 3150. Damages were near $1 million. The operator had just left the room to consult a programmer about a program "bug". Luckily, no injuries resulted.

*(4850)*70*ac*ai*cd*dc*ga*gf*jf*mj
Huggins, Phyllis. "Rebuilt Fresno State DP Center Follows Tight Security." COMPUTERWORLD, 8 July 1970.

The article discusses new security measures taken by Fresno State College after their computer center was totally destroyed by students using molotov cocktails.

*(4860)*00*ad*be*cb*cc*de*fi*hp*hr
"Human Error." AD-689 365, National Technical Information Service, Springfield, Virginia 22151, 246 pp.

This is a very comprehensive treatment on the subject of detecting and correcting data input errors.

*(4870)*72*ab*cc*fm
Hurtado, C. D. "A System to Measure EDP." JOURNAL OF SYSTEMS MANAGEMENT, January 1972, pp. 32-35.

*(4880)*72*ab*cb*dg*ng*nk*no*x2
"IBM Launches Program to Protect Access to Sensitive Data." MANAGEMENT ADVISOR, July 1972, pp. 6-7.

IBM has embarked on a five year, $40 million program to give the computer user the means to control sensitive data in his system. The envisioned system will allow the user to specify the amount of security protection implemented. It will also likely contain advanced forms of authorization and audit trails. The program is attempting to answer these questions: what is a fair measure of system secureness, what facilities should be taken into account, what differences does the environment make, how can levels of authorization be handled, what constraints will data security place on users, what will security cost in terms of performance and dollars?

*(4890)*72*ac*ai*cb*da*de*hd*ka*ng*nk*nm*no*x1
"IBM Plans $40 Million Study to Develop 'Secure' DP." COMPUTERWORLD, 24 May 1972, pp. 1-2.

This article quotes T. Vincent Learson, IBM chairman, in his keynote address to the recent Spring Joint Computer Conference. The goal of IBM's five year, $40 million research program is to give the customer the means to control access to sensitive data in his system. Learson also said that public policy must dictate how much and what kinds of information shall be collected, who shall have access to it, and for what reasons. He feels that this data security project will have direct effects on privacy legislation.

*(4900)*71*ac*bc*cc*dc*fw*jg*nk
"IBM Puts Volkswagen Back on the Road Three Days After a Total-Loss Fire." WALL STREET JOURNAL, 21 April 1971, (Advertisement).

*(4910)*68*ad*ak*cb*dg*ec*ed*ei*ej*gh
"IBM System/360 Operating System Concepts and Facilities." GC28-6535, IBM Corporation, White Plains, New York, November 1968.

This manual describes the protection architecture present in IBM's 360 series.

*(4920)*68*ad*ak*cb*dg*ec*ed*ei*ej*gh
"IBM System/360 Principles of Operation." GA22-6821, IBM Corporation, White Plains, New York, September 1968.

This manual describes the data access protection present in IBM's 360 series.

*(4930)*70*ad*ak*cb*dg*ec*ed*ei*ej*gh
"IBM System/370 Principles of Operation." GA22-7000, IBM Corporation, White Plains, New York, June 1970.

This manual describes data access protection present

in IBM's 370 series.

*(4940)*72*ac*cb*da*ka*ng*nk*nm*no*x1
"IBM to Seek Ways to Teach Computers How to Keep Secrets." WALL STREET JOURNAL, 17 May 1972, p. 9.

IBM plans to spend $40 million over the next five years to study techniques for assuring the confidentiality of data stored in computers. This short article presents a few statements made by T. Vincent Learson, IBM chairman, before the Spring Joint Computer Conference. Learson acknowledged that, "Public policy must decide who is to have access to what information. But the question of how to limit information access only to those who are authorized to have it, begins with the manufacturer of systems."

*(4950)*71*ab*cd*da*db*dc*gf*gh*x2
"Identi-Logic Spreads Security Blanket." DATAMATION, 1 May 1971, p. 66.

This article describes the Identi-Lock 1001 magnetic card reader and lock system used for physical access control. The system produces a hard record of the key number, date and time of entrance and exit, and area entered and exited. A pushbutton device can be substituted for magnetic cards. A special magnetic card that must be destroyed to be duplicated is also available. Identi-Logic, a division of Eaton, Yale and Towne Inc., produces the system. Identi-logic will also determine "who should be where and when" for its customers.

*(4960)*70*ab*cc*da*fh*he*ka*nm
"Identity Code for Individuals." THE OFFICE, June 1970.

This article discusses the use of social security numbers as universal identifying codes for EDP processing.

*(4970) 73*ab*np*pb*x1
IEEE TRANSACTION ON COMPUTERS. Institute of Electrical and Electronic Engineers Inc., 345 East 47th Street, New York, New York 10017, 1968-, (Monthly, with annual cumulative index).

Every issue contains roughly a ten page section entitled "Abstracts of Current Computer Literature". A description-in-context index with 'privacy' and 'security' as descriptors provides easy access to desired articles. A cumulative index is usually published every year. The abstracts average about 150 words in length, are well written, and quite informative. However, only about 25 articles on computer security were abstracted in the years 1967-1972, and all of them could be easily found in other references.

*(4980)*71*ac*bg*cc*cd*dg*nd*x2
Immel, Richard A. "Whir, Click-Blooey! Sabotage, Accidents, and Fraud Woes for Computer Center." WALL STREET JOURNAL, 22 March 1971, p. 1.

Several recent cases of computer sabotage, errors, and fraud are described. The article presents the views of several computer security experts who all agree that computer security is dangerously lax in a large majority of all computer installations. Some of these experts blame part of the computer's vulnerability on manufacturers who have failed to build security into their systems. Louis Scoma of Data Processing Security will put a team of consultants to work running through a 172 point checklist and preparing a survey report for $3,000 to $5,000. Purchasing security equipment is the expensive part. A double-door "buffer" system with electronic locks, magnetic sensors, and closed circuit TV can easily cost $25,000. Backup power systems cost from $50,000 for a simple generator to over $1,000,000 for a very elaborate system.

*(4990)*64*ab*cc*dc*fy*gc
"Importance and Complexities of EDP Units and Media Cause Many Insurance Problems." THE NATIONAL UNDERWRITER, 17 July 1964.

*(5000)*68*ad*cb*dg*ep*nk
"In the Matter of Regulatory and Policy Problems Presented by the Interdependence of Computers and Communication Services and Facilities." Docket No. 16979, Responses to the Federal Communications Commission, 5 March 1968.

This docket gives IBM's and BEMA's (Business Equipment Manufacturers Association) views on protecting private data stored in computers and transmitted over common communications lines. The section of the docket entitled "Security of Data Stored in Computers and Transmitted Over Communications Facilities" discusses both present and future techniques of security control, and legal and policy considerations. Two attachments to this response are "Major Economic Issues in Data Processing/Data Communication Services" by Horace J. De Padwin Associates and "Study of the Interdependence of Computers and Communications Services" by Booz, Allen, and Hamilton.

*(5010)*69*ab*bb*cc*db*fi*hj*hl*hm*kd*me
"Individual Responsibility." DATA SYSTEMS NEWS, February 1969, p. 4.

Computer programs at New York City's Human Resources Administration were altered to illegally make out over 40,000 paychecks. The result was one of the largest computer-related frauds discovered so far. The loss was near $2,700,000.

*(5020)*66*ad*cc*da*fe*fl*kb
"Industrial Security Manual for Safeguarding Classified Information." DOD 5220.22-M, U.S. Government Printing Office, Washington, D.C., 1 July 1966.
This manual describes security procedures to be taken by all organizations having Department of Defense classified information. Nothing is explicitly said about computers.

*(5030)*72*ab*cd*dc*dd*gc*gd*gf*mi*x1
"Inside Eastern's Data Center." BUSINESS WEEK, 5 February 1972, pp. 60-61.
This article describes physical security safeguards taken by Eastern Airline's new data center. The center, which will open in late 1972, is located in a new $8 million building near Miami airport. Computer hardware worth $22.8 million is kept in the building. Eastern's present computer center, located at Miami Airport, is nearing its saturation point in handling 2 million inquiries daily. Physical security measures include: acres of open land around the building; an eight foot chain-link fence; gates with electronic locks; metal detectors at entrances; twenty-four hour guard protection backup and, in some cases, double backup of all electronic motors, fans, switches, and power sources; and power from two external generating stations. The outside power drives local generators to avoid power spike and frequency change problems.

*(5040)*71*ab*cc*dc*fy
"Insurers Shy Away from EDP Coverage, Newsletter Says." MANAGEMENT ADVISOR, July 1971, p. 6.

*(5050)*70*ab*cc*dc*fy*kf
"Insuring List is a Must for Mail Users." DIRECT MARKETING, May 1970, p. 32.

*(5060)*67*aa*cc*dg*ff*kd
INTERNAL AUDITING OF ELECTRONIC DATA PROCESSING SYSTEMS. Institute of Internal Auditors, 1967.

*(5070)*65*aa*cc*da*db*ff*hj*kd
INTERNAL CONTROL IN ELECTRONIC ACCOUNTING SYSTEMS. Haskins and Sells Inc., 1965.

*(5080)*00*af*cd*ed*ii
"Introduction to CODE." Sales Brochure, Economatics, 275 South Los Robles Avenue, Pasadena, California 91106.
A software program is described that mixes false data with a user's input or output if he does not provide

a correct user identification code.

*(5090)*72*ac*ai*ba*cc*da*f1*hc*ii*kb*ma*nj*x1
"ISD Awarded $300,500 in UCC Trade Secret Suit." COMPUTERWORLD, 13 September 1972, p. 1.
Information Systems Design has been awarded damages amounting to $300,500 in its civil suit against University Computing Center and two of its employees. The suit alleged that two UCC employees had illegally accessed ISD's computer and stole valuable computer programs.

*(5100)*69*ac*cd*ga*ge
Jackson, W. A. "Fire Protection Systems." DATA PROCESSING, March 1969.

A 10 point fire protection guide is presented.

*(5110)*72*ab*cc*ff
Jacobsen, G. G. "Auditing Aspects of Data Processing." DATA MANAGEMENT, July 1972, pp. 17-19.

*(5120)*73*ac*ai*cc*dg*fb*nf*x2
Jacobson, Robert V. "Big-Time Security Analysis Needed." COMPUTERWORLD, 27 June 1973, p. 19.

The small business that has just installed a minicomputer is exposed to many of the security problems of a large business and has special problems that large businesses don't have. Separation of duties, reduced dependence on the knowhow of specific individuals, and ample personnel for assignment to emergency duties are all more difficult to obtain in a small business with only four or five EDP personnel. The author recommends use of risk analysis where: the potential dollar expense is estimated for loss of each computer application; the probability of occurrence is estimated for each thing that could go wrong; and the above two estimates are combined to determine the most significant threats. Although risk analysis is not easy to do, it pinpoints what needs protection, and it helps the manager decide what is a reasonable amount to spend. The small business manager must keep himself involved in the EDP area. He should also remember that most frauds are discovered through a foolish blunder by the embezzler.

*(5130)*71*ae*cb*cc*cd*nb
Jacobson, Robert V. "Cost Effectiveness of Security Measures." ABA NATIONAL AUTOMATION CONFERENCE, May 1971.

*(5140)*69*ae*cd*dc*fv*fw*ga*gf*nf
Jacobson, Robert V. "Planning for Back-Up Facilities." COMPUTER SERVICES, A.Z. Publishing Company, May 1970, pp. 22-29; or American Management Association on Security and Catastrophe Prevention Management of the Computer Complex, November 1969.

Access control, site selection, and disaster prevention are discussed. Four types of system failures are described and recommended safeguards are given for each. The author believes that selective backup may, in many cases, be more practical than full backup when all facts are analyzed.

*(5150)*70*ab*be*cc*cd*df*dg*fg*fv*fx*gf*hq*x2
Jacobson, Robert V. "Providing Data Security." AUTOMATION, June 1970, pp. 85-90.

The author discusses each of the following safeguards in some detail: timely and reliable operation, backup files, making programs fail-safe, internal data-control group, physical access controls, and periodic testing of the security system. For each of the above safeguards, numerous reasons are given to show that implementation of the safeguard is highly desirable. A protection matrix is also presented. The rows of the matrix represent the computer system elements of hardware, software, personnel, procedures, and facilities. The columns represent the following hazards: loss (destruction of hardware or data), defects (errors and fraud), and illegal disclosure. Each element of the matrix contains specific protective measures for the pertinent computer system element and hazard.

*(5160)*70*ab*bb*cc*dg*ff*fg*fi*hj*if*kb*kd*x3
Jacobson, Robert V. "Providing Security Protection for Computer Files." BESTS REVIEW: Life/Health Insurance Edition, May 1970, pp. 42-44; or Property Edition, June 1970, pp. 44-46.

There are really only three ways in which a process can go wrong: errors in the input data, errors in the programs, or changes in the data files. Only two basic kinds of files exist: those mainstream to the processing; and those used for control, audit, and protective purposes. Files are subject to the following hazards: accidental erasure; loss by fire, sabotage, etc.; data input errors; defective or altered programs; and deliberately introduced errors. After briefly making the above statements, the author discusses in some detail; file backup; internal control groups; and program validation and revalidation procedures. He believes that there should be flow diagrams which show: relationships between input data, files, processes, and output data; and details of file structure and processes that allow determination of what audit trails and controls are available. One actual fraud case is discussed.

*(5170)*71*ac*ai*cd*dc*ge
Jacobson, Robert V. "Special Fire Needs for DP Users." COMPUTERWORLD, 30 June 1971, p. S-1.

*(5180)*73*aa*cc*dg*ff*fm*kd
Jancure, E.; and Berger, A. (eds.) COMPUTERS, AUDITING, AND CONTROL. Auerbach Publishing Company, Philadelphia, Pennsylvania, 1973.

*(5190)*71*aa*cc*da*db*hj
Jaspan, Norman. THE THIEF IN THE WHITE COLLAR. J. B. Lippincott Company, Philadelphia, Pennsylvania, 1971.

This book documents many of the reasons that cause employees, even at high management levels, to attempt embezzlement. The motives cited are quite universal. In the early days of the computer, many top executives hoped the computer would provide better methods of internal control. They felt that the computer could provide many more ways of keeping control, its complexity would discourage frauds, and the fewer accounting personnel needed would lessen fraud attempts. Unfortunately, these generalizations haven't proven to be true.

*(5200)*69*ab*cb*dc*dd*de*em*lb*nb
Jasper, David P. "A Discussion of Checkpoint/Restart." SOFTWARE AGE, October 1969.
Problems encountered in time-sharing systems and criteria for determining an optimal checkpoint frequency are discussed.

*(5210)*70*ab*cc*dg*ff*fx*kd
John, Richard C.; and Nissen, Thomas J. "Evaluating Internal Control in EDP Audits." THE JOURNAL OF ACCOUNTANCY, February 1970.
This article discusses several things that must be checked when evaluating EDP internal controls.

*(5220)*69*ab*cc*cd*dg*fv*fy*kb*kd*mc*nf*x1
Johnson, C. B. "Protection Primer for EDP Records." BANKING, December 1969, pp. 85-86.
The author briefly discusses the following data protection methods: remote storage of important backup files; three-generation backup; insurance; and fireproof vaults. He believes that a combination of these methods is necessary. Although insurance can be purchased to provide computer coverage, its cost usually forces the purchaser to obtain only minimal coverage that does not begin to cover the actual losses resulting from disasters. (An article by Edward J. Bride in the September 6, 1972 issue of COMPUTERWORLD states that, "Insurance may be cheaper than security".) The author concludes by listing the following four steps in developing a data protection system: determine the files needing protection; determine the ideal combination of safeguards; balance the ideal combination against its cost; and periodically test the security of the implemented system.

*(5230)*68*ab*cc*cd*da*hc*kb
Johnson, D. "Control and Prevention of Thefts of Proprietary Information." INDUSTRIAL SECURITY, February 1968.

*(5240)*72*ab*cc*dg*fy*x1
Johnson, J. D. "Most Loss-Prone Computer Systems Seen as Dangerously Underinsured." NATIONAL UNDERWRITER: Property

and Casualty Insurance Edition, 12 May 1972, p. 24.

The article states that only an estimated 25% of more than 60,000 computer installations have sufficient security and insurance protection. This statement is not supported or expanded on. A few basic safeguard measures are recommended.

*(5250)*71*ac*ai*cc*cd*da*dc*fb*nb*nd*x3
Johnson, James H. "DP Security Needs Not Unusual." COMPUTERWORLD, 11 August 1971, p. 8.

The concept that physical security must be tailored for a computer center is a myth. Scare tactics are sometimes used to exploit the corporate executive and sell him unjustifiably expensive equipment. If your firm doesn't have a security officer select two security firms to bid on conducting a security study. Have each firm prepare a report giving: a security plan, a recommended list of suppliers for each item recommended, and an estimate of the cost of complete installation. Purchase the equipment on a competitive bid basis. If the security firm isn't well known, question the background of its personnel. Physical security for computers does not require any special knowledge of EDP. Physical security is simply physical security!

*(5260)*68*ae*ag*cb*db*dc*dd*eb*ed*eh
Jones, R. S. "Data File Two - A Data Storage and Retrieval System." AFIPS CONFERENCE PROCEEDINGS, Spring Joint Computer Conference, Vol. 32, 1968, pp. 171-181.

Data integrity was one of the major design considerations of this system.

*(5270)*64*ab*cc*ff*ni
Joplin, B. J. "An Internal Control Checklist for EDP." MANAGEMENT SERVICES, July 1964, pp. 32-37.

*(5280)*66*ab*cc*fc*ff
Joplin, H. B. "The Accountants Role in Management Information Systems." JOURNAL OF ACCOUNTANCY, March 1966.

*(5290)*68*ac*ai*bb*cc*db*hj*hk*hl*hm*ku
"Journal Warns of Dishonest 'Computer-Operators'." COMPUTERWORLD, 17 April 1968.

This article refers to a WALL STREET JOURNAL article on computer operator fraud. Some fraud cases are described, but most do not deal with computer operators. In one case, a brokerage firm employee modified a computer program to mail dividend checks to his address. He had stolen $18,000 before being caught. In another case, a brokerage firm vice-president stole $250,000 before being caught.

*(5300)*71*ab*cc*ff
Juranas, L. A. "Auditing in the Systems Design Environment." THE INTERNAL AUDITOR, September 1971.

*(5310)*70*ac*bb*cc*db*hj*la
"Just Plain Grabbing is Becoming Old Hat to Securities Thieves." WALL STREET JOURNAL, 26 October 1970.

The article discusses the increasing sophistication of fund transfer and stock certificate frauds occurring in Wall Street brokerage firms. The brokerage firms are implementing better safeguards, but the embezzlers are also expected to improve their techniques.

*(5320)*aa*eq*nn*x3
Kahn, D. THE CODEBREAKERS. Macmillan Company, New York, 1967, 1164 pp.

This classic book is a chronicle of the entire history of cryptology from over 4000 years ago up to 1966. Its author narrates the development of various methods of making and breaking codes and ciphers, and tells how these methods have affected men and history. Mr. Kahn believes that 90% of the material in his book has not been previously published in other books. He also states that his book is not a textbook. He only explains at length two basic methods of solution, although many others are briefly sketched. The book isn't completely exhaustive either, since considerable foolish secrecy still surrounds World War II cryptology. A useful glossary of cryptology terms can be found on pages 13 through 16 of the introduction. Unfortunately, there is no discussion of recent computer aided cryptology systems.

*(5330)*66*ab*cc*da*de*ka*mb*nl*nm
Karst, K. L. "THE FILES: Legal Control Over the Accuracy and Accessibility of Stored Personal Data." LAW AND CONTEMPORARY PROBLEMS, Vol 31, Spring 1966, pp. 342-376.

*(5340)*69*ad*cb*cc*da*mb
Karush, A. D. "The Computer System Recording Utility: Application and Theory." SP-3303, System Development Corporation, 2500 Colorado Avenue, Santa Monica, California 90406, March 1969.

*(5350)*69*ad*cb*da*db*el*ff
Karush, A. D.; and Larson, R. H. "Analysis and Measurement of the AUDIT Recording Function." TM-4435, System Development Corporation, 2500 Colorado Avenue, Santa Monica, California 90406, August 1969.

*(5360)*71*ab*cc*ff
Kelly, W. E. "Computer Systems: Slaves or Masters?" MANAGEMENT ACCOUNTING, October 1971, pp. 9-11.

*(5370)*73*ac*cc*da*fe*ka*mf*nm*x2
Kenney, Michael. "Sargent Told FBI Data System Will Include Rights Safeguards." THE BOSTON GLOBE, 13 July 1973, p. 5.

U.S. Attorney General Elliot Richardson assured Governor Sargent of Massachusetts that "appropriate operational and legislative safeguards" will be put around the FBI's national crime information system. Governor Sargent had earlier said that Massachusetts would not participate in the national crime information system because it lacked internal, external, and statuatory safeguards. Massachusetts' own criminal history system does have extensive safeguards. Unfortunately, the federal government is now challenging in court Massachusetts' right to limit access to its system.

*(5380)*69*ae*cb*da*db*dc*ea
Kersta, L. G. "Voice Pattern Identification of Speakers." PROCEEDINGS OF CARNAHAN CONFERENCE ON ELECTRONIC CRIME COUNTERMEASURES, University of Kentucky, Lexington, Kentucky, 1969, pp. 127-136.

*(5390)*71*ab*cc*fa*ff
Kessler, L. M. "Accounting Profession's Opportunities in EDP - Today and Tomorrow." MANAGEMENT ADVISOR, May 1971, pp. 44-48.

*(5400)*72*ab*bb*cc*db*hk*ii*mc*x3
"Key Punch Crooks." TIME MAGAZINE, 25 December 1972, p. 69.

Five examples of computer fraud are discussed. The following two are particularly interesting. A Washington, D.C. man pocketed all the blank deposit slips at the writing desks of the Riggs National Bank and replaced them with his own electronically coded forms. For the next three days every customer who used these blank forms had his deposit credited to the culprit's account. The thief reappeared, withdrew $100,000, walked away, and has not yet been identified. In another case, Jerry Schneider, a 21-year-old UCLA engineering graduate, studied Pacific Telephone and Telegraph's computer by posing first as a journalist and later as a customer. He learned enough to place commercial orders for telephone equipment simply by punching the right beep tones on his own touch tone telephone. He then illegally ordered over $1,000,000 worth of electronic equipment and sold it through a dummy firm. Schneider was caught when one of his employees in the dummy firm became dissatisfied with his share of the loot and turned him in. Schneider received a forty day jail sentence. He has recently started his own computer security firm.

*(5410)*72*ab*cc*fc*ff
Keyes, E. G. "The Auditor's Role in New Systems Development." THE INTERNAL AUDITOR, January 1972.

*(5420)*72*ab*cc*ff*fx
Kiefer, G. H. "Systems Auditing with Test Decks." MANAGEMENT ACCOUNTING, June 1972, pp. 14-18.

*(5430)*73*ab*cc*ff
King, K. G.; Crowe, Chizek; and Welke, W. R. "Data Processing and the Auditor." DATA MANAGEMENT, February 1973, pp. 13-16.

*(5440)*69*ab*cc*dg*fp*gc*ge
Koefod, Curtis F. "The Handling and Storage of Computer Tape." DATA PROCESSING MAGAZINE, July 1969.

*(5450)*73*ab*ba*cb*da*ep*eq*hb*je*kb*x3
Koehn, Hank E. "Are Companies Bugged About Bugging?" JOURNAL OF SYSTEMS MANAGEMENT, January 1973, pp. 12-13.

Richard M. Nixon and his friends have provided us with an excellent example of the invasion of privacy through wiretapping. The apparent lack of concern over wiretapping is probably due to the naive attitude that wiretapping is only used against criminals. However, widespread illegal use of wiretapping does exist. Wiretapping may be illegal, but the equipment isn't. Several large electronic supply houses readily sell wiretap devices. Wiretapping is almost impossible to prevent, and commercial telephone/telegraph lines are not secure. The author suggests that cryptography and scrambling devices be used to protect sensitive communications. Their cost is not prohibitive. One very interesting example is given of successful use of cryptography. A local syndicate attempting to purchase several city blocks for a real estate development encrypted its computerized status reports that were processed at a service bureau. Known unauthorized access attempts failed to decipher the data.

*(5460)*72*ac*cc*da*f1*hc*nl*x2
Kohlmeier, Louis M. "Computer Work Isn't Patentable, High Court Says." WALL STREET JOURNAL, 21 November 1972, p. 3.

The Supreme Court in a six to zero vote ruled that computer programs are not patentable. This article briefly describes some facts of the case upon which this decision was made. Several quotes from the majority opinion, written by Justice William O. Douglas, are given. Computer manufacturers were against patentability because they felt it would hinder development of programming and the future of computer sales.

*(5470)*69*ab*cb*ek*ff
Korn, S. W. "Pre-Packaged Computer Programs Expand Computer Services." CPA JOURNAL, November 1969, p. 851.

*(5480)*69*aa*cc*dg*gg
Krauss, Leonard I. ADMINISTERING AND CONTROLLING THE COMPANY DATA PROCESSING FUNCTION. Prentice-Hall Inc., Englewood Cliffs, New Jersey, 1969.

*(5490)*72*aa*cc*cd*dg*nf*ni*nn*x3
Krauss, Leonard I. SAFE: SECURITY AUDIT AND FIELD EVALUATION FOR COMPUTER FACILITIES AND INFORMATION SYSTEMS. Firebrand, Krauss and Company, P.O. Box 165, East

Brunswick, New Jersey 08816, 1972, 284 pp., $24.95 (loose-leaf).

250 pages of this workbook are devoted to rating sheets covering 392 checkpoints for physical and procedural safeguards. The odd-numbered pages are rating sheets, and the even-numbered pages are left blank for the user to enter comments. The rating sheets, organized for quantitative scoring of an installation's secureness, are divided into the following eight areas: physical controls; operational controls; data, programs, and documentation; backup; development controls; personnel; insurance; and overall security program.

*(5500)*72*ad*ak*cb*da*dc*gf

Krewson, N. N.; and Tait, J. B. "Holographic Security Key." IBM TECHNICAL DISCLOSURE BULLETIN, Vol. 14, No. 12, May 1972, pp. 3832-3834.

This article describes a device that can be used to identify and authenticate remote terminal users, or control access to a computer room. The key must be placed in a certain position and then, in sequence, turned to any of a number of positions in a prearranged order. The key includes a window and a reflective hologram. The key-receptacle includes a light source and a light sensor.

*(5510)*70*ab*cb*da*eq

Krishnamurthy, E. V. "Computer Cryptography Techniques for Processing and Storage of Confidential Information." INTERNATIONAL JOURNAL OF CONTROL, November 1970, pp. 753-761.

*(5520)*72*ab*cb*eq*gh

Kugel, H. C. "Three Cipher-Decipher Programs Make Good OS/360 Demo's." CANADIAN DATASYSTEMS, April 1972, pp. 38-40.

*(5530)*73*aa*cb*cc*cd*dg*ni*np*x4

Kuong, Javier F. COMPUTER SECURITY, AUDITING AND CONTROLS - A BIBLIOGRAPHY. Management Advisory Publications, P.O. Box 151, Wellesley Hills, Massachusetts 02181, 1973, $7.50.

The three hundred articles in this non-annotated bibliography are classified into the following main headings (and subheadings): EDP Auditing and Controls (EDP Auditing - General Aspects, Auditing With the Computer, Generalized Software Packages, EDP System and Internal Auditing Controls, EDP Education for the Auditor); Computer Security and Privacy (Physical Security, Fraud and Theft, Privacy and Legal Aspects, Insurance); EDP Planning and Operations Control; Management Review and Evaluation of EDP; On-Line and

Real-Time Systems; and Checklists and Guidelines. The classification scheme is designed to simplify the task of locating relevant articles, and the author concedes that it is somewhat arbitrary. Only relevant articles already generally available to the public in published form are included in the bibliography. The author avoided listing more articles than he felt could reasonably be investigated within a practical time frame. Marginally relevant articles are omitted. The bibliography is an especially valuable reference source for computer auditing and control articles since these articles are scattered over a rather large number of sources which publish these relevant articles on an irregular basis.

Kuong's bibliography covers the period from 1964 to June 1973. He plans to publish semi-annual updates with the first update being available in January 1974. Subscription costs for these updates will be $30 per year. Detailed guidelines and procedures manuals can also be obtained through special arrangements with Management Advisory Publications. Manuals can be currently obtained for "EDP Security, Auditing and Controls Planning" and "EDP Operations Center Auditing and Evaluation". Comprehensive flow charts and checklists are included in these manuals to facilitate their use.

*(5540)*73*aa*cb*cc*cd*dg*fa*fb*ff*fx*nf*nn
Kuong, Javier F. COMPUTER SECURITY, AUDITING AND CONTROLS, TEXT AND READINGS. Management Advisory Publications, P.O. Box 151, Wellesley Hills, Massachusetts 02181, 1973 (in preparation).

This book, currently in preparation, will contain a text section and a selection of some of the most useful and informative articles on computer security, auditing, and controls. Topics to be covered include: EDP auditing; computer security principles and procedures; computer center management and control; systems internal controls; and guidelines on how to conduct management reviews of data processing activities. The author plans to condense into one book the accumulated experience of experts in the field, and knowledge gained from extensive experience in conducting consulting assignments on organizational and audit studies of DP installations.

*(5550)*65*ab*cc*da*kb
Lachter, Lewis E. "Preventing Business-Secret Espionage." ADMINISTRATIVE MANAGEMENT, December 1965.

This article describes safeguards to prevent loss of business secrets.

*(5560)*69*ae*ag*cb*ed*ei*gh*x2
Lampson, B. W. "Dynamic Protection Structures." AFIPS CONFERENCE PROCEEDINGS, Fall Joint Computer Conference, Vol. 35, pp. 27-38.

The author describes an access control scheme that has been developed as part of the operating system for the Berkeley Computer Corporation Model 1. This scheme is mainly concerned with how information which specifies protection and authorizes access, can itself be protected and manipulated. Some fundamental concepts of Lampson's model are briefly described below. "Objects" (files, pages of memory, processes, domains, interrupt calls, terminals, and access keys) are named by "capabilities" which are names protected by the system. Users can not create or modify capabilities arbitrarily. Thus possession of a capability can be taken as prima facie proof of the right to access the object it names. A new kind of object called a "domain" is used to group capabilities. Any process executing in some domain can exercise all the capabilities belonging to that domain. The only reason for creating a new domain is to establish an environment in which a process may execute with different protection than that provided by any existing domain. To provide an adequate mechanism for transfers between domains, the idea of a protected entry point or "gate" is introduced. Normally all transfers are allowed only at gates. To pass through a gate an appropriate "access key" must be presented. These access keys are themselves objects and can only be obtained in the same manner that other objects are obtained.

After describing the above concepts, the author goes into a detailed discussion on implementing his model. The model allows two domains to work together with any degree of intimacy, from complete trust to bitter mutual suspicion. It also allows a domain to exercise firm control over everything created by it or its subsidiaries.

*(5570)*70*ae*cb*dd*ei
Lampson, B. W. "On Reliable and Extensible Operating Systems." INFOTECH STATE OF THE ART PROCEEDINGS, 1970.

*(5580)*69*ad*bc*dg*ed*gh*lb
Lampson, B. W. "An Overview of the CAL Time-Sharing System." Computation Center, University of California, Berkeley, California, September 1969.

*(5590)71*ae*cb*dg*ee
Lampson, B. W. "Protection." PROCEEDINGS - FIFTH ANNUAL PRINCETON CONFERENCE ON INFORMATION SCIENCES AND SYSTEMS, Department of Electrical Engineering, Princeton University, Princeton, New Jersey, March 1971, pp. 437-443.

This paper discusses Lampson's theory on access control. Much of his theory is based on concepts first developed by J. B. Dennis and E. C. Van Horn, such as "objects" possessing "capabilities".

*(5600)*67*ad*cb*ec*ed*ei
Lampson, B. W. "Scheduling and Protection in an Interactive Multi-Processor System." Ph.D. Dissertation, University of California, Berkeley, California, March 1967, 82 pp.

The following four types of protection are described: protection of the system from users, users from the system, users from themselves, and the system from itself. The author recommends that authorization for executing privileged instructions be determined, not by job identification, but by the location of the job in a special area of main memory. Four types of memory hardware protection schemes are discussed. They are: memory bounds registers which set limits on addressable space; page memory protection where access control is regulated by a page table; segmented memory protection where pages are grouped into segments; and partitioned memory protection where the entire main memory is divided into separate areas.

*(5610)*68*ab*ah*cb*ec*ed*ei
Lampson, B. W. "A Scheduling Philosophy for Multi-Processing Systems." COMMUNICATIONS OF THE ACM, May 1968.

This article is essentially a brief summary of important items in Lampson's Ph.D. dissertation.

*(5620)*66*ae*cb*ed
Lampson, B. W. "A User Machine in a Time-Sharing System." IEEE PROCEEDINGS, Vol. 54, No. 12, December 1966.

*(5630)*71*ab*cc*dc*fv*x1
Lang, William Jr. "Backup Files are a Must." ADMINISTRATIVE MANAGEMENT, October 1971, p. 55.

The author states that grandfather-father-son backup must be kept for important data files if a firm is to survive a disaster in its computer installation. He briefly explains how these backup files should be updated and stored.

*(5640)*71*ac*ai*cc*dg*fb*fr*fs*ft*ia*ic*id*ie*jb*x3
Lange, Diane. "Employees Called Biggest Security Risk at Centers." COMPUTERWORLD, 23 June 1971, p. 2.

This article discusses a speech made by Robert E. Wiper, educator and behavioralist, before the Computer Protection/Insurance Workshop sponsored by BUSINESS INSURANCE NEWS MAGAZINE and COMPUTERWORLD. As increased physical protection has made access to DP centers more difficult, employees are becoming the biggest security risks. Many security measures undertaken by data centers have placed the employees in a position where they are more subject to attempts at bribery or extortion. Some personality conditions that can create losses are: members of anti-establishment groups; real or imagined grievances against employers; employees with jobs that have no future; and employees who have mismanaged their personal goals and objectives. Mr. Wiper suggests that behavior profiles be given to job candidates before hiring them. He also strongly suggests that all DP jobs have a path leading to a better job. Dead end jobs do not help employee morale and could produce enough dissatisfaction to result in a disaster. Authorization control of employees should be replaced by goal-oriented management.

*(5650)*70*ab*be*cc*de*fh*hp*hr*ka*x1
Lauren, Roy H. "Reliability of Data Bank Records." DATAMATION, May 1970, pp. 88-89.

The author lists some typical databanks that the average individual is likely to be part of, and gives two examples showing that these databanks will often contain errors. He suggests that more control over databank errors is necessary, but doesn't say how this could be done. The public needs to be convinced that databanks can benefit them, but this may be difficult if databanks only store negative information on individuals.

*(5660)*64*ab*ah*cc*da*db*f1
Lawlor, Reed C. "Copyright Aspects of Computer Usage." COMMUNICATIONS OF THE ACM, October 1964.

This article is somewhat obsolete, but it still serves as a good introduction to the copyright field.

*(5670)*70*ac*ai*bc*cd*dc*me*nk
"Leaky Center May Lose Vendor Support." COMPUTERWORLD, 7 October 1970.

Burroughs Corporation is threatening to discontinue its services to the Jacksonville, Florida EDP Center. It wants the center to move its EDP equipment to a safer location.

*(5680)*70*ac*ai*cb*da*db*ed*eq*gh
Leavitt, Don. "Cipher/1 Designed for Assurance of Total File Privacy." COMPUTERWORLD, 10 June 1970.

A cryptographic software security package is described.

*(5690)*72*ac*ai*cb*da*ep*er*x2
Leavitt, Don. "Compression Shields Data While Operations Improve." COMPUTERWORLD, 6 December 1972, p. 16.

Users who don't want to go as far as encrypting to protect their data have other options such as data compression. Compression packages function by collapsing "extra" repeated characters, whether blanks or actual data, into a single character (or bit) ahead of the compression. Some packages go further and allow two alphabetics or four numerics to be stored in a space normally required for one character. Compression is used to reduce storage requirements, but this saving in disk and tape storage is offset by processing costs for encoding and decoding the data. Compressed data is often not normally recognized by a data thief. However, the compression routines are often part of an installation's operating procedure, and a persistent thief will not be stopped by compressed files.

*(5700)*72*ac*ai*cb*da*eq*gh*x1
Leavitt, Don. "Encrypting Routines Offered, But Not Widely Used." COMPUTERWORLD, 6 December 1972, p. 18.

This article contains a short general discussion on cryptography. Some of the more interesting comments are briefly stated below. Although various software houses offer efficient cryptographic packages, there has been no great demand for this type of support. One very serious restriction on the use of encrypting lies in the inability of some central processor units or other equipment to accept all the characters generated by the encoding routines. Some communications gear, for example, reserve certain codes as control characters. Encrypting adds very little time to the processing. One vendor has a routine that can process 23,000 80-character records per minute on an IBM 360/30. Also, most encrypting routines require little storage. One routine needs only 500 bites for the coding and 880 bites for work space.

*(5710)*72*ac*ai*cb*da*ed*x1
Leavitt, Don. "Passwords Protect Data and Programs." COMPUTERWORLD, 6 December 1972, p. 13.

Most of this article describes simple uses of passwords that would be useful only to those unfamiliar with computers. However, a few interesting statements are made, and some of them are stated below. Some software houses include controllable "self-destruct" routines in their programs to block extended use of a proprietary product on a pre-installation trial. Sometimes variants of these routines are used if an authorized user fails to pay the agreed-upon rental or if the package is stolen from a legitimate user. The author does not describe any particular "self-destruct" mechanisms, but he suggests that any user could incorporate them into his programs. Database management systems make it easier for a user to interface with his data. They also provide access-control security because users do not access data by its physical location and must know the proper file name to access someone else's file. Therefore, proper access-control over the dictionary of file names will provide at least some security.

*(5720)*73*ac*ai*bb*cc*db*hk*if*kb*kd*mc*x2

Leavitt, Don. "Physical DP Tampering Discounted in Bank 'Shuffle'." COMPUTERWORLD, 25 April 1973, p. 4.

An investigation into the embezzlement of funds from the Union Dime Savings Bank has shown the theft did not involve unauthorized computer hardware or software changes. However, changes were made to computerizes customer account records through unauthorized use of a teller's terminal. These data input changes appeared to be valid transactions to the computer programs. The thief, a supervisor, circumvented the bank's dual control system by gaining unauthorized access to both the teller's terminal and the branch reserve cash supply. Fortunately, the computer system's audit trail routines will enable the bank to easily identify the defrauded customer records.

*(5730)*73*ac*ai*bc*cb*cd*dc*fv*gc*jg*nk*x2

Leavitt, Don. "Tornado Levels DP Center, 90 Hours Later CPU Is Up." COMPUTERWORLD, 18 April 1973, p. 1.

Rapid recovery was made possible according to Charles Darnell, Lithonia Lighting's DP manager, by hard work by his own staff, an impressive dedication to the job by IBM engineers (even though the CPU was on a third-party lease), and good audit trails provided by the Environ/I-Total database management system. Most of the article's focus is on the resulting damage and IBM's support.

*(5740)*67*ab*cc*db*de*ff*hk*hp

Lee, D. F. "A Structural Check of Accounting Input Data in a Computer System." JOURNAL OF ACCOUNTING, June 1967, p. 54.

*(5750)*70*ab*ba*bb*cc*cd*da*db*fd

Lefer, H. "How to Shield Your Office Against Crime." MODERN OFFICE PROCEDURES, April 1970, pp. 21-29.

Part of this article discusses security for EDP installations. A method is given for determining what records are vital. Several fraud and theft examples are also given.

*(5760)*69*ab*cc*da*f1*kc*nl*x1
"Legal Protection for Computer Programs." COMPUTERS AND AUTOMATION, February 1969, pp. 12-13.
This is a position paper favoring legal protection by patents for computer programs. It was adopted by the Association of Independent Software Companies at their first annual meeting on November 21, 1968. The paper discusses advantages of patent protection, recent related activity in the legislative and executive branches of government, and an example supporting patent protection. But in view of the December 1972 Supreme Court ruling against software patents, this article is purely academic. A more current discussion on this subject can be found in an article by David Goldberg entitled "Legal Protection of EDP Software" and printed in the May 1972 issue of DATAMATION.

*(5770)*71*ab*cc*ff
Leishman, R. O. "The Computer as an Audit Tool." THE INTERNAL AUDITOR, January 1971.

*(5780)*68*ad*ca*dg*ee
Lesser, V. R. "A Multi-Level Computer Organization Designed to Separate Data-Accessing from Computation." CS90, Computer Science Department, Stanford University, Stanford, California, March 1968.

*(5790)*71*ac*ai*cc*dg*fz*ma
"Let Customer Beware in Computer Contracts." COMPUTERWORLD, 13 January 1971, p. 1.

*(5800)*69*ab*cc*df*dg*ff*fv*kb*kd*x2
Levine, R. A. "How to Protect Your EDP Records." NEW YORK CERTIFIED PUBLIC ACCOUNTANT, May 1969, pp. 353-356.
The author gives a number of brief recommendations for protecting EDP records through validation of processing program operation, validation of input data, and backup for files and equipment. A few of these recommendations are given below. The processing should include: a sequence check of files; a check of computation results against predefined limits; an accumulation and verification of input and output record counts; and an accumulation and verification of hash totals of numerical fields against totals stored in trailer records. All output files should be label-checked to determine if the file name and real sequence correspond with the program requirements. Planning should include appraisal of each piece of equipment as to the effects of its failure on the

over-all processing system. A son-father-grandfather backup concept should be used with the grandfather copy retained at an off-site location.

*(5810)*73*ab*cc*da*dd*de*hd*ka*x2
Lewis, Ephraim A. "A Myth-Destroying Study of Computers." BUSINESS WEEK, 13 January 1973, pp. 9-10.

This article reviews a recently published book by Alan F. Westin and Michael A. Baker entitled DATABANKS IN A FREE SOCIETY. For a summary of this article, read the annotation under the entry for the book.

*(5820)*71*ab*cc*ff
Lewis W. F. "Auditing On-Line Computer Systems." JOURNAL OF ACCOUNTANCY, October 1971, pp. 47-52.

*(5830)*70*ab*bc*cd*dc*jg
"Light Plane Lights ADR's Fire." DATAMATION, January 1970, p. 174.

This article describes an accident where an out-of-gas, light plane crashed into Applied Data Research, Inc. and started a fire which caused serious damage to ADR's computer room.

*(5840)*70*ac*ai*cc*cd*dg*ft*ga*gf*x1
"Limiting Access to Centers Called a Major Problem." COMPUTERWORLD, 24 June 1970.

Joseph Wasserman and Louis Scoma are quoted on physical access problems. These two security consultants feel that a showcase computer room is asking for trouble. They recommend periodic six month EDP personnel investigations and immediate dismissal of fired or laid-off employees.

*(5850)*69*ae*ag*ca*da*db*gh*hb*lb*mh
Linde, R.; Weissman, C.; and Fox, C. "The ADEPT-50 Time-Sharing System." AFIPS CONFERENCE PROCEEDINGS, Fall Joint Computer Conference, Vol. 35, 1969, pp. 39-50.

This paper describes the unique system architecture of ADEPT-50. The ADEPT system operates on IBM System/360 computers. It is a general purpose system designed to operate in a military context and to support a limited number of large, compute and I/O bound programs, dependent upon large files of data. The system will adequately serve a larger number of users if their programs are small and if they limit their demands on the systems resources. The user can have the same commands for controlling his program as those used by the executive program. The security techniques built into the system are novel. They are described in detail in "Security Controls of the ADEPT-50 Time-Sharing System" by Clark Weissman. This Weissman article is also in volume 35 of the AFIPS CONFERENCE PROCEEDINGS.

*(5860)*69*ab*cc*ff
Lindgren, L. H. "Auditing Management Information Systems." JOURNAL OF SYSTEMS MANAGEMENT, June 1969, pp. 22-27.

*(5870)*72*ab*cc*fc*fm
Lo Russo, P. M. "The Operations Manager's Job." DATA MANAGEMENT, September 1972, pp. 32-34.

*(5880)*71*ab*cc*ff
Lobel, J. "Auditing in the New Systems Environment." JOURNAL OF ACCOUNTANCY, September 1971, pp. 63-67.

*(5890)*69*ab*cc*ff*mc
Lombara, S. E. "Auditing Credit Cards Via Computer." MAGAZINE OF BANK ADMINISTRATION, November 1969, p. 37.

*(5900)*70*ab*bc*cd*dc*jg*x3
"Looking at Fire Hazards." FIRE JOURNAL, May 1970.

Approximately twenty-five examples of actual computer room fires are given. Losses ranged from $900 to $4,500,000 with the average well over $100,000. The article should definately be read by those concerned with fire protection of computer equipment.

*(5910)*71*ab*cc*df*fm
Lucas, H. C. "Performance Evaluation and Monitoring." COMPUTING SURVEYS, September 1971, pp. 79-91.

*(5920)*69*ae*cb*da*db*dc*ea*gh
Luck, J. E. "Description of a Real-Time Completely Automatic Speaker Verification System." PROCEEDINGS OF CARNAHAN CONFERENCE OF ELECTRONIC CRIME COUNTERMEASURES, University of Kentucky, Lexington, Kentucky, 1969, pp. 98-113.

*(5930)*72*ac*ai*bb*cc*if*ka*kf*me*nj*x2
Lundell, E. Drake Jr. "'Absent' DPer Cites City Misuse." COMPUTERWORLD, 20 December 1972, p. 4.

After charging that the Honolulu mayor improperly used the city's computers in a reelection bid, Larry Stevens, a computer specialist, mysteriously disappeared and is still missing after a two month police investigation. In the meantime, Mayor Frank F. Fasi has been reelected. On the day before he disappeared, Stevens charged in a notorized statement that the Fasi campaign organization had illegally used computer equipment and programming manpower, valued at between $50,000 and $100,000, at the expense of the taxpayers.

*(5940)*72*ac*ai*bc*cd*dc*jg*jh*na*nk*x2

Lundell, E. Drake Jr. "Big Cleanup Beings After Agnes Cripples DP Centers in 5 States." COMPUTERWORLD, 5 July 1972, p. 1.

Hundreds of computer systems were buried under tons of water and mud as floods spawned by tropical storm Agnes inundated the Middle Atlantic section of the country, killing over 100 people and leaving thousands homeless. This article briefly describes damage done to a score of flooded installations. All the users interviewed by COMPUTERWORLD were impressed with the aid they were getting from vendors.

*(5950)*72*ac*ai*cb*cc*da*ka*mb*ng*nl*nm*x2

Lundell, E. Drake Jr. "Canadian Study Sees Role for United Nations in Privacy Issue." COMPUTERWORLD, 20 December 1972, p. 2.

This article briefly reveals some of the findings made by a Canadian Task Force studying the issue of computers and their relationship to personal privacy. One of the more interesting findings was that a great deal of data about citizens of one country is presently being stored in computer databanks in other countries. The task force suggested that the United Nations might provide an appropriate forum for consideration of this problem. An overall government program to establish rules for Canadian governmental databanks was proposed. Other findings include: personal information is being collected faster than most Canadians suspect, a large amount of data interchange is occurring among firms, and few safeguards are used.

The "Privacy and Computer Task Force Report" is available for $2.50 from Communications Canada, Information Service, 100 Metcalfe Street, Ottawa, Ontario. For a more detailed discussion of this report see an article by John M. Carroll entitled "Snapshot 1971 - How Canada Organizes Information About People" in the 1972 Fall Joint Computer Conference proceedings.

*(5960)*72*ac*ai*cc*da*db*ka*mb*nl*nm*x3

Lundell, E. Drake Jr. "Disclosure of Federal Dossiers Proposed." COMPUTERWORLD, 28 June 1972, p. 1.

A bill, H.R. 9527 in the House and S. 975 in the Senate, is described which would require all government agencies maintaining dossiers on individuals to disclose the existence of those files to the individuals concerned. The bill, known as the Citizen's Privacy Act, would: prohibit any one government agency from disclosing an individual's file to anyone outside the agency without the individual's consent; require agencies to notify the individuals that they plan to start files on; and give individuals the right to inspect their files and add supplementary information if needed. Files relating to national security and law enforcement are excluded. The bill is viewed by several lawmakers as a test case of Congressional attitudes toward the protection of privacy in computer databanks. It is much stronger than the Credit Information Act passed last year.

*(5970)*71*ac*ai*ba*cb*cc*da*el*f1*hc*hm*ih*kc*ma*nj*x2
Lundell, E. Drake Jr. "Firm Sues Ex-Employees Over Proprietary Programs." COMPUTERWORLD, 22 December 1971, p. 6.

Computer Sharing Services (CSS) has filed a suit against Computer-Time Corporation (CTC) and three former CSS employees now with CTC. CSS has charged that the defendants stole a least several of its proprietary programs and were using them in CTC's operations. CSS couldn't determine the exact programs allegedly stolen because part of its computerized audit trail, that would have revealed the theft, was also missing. The defendants are challenging CSS's claim that certain of its programs are proprietary.

*(5980)*72*ac*ai*cb*cc*cd*da*db*dc*ft*nf*nn*x3
Lundell, E. Drake Jr. "'Inflexible' DP Systems Said to Attract Dishonesty." COMPUTERWORLD, 1 November 1972, p. 2.

Some comments made by Donn B. Parker at the First International Conference on Computer Communication are presented. Computer related crimes are described under categories of conventional crime such as: fraud, theft, larceny, forgery, conspiracy, vandalism, burglary, etc.. Typical reasons for computer criminal acts include: revenge, competition, politics, challenge to ability, power, wealth, avoidance of harm, sympathy to desires and needs of others, respect, peer group acceptance, and absence of positive motives.

Threats should not be confused with methods of penetration such as: software trapdoors, wiretapping, and password detection. Threats are the potential and actual actions of people. The nature of threats includes: (1) circumstances of peoples actions; (2) their ability to act; (3) procedures they use; and (4) technical methods they employ. Poking about in the system itself to find weaknesses and theorizing points of unintended penetration with little knowledge of the treats will only lead to serious discontinuities and inconsistencies in security. The owner's evaluation of the various assets to be protected may not coincide at all with the values placed on them by potentially dishonest people. The author predicts that the number of computer crimes will decrease in the future due to improved safeguards, but the losses per crime can be expected to increase.

*(5990)*72*ac*ai*bc*cc*dc*fw*gc*jg*na*x1
Lundell, E. Drake Jr. "Innovation Marks Efforts to Capture 'Flooded' Data." COMPUTERWORLD, 12 July 1972, p. 1.

This article describes efforts by several different computer users to recover data from damage done by tropical storm Agnes. The lost data, and not the equipment, was the main worry of most DP managers because manufacturers replaced most damaged equipment within a week or two of the storm. Almost all of the data salvaging involved cleaning cards and magnetic tapes of water and mud. A typical innovative cleanup idea was described as "wash gently with Lestoil, rinse, spin on a tape drive for five minutes, and dry under a hair dryer". A brief summary of physical damage done to equipment is also included.

*(6000)*72*ac*ai*bd*cc*dd*hr*mc*nj*x2
Lundell, E. Drake Jr. "Judge Rules Against 'DP Error' Defense." COMPUTERWORLD, 22 March 1972, p. 1.

State Farm Mutual Automobile Insurance Company claimed that it was not liable for an accident involving a policy holder who didn't renew his expired policy until after an accident. State Farm's computer made an error by automatically renewing the policy as effective before the accident upon receiving the late payment. The Colorado Tenth Circuit Court of Appeals ruled that the actual processing of the policy carried out by an unimaginative mechanical device can have no effect on the company's responsibilities for those errors and oversights.

*(6010)*72*ac*ai*cb*gh*id*x3
Lundell, E. Drake Jr. "More Secure (But Vulnerable) Systems Expected Soon." COMPUTERWORLD, 13 December 1972, p. 13.

This was the conclusion drawn by the ACM Special Interest Group on Computer Systems Installation Management during the Fall Joint Computer Conference. However, there is still debate on different security styles, including centralized versus decentralized access authorizations, the potential affects of unauthorized access to a firm's assets, and the population of potential penetrators. Jerry Kennedy, president of Basic Computing Arts, described the Data Sentinel System Monitor manufactured by his firm. The system is essentially a PDP-11 computer that monitors and controls all incoming requests to access databases that a firm wishes to keep secure. Robert Abbot, of Lawrence Livermore Laboratories, stated that such external systems have a place in security controls but cannot really protect a system from systems programmers.

*(6020)*72*ac*ai*cd*dc*ga*me

Lundell, E. Drake Jr. "State Mulls Flood Guides for Its Sites." COMPUTERWORLD, 13 September 1972, pp. 1-2.

*(6030)*72*ac*ai*cb*cc*cd*dg*ea*ed*ft*ia*nb*no*x3
Lundell, E. Drake Jr.; and Upton, Molly. "Users Awaken to Security Needs: Guarding Centers Primary Concern." COMPUTERWORLD, 6 December 1972, p. 1.

This article summarizes the results of a recent COMPUTERWORLD survey of large sophisticated computer users. Eighty percent of these large users said they would be willing to pay up to ten percent more on their monthly equipment rentals for a successful and workable data security system. All of the users indicated data security was "extremely" important to them. However, few have made use of scramblers or encryptors. Personnel screening and password hierarchies were the most relied upon methods of protecting sensitive data. They were used by ninety percent and seventy-five percent of the users respectively. But even with this awareness to protect sensitive data, most users still put most of their security efforts into physical protection. A majority of the users do not trust operators to handle sensitive printouts. Few of these users had strict personnel screening procedures, but most wished that they could have such screening.

*(6040)*73*ac*ai*bb*cc*db*hm*mk*x1
Lundell, E. Drake Jr. "Watergate Spawned Fear of 1972 Vote-Count Fraud." COMPUTERWORLD, 23 May 1973, p. 1.

With the tales of Watergate and other Republican political sabotage tactics rampant during the late stages of last year's Presidential campaign, officials in the McGovern for President organization became increasingly concerned that there would actually be tampering with the vote-count process, especially in computerized vote systems. An outside consultant was hired to give seminars in several states on what to look for in possible vote tampering. However, the effect was too little and probably too late. No vote fraud was uncovered.

*(6050)*73*ac*ai*cc*da*db*de*fe*ka*mb*nl*nm*x1
Lundell, E. Drake Jr. "World Group Urges Right of Inspection of Data Banks." COMPUTERWORLD, 9 May 1973, p. 7.

A report by a subcommittee of the Organization for Economic Cooperation and Development (OECD) recommends that all private databanks containing personal informtion be regulated just as credit databanks are now regulated in the United States. OECD, which has members from fourteen countries, noted that governments are faced with the problem of alienating the public over personal and societal implications of the computer, particularly in the area of personal privacy. The subcommittee felt government agencies could not meet all demands that would likely occur if everyone had unlimited access to see all his files at any time. Therefore, a regulation similar to the U.S.'s Fair Credit Reporting Act was suggested. The use of security techniques in personal data bases was not being actively considered by any country, since legal regulations were considered to be sufficient to protect sensitive data.

*(6060)*68*ae*cc*dc*fv*x1

Lunin, Lois F. "Protection Against Catastrophe: A Plan for Insuring Continuity of Information." PROCEEDINGS OF THE AMERICAN SOCIETY FOR INFORMATION SCIENCE, Greenwood Publishing Corporation, New York, Vol. 5 - Information Transfer, 1968, pp. 295-299.

The author briefly describes a file backup plan developed for the Information Center for Hearing, Speech, and Disorders of Human Communication at John Hopkins University. The backup plan was prompted by several Baltimore riots in 1968.

*(6070)*70*ab*cc*cd*da*db*dc*gf*x1

Luther, Frederick H. "Keeping the Computer Secure." ADMINISTRATIVE MANAGEMENT, October 1970, p. 10.

Several specific physical access control procedures are presented. All of them are well known. A few simple suggestions on storing backup files are also given.

*(6080)*70*ab*cc*dg*eh*ff*kd*x1

Lutter, Frederick H. "Protect the Database." ADMINISTRATIVE MANAGEMENT, November 1970, p. 10.

To prevent fraud, the following three interrelated areas must be controlled: database protection, program security, and application audit trails. This article presents some interesting but very brief comments on these three areas. File integrity checking must be kept separate from other processing, and a senior person should be responsible for it. Source language copies of production programs should not be sent to the computer room. Audit trail procedures must allow reconstruction at any time of any master record taken at random. These procedures must make it possible to trace any transaction, action document, or report to the corresponding master record as it existed at a specific past time.

*(6090)*67*ab*cc*cd*da*db*dc*fd*fs
MacDonald, M. B. Jr.; and Brown, J. K. "Company Security Practices." THE CONFERENCE BOARD RECORD, October 1967, p. 40-47.

The results of a survey on industrial security policies and procedures are presented. Visitor control, employee indoctrination, and identification of proprietary data are discussed.

*(6100)*69*ab*cb*dg
"Machine That Takes Secrecy in Hand." BUSINESS WEEK, 10 May 1969, p. 151.

*(6110)*73*ae*cb*ed*ei*x3
Madnick, Stuart E.; and Donovan, John J. "Application and Analysis of the Virtual Machine Approach to Information System Security and Isolation." Presented at ACM WORKSHOP ON VIRTUAL COMPUTER SYSTEMS, Cambridge, Massachusetts, 26 March 1973, 15 pp.

This paper shows that a combined virtual machine monitor - operating system (VMM/OS) approach to information system isolation provides substantially better software security than a conventional multiprogramming operating system approach. This added protection is derived from redundant security, using independent protection mechanisms that are inherent in the design of most virtual machine monitor - operating system systems. The improved security applies to complete isolation security in which no user is allowed access to other users' information. Generalized access control where users are allowed controlled partial access to each other's files is not considered.

*(6120)*72*af*cd*dc*dd*gc
"Magnetic Intrusion: The 'Silent Saboteur'." ADP NEWSLETTER, 18 September 1972, pp. 1-4.

This article summarizes a National Bureau of Standards technical note entitled "The Effect of Magnetic Fields on Magnetic Storage Media Used in Computers". Several commonly asked questions on the vulnerability of magnetic storage media are answered.

*(6130)*72*ac*ai*cb*dc*gc*jf*x3
"Magnets: A Surface Issue." COMPUTERWORLD, 30 August 1972, p. 1.

Two somewhat conflicting views are given on the vulnerability of magnetic tapes to magnets. W. D. Tiffany, manager of the security system research program at Stanford Research Institute, claims that a common "dime store" magnet of 250 gauss would affect a tape if held on the tape's surface, but it would have no affect if held 1/8th of an inch away or more. He believes that the tape canister would protect a tape from most magnets, at least small ones. But according to L. Conroy, director of Securitronics, relatively small magnets of 250-1000 gauss will make tapes useless, although not completely erasing them, when run over their plastic housing or metal container. For detailed information on Tiffany's research, read an article in the September 1972 issue of THE OFFICE entitled "Are Computer's Files Vulnerable to Magnets?"

*(6140)*71*ae*cb*cd*da*ep*jd*je
Maitland, P. "Data Transmission Privacy: Vulnerability and Protection." 43rd ANNUAL CONFERENCE OF THE PETROLEUM INDUSTRY, Electrical Association, April 1971.

*(6150)*71*ac*bc*cc*cd*da*db*dc*fr*jd*jf*nd*x3
Mandell, Mel. "Computer Scare Talk: Sabotage Fears of 'Experts' Discounted." NEW YORK TIMES, 9 May 1971, Sect. 3, p. 3.

The author shows that three major computer insecurities being widely discussed in the press and at business and technical gatherings are largely exaggerated. He blames security consultants who also sell security systems for greatly exaggerating threats in order to sell their equipment. These three threats are: radical attacks, infiltration of saboteurs with magnets, and "superspy" trucks that receive and process radiation from the nearby computers. The third threat is completely infeasible. As for sabotage by radicals, all the attacks to date have been at universities, giant corporations, or large banks. Mandell states that the real threat comes "not from long-haired radicals but from well barbered embezzlers". Embezzlement is one of the leading causes of business failure. A lesser threat comes from disgruntled employees. An intellegent security program should provide: adequate protection against well known hazards such as fire, water, and power failures; good hiring practices; good advancement opportunities; and proper discipline in the computer room.

*(6160)*71*ab*bc*cc*cd*da*db*dc*fr*jd*jf*nd*x3
Mandell, Mel. "Computer Security: Sabotage Fears Discounted." COMPUTERS AND AUTOMATION, October 1971, p. 29.

This article is a reprint of another article written by Mandell which appeared in the NEW YORK TIMES under the title "Computer Scare Talk: Sabotage Fears of 'Experts' Discounted".

*(6170)*71*ad*cb*dg*ed*ef*el*gh*lb
Manola, F. "An Extended Data Management Facility for a

General-Purpose Time-Sharing System." Master's Thesis, Moore School of Electrical Engineering, University of Pennsylvania, Philadelphia, Pennsylvania; or AD-724 801, National Technical Information Service, Springfield, Virginia 22151, May 1971.

This thesis describes the Extended Data Management Facility (EDMF) system developed by the Moore School. The system had data privacy as one of its main objectives. It implements the "authority item" concept developed by D. K. Hsiao in 1968. Protection can be provided at the field or record level, as well as at the file level. Both pre- and post-analysis of data retrieval is made. The system runs on a RCA SPECTRA 70/466 computer.

*(6180)*70*ac*ai*cb*dg*ep*lb*nk*x1

"Manufacturers' Safeguards for Data Called Inadequate." COMPUTERWORLD, 11 November 1970, p. 3.

Discussions at a recent Advanced Management Association Seminar are summarized. Louis Scoma, a computer security consultant, criticized computer manufacturers for not providing adequate hardware and software safeguards for data transmission. The Continental Airlines Reservations System was also described.

*(6190)*70*ac*ai*cb*nk

"Manufacturer Has Special Responsibility for Security Safeguards, Says FCC's Lee." COMPUTERWORLD, 16 December 1970, p. 7.

*(6200)*71*ab*cc*ni

Mariotti, J. J. "Checklists in Problem Solving." MANAGEMENT ADVISOR, May 1971, pp. 28-37.

This is a basic article on preparation of checklists.

*(6210)*70*aa*cc*fe*gg*nl*nm*x2

Martin, James; and Norman, Adrian R. D. THE COMPUTERIZED SOCIETY. Prentice-Hall Inc., Englewood Cliffs, New Jersey 07623, 1970, 574 pp., $10.95.

This book attempts to explain, to the man with little or no computer knowledge, what is happening in the computer industry and its laboratories, and what impact this is likely to have upon society in the next 15 years. It is not very informative to someone interested in security issues and knowledgeable in computers. Most of the book is concerned with privacy issues. Only four of the twenty-nine chapters are concerned with computer security issues. Chapter 18, "Crime and Sabotage", briefly discusses common problems unique to the computer that make it quite vulnerable to crime and sabotage.

Chapter 24, "The Laws That Are Needed", makes twelve strong recommendations for new laws. Chapter 25, "Locks, Guards, and Burglar Alarms", recommends 24 currently available safeguards that can and should, in most cases, be used to protect valuable and sensitive data. The title of chapter 25 is misleading, since only one of twenty-four safeguards is a physical safeguard. None of the safeguards mentioned are unique to this book and most can be easily found elsewhere. Chapter 26, "Systems Controls That Are Needed", briefly discusses the authorization problem, the user's legitimate need-to-know, encoding data, and controlling data collection.

*(6220)*70*ad*cb*da*ep

Massey, J. L.; Chang, J.; Geist, J.; Hartman, W.; and Seguin, G. "Convolutional Coding Techniques for Data Protection." NASA-CR-109773, University of Notre Dame, Notre Dame, Indiana, March 1970, 10 pp.

This article is quite technical and probably only useful to those familiar with coding techniques. A modified Fano sequential decoding algorithm is described. Also discussed is a class of complementary rate 1/2 non-systematic codes for sequential decoding.

*(6230)*72*ab*cc*fm*fn

Matheny, C. S. "Operations Planning and Scheduling." DATA MANAGEMENT, September 1972, pp. 32-34.

*(6240)*69*aa*cb*cc*dg*ep*lb*nl*nm

Mathison, S. L.; and Walker, P. M. COMPUTERS AND TELECOMMUNICATIONS: ISSUES IN PUBLIC POLICY. Prentice-Hall Inc., Englewood Cliffs, New Jersey 07623, 1969.

One chapter is devoted to privacy. It discusses possible regulatory controls.

*(6250)*72*ab*cc*fc*ff

Matson, M. C. "Systems Design and Internal Audit - An Effective Interface." THE INTERNAL AUDITOR, March 1972.

*(6260)*73*ac*bb*cc*db*hj*if*mc*x2

Maxwell, Neil. "Voice of Experience: Lamer Hill, Embezzler, Says Stealing is Easy." WALL STREET JOURNAL, 26 January 1973, p. 1.

Mr. Lamar B. Hill, former director and president of First National Bank of Cartersville, recently pleaded guilty to 60 of 180 counts of bank fraud. This article summarizes an interview with Mr. Hill on the day before he was to start serving a 10 year prison term. Mr. Hill had embezzled $4,600,000 over the last 21 years, but got tired of "remembering all those figures" and finally let himself get caught. He gave several reasons why bank embezzlement is easy. Incompetent directors who don't understand banking is one reason. Auditors who pay too much attention to bankers' complaints that earlier-morning audits inconvenience customers, and who stand around for 30 minutes before they get started is another reason. Mr. Hill said, "You give me 30 minutes and I can hide anything so that you'll never find it". When asked what happened to all that money, Hill appeared genuinely puzzled. "I just don't know", he said, "I've gambled some". He plans to write a book on embezzlement while in jail.

*(6270)*71*ab*cc*dg*fy*nb
McCahill, F. X. Jr. "Avoid Losses Through Risk Management." HARVARD BUSINESS REVIEW, May 1971.

The use of insurance to provide protection is discussed.

*(6280)*66*ac*cc*da*fj*ka*mb*nj*nl*nm
McCarthy, John. "Information." SCIENTIFIC AMERICAN, September 1966, pp. 65-72.

The author believes that privacy invasion from a single national information center can be controlled. However, laws must be passed which give the individual the right to inspect his own file and challenge its accuracy. Unauthorized access to certain information should be made legal grounds to bring a civil suit.

*(6290)*69*ab*cc*ff
McCollum, P. "Computer Systems Audit." MANAGEMENT ACCOUNTING, May 1969, pp. 51-52.

*(6300)*73*ad*cc*fb*fx
McFarlan, W. F. "Management Audit of the EDP Department." HARVARD BUSINESS REVIEW, May 1973, pp. 131-142.

*(6310)*69*ae*ag*cb*df*dg*ed*el*lb
McGeachie, J. S. "A Flexible User Validation Language for Time-Sharing Systems." AFIPS CONFERENCE PROCEEDINGS, Spring Joint Computer Conference, Vol. 34, 1969, pp. 665-671.

It is quite important to establish reasonable limits on the system resources available to users of a time-sharing system. For systems with 5,000 or more users, this task can get very complex. The article describes a user classification scheme which greatly simplifies resource allocation and security control for each user. A special purpose language is used for easy manipulation of large blocks of users as a group.

*(6320)*70*ad*cb*dg*el

McKeeman, W. M. "Data Protection by Self-Aware Computing Systems." Report Vol. 2, No. 6, Computer Evolution Project, Applied Science Department, University of California, Santa Cruz, California, June 1970.

*(6330)*72*ac*cd*dc*ga*ge*jf*x1

McLaughlin, Ed. "Set Guideline Revisions for EDP Fire Protection." ELECTRONIC NEWS, 5 June 1972, p. 43.

Incidents of sabotage, arson, and accidental fire damage to computers have caused the National Fire Protection Association to begin revising its standards for EDP equipment. New standards will call for a solid partition surrounding computer areas, which will be strong enough to withstand fire for an hour and a half. The association is also recommending the addition of Halon 1301, a freon material, as a means of extinguishing fires.

*(6340)*73*ab*bb*db

McLaughlin, R. A. "Equity Funding: Everyone is Pointing at the Computer." DATAMATION, June 1973, pp. 88-91.

*(6350)*70*ad*cb*da*ha*lb

McLellan, P. M. "A Survey of Privacy Considerations in Resource-Sharing Computer Systems." Masters Project, University of Western Ontario, May 1970.

*(6360)*62*aa*bb*cc*db*mc*nf

McNew, Bennie B.; and Prather, Charles L. FRAUD CONTROL FOR COMMERCIAL BANKS. Richard D. Irwin., 1962.

*(6370)*73*ab*ah*cc*da*nl*nm

"Measures to Protect Personnel Privacy Increase at State Level." COMMUNICATIONS OF THE ACM, January 1973, pp. 65-66.

*(6380)*71*ab*cb*cc*da*nm

Medak, G. M.; and Whisenand, P. M. "Security, Justice, and the Computer." DATAMATION, 15 June 1971, p. 24.

*(6390)*73*ae*ag*cb*da*eq*ng*x3

Mellen, G. E. "Cryptology, Computers, and Common Sense." AFIPS NATIONAL COMPUTER CONFERENCE PROCEEDINGS, Vol. 42, 1973, pp. 569-579.

This article is a good introduction to cryptography. It is only mildly technical and doesn't require a great deal of effort to understand. However, those completely unfamiliar with the subject and having a minimal mathematical education may find it desirable to first read a more basic article such as "Cryptographic Techniques for Computers" by Dennis Van Tassel.

First, several basic substitution and transposition cryptographic techniques are explained in detail. These techniques were all developed fifty or more years ago and are easily decipherable. The author then discusses Vernam cryptographic techniques and Friedman's "index of coincidence" which is extremely useful for breaking most Vernam ciphers. Algebraic cryptography and poly-dimensional transposition ciphers are also described. They make much greater use of computer processing capabilities than any of the preceding techniques. As one might suspect, they also offer considerably greater security in most cases. Theoretically unbreakable cryptographic techniques exist, but they are generally too expensive for most applications.

The author also presents a brief discussion on currently available commercial cipher systems. He describes a few limitations of existing systems and states what he believes are the best and worst systems commonly available. The last section of this paper presents a very good discussion of why nongovernment cryptographic users can expect, at most, a very limited effort by an enemy in deciphering their transmitted information. Several human behavior problems which can significantly reduce the secureness of a cryptographic system are presented throughout the paper.

*(6400)*73*ab*cb*cc*cd*dg*ff*fh*fl*fv*gg*kd*nf*ni*x3
Menkus, Belden. "Computer Security Needs a Common Sense Approach." ADMINISTRATIVE MANAGEMENT, March 1973, pp. 28-29.

Some aspects of computer threats have been exaggerated, and actions suggested to management for improving security have not always been realistic. The author presents what he believes is a more common sense approach to computer security. Some of his recommendations are: make the facility as inconspicuous as possible; strengthen physical access controls; review the facility's exposure to fire and water damage; provide sufficient emergency power generation capacity; assure alternative emergency computer facilities are truly compatible and have sufficient reserve processing cabability; copy essential master files onto duplicate tapes and store at a remote location; design input data editing routines to reject spurious information; design programs to selectively restrict user access to key file segments; maintain a log inaccessible to computer operators that records programs processed, files used, operator, user, and elapsed operating time; require full documentation of all production programs and modifications to them; give leased programs equal protection; assign computer operators in pairs; include intensive job completion condition checks; rotate work shifts and/or duties; and have procedures for destroying carbon paper, printer ribbons, and discarded printouts that might contain sensitive information. Most of the above changes will not be expensive, but failure to make these changes could prove costly.

*(6410)*71*ab*cc*dg*fk*fv
Mankus, Beldon. "Retention of Data . . . for the Long Term." DATAMATION, 15 September 1971, pp. 30-32.

*(6420)*71*ac*ai*bb*cc*db*hl*ia*if*kb*kd*mc*x1
Merritt, Michael. "DP Figures in Bank Loss of $128,000." COMPUTERWORLD, 3 February 1971, p. 1.

Five persons, including the bank's assistant vice-president in charge of computer systems and the senior computer operator, have been arrested in connection with the alleged embezzlement of $128,000 from the New Jersey National Bank. Money was transferred from infrequently used savings accounts to new accounts opened by the three embezzlers not employed by the bank. After the exchange, the new accounts were closed out. Customer statements of the altered savings accounts were removed and substituted with fraudulent ones before being mailed. The embezzlement was detected because conversion of the bank's computer to a new system disrupted normal operations and didn't give the embezzlers time to substitute fraudulent customer statements before they were mailed.

*(6430)*71*ac*ai*bb*bf*cb*cc*db*df*ep*fr*ie*jb*lb*mc*x2
Merritt, Michael. "System Sabotaged by Phone." COMPUTERWORLD, 15 December 1971, p. 1.

The extensive computer communications network of Metropolitan Life Insurance Company has been the victim of sabotage, allegedly by union members striking against Metroploitan's computer vendor, Honeywell. The striking workers are all involved in maintenance of Metropolitan's remote data stations. By telephoning a tape recording of the signals used by a central computer to poll these remote data stations, the saboteurs managed to prevent the printout of processed data in some twenty-five remote Metropolitan offices for over a month. No loss of data or physical damage occurred.

*(6440)*73*ae*ag*cb*da*eq*x2
Meyer, C. H. "Design Considerations for Cryptography." AFIPS NATIONAL COMPUTER CONFERENCE PROCEEDINGS, Vol 42, 1973, pp. 603-606.

One commonly publicized method (called the Vernam method) of encrypting data is to perform an "exclusive or" operation using the data and a long set of pseudorandom numbers generated by a linear shift register. The author shows that if a shift register of "N bits" is used, then only 2N-1 contiguous bits of the actual unciphered text need to be known in order to break the cipher. The location of these 2N-1 known bits in the text does not have to be known. In a few cases, knowledge of only 2N-1 bits will not break the cipher because division by zero in the deciphering process produces an indeterminate situation. However, knowledge of 2N+10 bits will assure a solution with a high probability. Varying the feedback switches of the shift register as a function of its output will make the effort to break the code more difficult, but knowledge of a limited sequence of bits will still enable the cipher to be broken.

For implementing good crypto schemes the author suggests use of several mathematical operations, one being nonlinear, in encrypting the data. A linear shift resister approach is equivalent to only one linear mathematical operation. A crypto system developed by Feisel, Notz, and Smith of IBM is presented as a good example of using multiple mathematical operations.

*(6450)*72*ab*cb*da*eq
Meyer, C. H.; and Tuchman, W. L. "Pseudorandom Codes Can Be Cracked." ELECTRONIC DESIGN, November 1972.

This article is similar to another article by Meyer entitled "Design Considerations for Cryptography."

*(6460)*67*ab*cc*ff
Miccio, J. V. "Use of Controls in EDP Accounting." FINANCIAL EXECUTIVE, August 1967, p. 50.

*(6470)*70*ab*cc*ff
Milko, E. M. "Auditing Through the Computer or Around?" MANAGEMENT ACCOUNTING, August 1970, pp. 45-48.

*(6480)*71*aa*cc*da*fd*fh*fj*fk*hd*ka*mb*nl*nm*nn*no*x3
Miller, Arthur R. THE ASSULT ON PRIVACY - COMPUTERS, DATA BANKS, AND DOSSIERS. University of Michigan Press, 1971, 333 pp.

This book, along with PRIVACY AND FREEDOM by Alan Westin, provides an authoritative and exhaustive treatment of computers and privacy. The author, a law professor, describes the expanding threats to individual privacy resulting from improvements in computer technology. Unless some positive action is taken we may be kept under constant surveillance with computer dossiers, and no one will be able to ever escape from his past. A new federal regulatory agency is proposed, because self-regulation has so far not proven successful in protecting an individual's privacy rights.

*(6490)*71*ae*cc*da*hd*ka*nl*nm*x2
Miller, Roger F. "Computers and Privacy: What Price Analytic Power?" PROCEEDINGS OF THE ACM, 1971, pp. 706-716.

Confidential data is extremely useful in social science research as well as in government administrative and private business. If the expansion of uses of confidential data is to sufficiently exceed the expansion of abuses, more than technical "know how" will be needed to prevent errors and buggings. Legislation is needed to provide essential standards for file maintenance and disclosure, and to provide for an individual to be informed as to what identifiable data about him is on file, where it is, and why.

Part 1 of this article gives an example of the use of confidential data of great practical business as well as public policy significance. Part 2 examines some basic issues and attempts to define some useful distinctions in order to put the twin problems of confidentiality and usability of data in perspective. Part 3 contains a substantive discussion on methods of protecting the privacy of individuals without seriously impairing the usability of their data.

*(6500)*67*ad*bc*da*df*eb
Miller, Roger F. "Confidentiality and Usability of Complex Data Bases." No. 6702, Systems Formulation and Methodology Workshop, Social Systems Research Institute, University of Wisconsin, May 1967.

*(6510)*68*ab*cc*da*fh*ka*no*nl*nm*x2
Miller, Richard I. "Computers and the Law of Privacy." DATAMATION, September 1968, pp. 49-55.

The author looks at some dangers to personal privacy which are a result of new inexpensive computers. A good description is given on the evolution of the concept of privacy in American case and statutory law. Proposals are then made for extending the individual's legal right to privacy. Individuals should be given notice of data collected about them and should have the right to verify that data. Government purchases of EDP equipment for storing personal data should need high administrative approval. Persons and firms engaged in collecting personal information should be liable to injured parties if that information is false or used for defamatory purposes.

*(6520)*70*ab*cb*cc*cd*dg*gg
Mintz, Harold K. "Safeguard Computer Information." SOFTWARE AGE, May 1970, pp. 23-25.

Categories of safeguards are reviewed and suggestions are made for protecting computerized data.

*(6530)*67*ae*cb*da*ep
Mitchell, J. F. "Communications Efficiency and Security." 74th ANNUAL CONFERENCE IACP, Kansas City, September 1967.

*(6540)*70*ad*cb*ed
Mittwede, William C. "Computer Operating Systems Capabilities: A Source Selection and Analysis Aid." ESD-TR-71-74, Contre Corporation, November 1970.

*(6550)*70*ad*ae*ag*cb*cc*db*dd*ec*ei*eo*fs*gh*hd*hu*id *ie*nc*ng*nk*x4
Molho, Lee M. "Hardware Aspects of Secure Computing." SP-3453, Systems Development Corporation, 2500 Colorado Avenue, Santa Monica, California 90406, December 1969; or AFIPS CONFERENCE PROCEEDINGS, Spring Joint Computer Conference, Vol 36, 1970, pp. 135-141.

This article is essentially a condensed version of a seventy page report by Molho entitled "Hardware Reliability Study". The report's annotation should be read to learn the contents of this article. The following is a brief outline of the major topics covered in this article and the report: weak points for logic failure, circumventing logic failure, subversion techniques, countermeasures to subversion, defeat of countermeasures, administrative policy, fail-secure versus fail-soft hardware, failure detection by faulty system operation, data checking and control signal errors, and conclusions.

*(6560)*69*ad*cb*cc*db*dd*ec*ei*eo*fs*gh*hd*hu*id*ie*nc *ng*nk*x4
Molho, Lee M. "Hardware Reliability Study." N-L-24276/126/00, Systems Development Corporation, 2500 Colorado Avenue, Santa Monica, California 90406, December 1969, 70 pp.

This paper is a detailed study of the hardware aspects of problem/supervisor state control and storage protection in the IBM 360/50 system. It should definately be read by those concerned with implementing hardware protection mechanisms in computers. The author traced the internal operations of the IBM 360 microprograms, and discovered approximately 100 single-failure hazards. At each point in a microprogram's operation the author asked, "If this element fails, will the hardware required for secure computing go dead without giving an alarm?" The author also took the position of a would-be system subverter looking for the easiest and best ways of using the IBM 360/50 to steal files from unsuspecting users.

Advantages and disadvantages of several different reliability test approaches are discussed in some detail. The author believes that security problems are mostly present in logic controls and not so much in data paths which most manufacturers load with error detecting hardware. He states that software tests can detect almost all hardware problems, and would eliminate 85% of the single hardware failures in SDC's ADEPT-50 system which is implemented on an IBM 360/50. The increase in overhead would be only .015% if the tests were implemented in microprograms. The author also feels that "fail-soft" systems endanger security. Interdependence of system components can be useful because hardware failures will be quickly detected by the resulting faulty system operation. An overabundance of "inhibit"-type asychronous logic is a good indicator of sloppy design or bad design coordination. The effort required for hardware certification of a system is briefly described. However, real-time testing appears to be a more reliable and inexpensive alternative. A condensed version of this report can be found in the 1970 Spring Joint Computer Conference proceedings under the title "Hardware Aspects of Secure Computing".

*(6570)*68*ab*cb*da*dd*em*eo*ep*lb*x2

Moloney, Robert F. "New Generation EDP Control Considerations." MANAGEMENT SERVICES, March 1968, pp. 15-22.

The purpose of this article is to discuss some error and access control requirements which systems analysts, programmers, and auditors should be aware of in designing any real-time system. These controls are primarily concerned with system hardware errors, system software errors, program errors, and remote terminal access. Some of the specific controls discussed in this article are: on-line controls (message identification handling procedures, message transmission verification, rerouting procedures, parity checks); data protection controls (preventing concurrent undating, passwords, series of passwords, authority lists or tables, boundary registers); diagnostic controls; emergency procedures (re-execute faulty instructions, restart faulty programs, transfer problems to an exception routine, initiate switchover, initiate closedown, halt); and graceful degradation (checkpoint/restart procedures). Although this article is somewhat out of date, its discussion on computer error control can be quite informative to those not very familiar with the subject.

*(6580)*68*aa*cc*cd*dc*jb*jf

Monbousse, R. M. INDUSTRIAL SECURITY FOR STRIKES, RIOTS AND DISASTERS. C. C. Thomas Publishers, 1968.

*(6590)*69*ab*cc*da*db*dd*de*el*fa*fc*ff*fi*fj*fp*fx*kb
*kd*nf*ni*x3

Moore, Michael R. "EDP Audits: A Systems Approach." THE INTERNAL AUDITOR, May 1969, pp. 9-25.

The purpose of this article is to show that a systems approach is desirable in the auditing of computer-based information and control systems. The basic premise that sound management objectives and sound audit objectives are substantially parallel is examined. Evaluation criteria and techniques are described which may be used to determine that an EDP system is soundly conceived and designed. The following is a rough outline of the criteria and techniques described: organization of EDP groups (independence, authority, and responsibility); programming (documentation, testing, modifications); control over day-to-day operations; and hardware and software (only superfically discussed). Testing techniques required to provide assurance that the system is, in fact, functioning as designed include: a test deck to validate new programs; error classification; and program modification control. The use of the computer in EDP auditing was not discussed because the author felt the subject was too large to be adequately covered in this article.

Although this article was written in 1969, it is still quite valuable, especially to those who are not familiar with an auditor's responsibilities in assuring that adequate data security exists. The comprehensive and detailed lists of evaluation and testing techniques should be quite useful for persons concerned with implementing or updating a data security program.

*(6600)*68*ab*cc*cd*de*df*hv

Moore, Michael R. "Pitfalls in Planning an EDP Installation." MANAGEMENT SERVICES, September 1968, pp. 25-32.

*(6610)*70*ab*bc*cc*dc*fw*jf

Moore, William C. "Riot Plan Worked." THE OFFICE, August 1970.

This article describes a riot plan which was tested during an actual riot.

*(6620)*70*ac*ai*cb*cc*cd*da*gg*jc

"More Work Needed to Solve Problem of Data Security." COMPUTERWORLD, 27 May 1970, p. 6.

Computerization of data make it more portable and thus easier to steal. Some data protection safeguards are discussed.

*(6630)*71*ab*cc*df*dg*fy*mc*x2

Morran, J. R. "How Does Your Bank Stack Up In Insurance Against EDP Losses?" BANKING, April 1971, p. 36.

The author discusses the coverage offered by several different types of bank and EDP insurance. The types of insurance discussed are: bankers blanket bond; bankers data processing transit and extra expense insurance; cash letter insurance; data processing errors and omissions insurance; and electronic data processing policies which usually offer coverage for equipment, media, extra expenses, valuable papers and records, and business interruption. This article should be quite useful to banks, but not other types of businesses.

*(6640)*73*ab*ah*cb
Morris, J. H. Jr. "Protection in Programming Languages." COMMUNICATIONS OF THE ACM, January 1973, pp. 15-21.

*(6650)*71*ac*ai*cc*fc*ff*kd*x1
Morton, Thomas J. "Auditor Must Be Involved in DP, ACM Speaker Says." COMPUTERWORLD, 24 February 1971, p. 6.

This short article summarizes a speech made by Robert W. London, of Brandon Applied Systems, before a group of auditors, financial business executives, and EDP professionals at an Association for Computing Machinery professional development seminar. Mr. London stressed that, "The auditor should play an ever increasing role in data processing from the earliest stages of system development right up through post installation evaluation."

*(6660)*70*ac*ai*bc*cd*dc*jf*kg*mh*mj
Morton, Thomas J. "Bomb Demolishes Army Computer Complex." COMPUTERWORLD, 2 September 1970, p. 1.

The bombing of the Army Mathematics Research Center at the University of Wisconsin is the subject of this article. One research employee was killed. Losses amounted to $1.5 million for the computer complex, $5 million for the building, and 1.3 million manhours of data.

*(6670)*70*ac*ai*bc*cd*dc*jg
Morton, Thomas J. "DP Centers Dig Out in Hurricane's Wake." COMPUTERWORLD, 19 August 1970.

This article describes damage done to Corpus Christi, Texas computer installations by hurricane Celia.

*(6680)*70*ac*ai*bc*cd*dc*jg
Morton, Thomas J. "DP Centers Feel the Brunt of Hurricane's Fury." COMPUTERWORLD, 12 August 1970, p. 1.

This article describes damage done to Corpus Christi, Texas computer installations by hurricane Celia.

*(6690)*70*ac*ai*ba*cb*da*hc*ii*lb
Morton, Thomas J. "FBI Accuses Youth of Tapping T/S Service, Copying Data Files." COMPUTERWORLD, 19 July 1970.

*(6700)*70*ac*ai*ba*cc*da*hc*ia*kb*kf*nj
Morton, Thomas J. "Firms Sue in Mailing List Theft." COMPUTERWORLD, 8 July 1970, p. 1.

Three Encyclopedia Britannica computer operators stole and sold the company's mailing list valued at approximately $3,000,000.

*(6710)*71*ac*ai*ba*bb*cc*da*db*hk*kb*kd*mi*x2
Morton, Thomas J. "Manipulation of Penn Central Computers Cited in Boxcar Theft." COMPUTERWORLD, 31 March 1971, p. 1.

FBI agents recently located 217 missing Penn Central boxcars on the tracks and in the yards of the LaSalle and Bureau County Railroad. Peter Vairce, a U.S. attorney, hinted that there had to be some manipulation of the Penn Central computers to obtain output necessary to allow the boxcars to be sent to the LaSalle and Bureau County tracks. Investigators feel that someone on the inside of Penn Central may have been modifying the input data to record the cars as scrapped or wrecked. They also suspect that organized crime is taking part in boxcar thefts. A Federal Grand Jury is beginning an investigation of the 2,800 boxcars missing throughout the country.

*(6720)*71*ac*ai*cb*da*ep*je*jf*x1
Morton, Thomas J. "Prevention of Public Access 'Key' to DP Center Security." COMPUTERWORLD, 9 June 1971, p. 2.

This short article briefly summarizes some comments made by speakers at the International Security Conference in Chicago. A few simple recommendations are given on data transmission security and cryptography. It was also said that a ten by two inch pipe bomb could be made with $10 of ingredients readily available in the commercial market.

*(6730)*70*ac*ai*cc*de*fd*ne
Morton, Thomas J. "Psychologist Views 'Insecurity' at DP Centers." COMPUTERWORLD, 22 July 1970.

Dr. Robert W. Varmin, a behaviorist and psychological consultant, discusses several reasons for computer security apathy. Computer personnel and computer users usually do not grasp the value of the information they are handling. They are usually unaware of many potential threats to their data.

*(6740)*69*ae*cb*dg*ed*el*gh*lb
Motobayashi, S.; Masuda, T.; and Takahashi, N. "The Hitac 5020 Time-Sharing System." PROCEEDINGS OF THE ACM'S 24TH NATIONAL CONFERENCE, 1969, pp. 419-429.

*(6750)*71*ac*ai*bd*cc*dd*hr*me

"Motorist Gets Stung by Small Bugs." COMPUTERWORLD, 13 January 1971, p. 6.

Errors in a motor vehicle department's computerized information system are described.

*(6760)*70*ab*cc*dd*de*ff*fg*hp*hr

Mroz, Gene P. "Computer 'Bug' Control." JOURNAL OF DATA MANAGEMENT, Jnauary 1970.

The author believes that internal auditors must be very familiar with the internal workings of a computer.

*(6770)*71*ab*cc*ff

Mullarkey, J. F. "Technical Proficiency for Auditing Computer Processed Accounting Records." JOURNAL OF ACCOUNTANCY, October 1971.

*(6780)*71*ad*al*cb*ed*gh*lb

"The Multiplexed Information and Computing Service: Programmer's Manual." Project MAC, MIT, Cambridge, Massachusetts 02139, Preliminary Edition, 1971.

This article describes file access controls in MIT's MULTICS system. Access control is associated with branches of a tree, not with links between branches as in MIT's CTSS system. A user's access rights are evaluated each time a segment is made known to him. The access modes are read, write, execute, append, and combinations thereof. They may be assigned on the basis of users and projects. MULTICS provides a ring structure for protection which is a generalization of the "user state"/"supervisor state" idea. Any attempt to access data from an insufficiently privileged ring must take place through a "gate" specified by the data owner via a program of his own choosing.

*(6790)*72*ab*ba*be*cc*da*de*fp*nf

Murphey, W. E.; and Olson, D. V. "Controlling Access to Large Tape Files." DATA PROCESSING MAGAZINE, Spring 1972, pp. 4-6.

A system is described for preventing the physical loss of computer tapes through rigid handling controls. The Minnesota Hospital Service Association developed the system after incurring large expenses from frequent tape losses.

*(6800)*72*ae*cb*ed*el*gh*hd*ka*lb*mg

Nakanishi, K.; and Hsiao, David. "A Cardiac Catheterization Information System - An Application of an Advanced Data Management Facility." PROCEEDINGS OF COMPUTER 72, IEEE Computer Society, June 1972.

This article describes a medical information system developed for the Cardiac Catheterization Laboratory of the University of Pennsylvania. It also discusses the Extended Data Management Facility that supports the medical information system.

*(6810)*72*ae*ag*ca*dg*ee*ei*nb*ng*x3

Needham, R. M. "Protection Systems and Protection Implementations." AFIPS CONFERENCE PROCEEDINGS, Fall Joint Computer Conference, Vol. 41, 1972, pp. 571-578.

This paper discusses different systems for protection of information in the central memory of a computer, and describes the potentialities and limitations of a varity of implementation approaches. It is based on a current protection system project at the University of Cambridge Computer Laboratory in Cambridge, England. A system which is being developed to the point of hardware implementation is also discussed. This paper should be valuable to those investigating or designing main memory protection schemes. However, the non-technical reader will likely find it quite confusing.

The author first defines several concepts which enable easier discussion and understanding of protection systems and protection implementation. A "segment" is a set of words whose addresses are contiguous in a virtual address space, and whose protection status is at all times the same. A "protection regime" is a list of those segments accessible to a process at a particular time, together with notes as to the kind of access permitted. A "capability" defines the physical position and size of a segment, and the access mode allowed. The paper is concerned with protection systems within a process, but not how or where a process obtains its resources.

After defining the above terms, the author focuses on the implementation of protection as the implementation of selection functions among capabilities. There are two apparent ways this can be accomplished. One way is to proceed by means of lock and key systems in which any segment has associated with it a lock. A process is associated with a certain key at any particular time and access is permitted to a segment only if the current key fits the lock of that segment. The other way to proceed is to use indirection tables as the means of selection of accessible segments. Addressing is much more bound up with the protection implementation when using indirection tables. The author concludes that powerful lock and key systems are too difficult in practice because of the allocation problem, and that lock and key systems in which one can face the allocation problem are not powerful enough. He then discusses in some detail a system based on use of indirection tables.

*(6820)*70*ab*bc*cd*dc*ga*gf*jf*mj*x1
Nelson, F. B. "Campus Computers - Target for Militants and Almost Anyone Else." DATAMATION, 15 October 1970, p. 37.

The author states that almost all colleges and universities have inadequate physical security to protect their computers from student saboteurs. He recommends computers be located off-campus and accessed through remote terminals.

*(6830)*70*ab*cd*dd*gb*gc*hu*jg*x3
Neumann, E. W.; and Riley, R. "Protecting the Computer In a Process Environment." CONTROL ENGINEERING, September 1970, pp. 72-75.

Massive investments in process plants that rely more and more on computer control to competitively serve their markets make shutdown caused by any form of failure expensive and often intolerable. Moreover, methods applied in the past to protect simpler process instrumentation are often not adequate for today's computer systems. The authors pass along their expertise in contaminated environments, pointing up practical ways to protect the computer in a variety of industrial applications. First, typical concentrations and potential dangers of various types of airborne pollution are discussed. Then the following environmental considerations are briefly examined: relative humidity, ambient temperature, room pressure, particle filters, gas filters, room maintenance, records and indicators, and facility support maintenance.

*(6840)*71*ab*ba*bb*bc*cc*da*db*dc*fb*fs*ft*hb*hg*hj*if
*kb*kd*mc*x2
Neville, Haig G. "Computer Capers Herald New Crime Wave of Embezzlement." THE NATIONAL UNDERWRITER: Property Edition, 20 August 1971, p. 1.

The author attempts to persuade the reader that security against embezzlement is dangerously lacking in most organizations. Most of the article is devoted to describing and commenting on ten recent cases of computer related fraud. Each case shared a remarkable similarity of circumstances in which the perpetrators, not management, had control of the computerized accounting system. The perpetrators almost always occupied a position of trust in which their loyalty was unquestioned. The author recommends that management reexamine its attitude toward employee dishonesty, and recognize that providing an opportunity to steal contributes to the crime.

*(6850)*69*ab*bc*cc*dc*fv*fw
Neville, Haig G. Letter to the Editor. HARVARD BUSINESS REVIEW, May 1969.

Some examples are given on why planned backup sites are often inadequate.

*(6860)*64*ab*cc*dd*de*fy
Neville, Haig G. "You Can Insure against Errors and Omissions in Data Processing." THE OFFICE, October 1964.

*(6870)*67*ab*cb*hd*ka*me*nm
"New Haven Designs City Data Bank." EDP WEEKLY, 15 May 1967, p. 5.

New Haven, Connecticut is designing an urban management information system that will store data on the city's inhabitants, its traffic intersections, buildings, crimes, population shifts, and welfare system. Access to this data will be made available to city officials by way of remote terminals. Some of the expected benefits of this system are improved planning and reduced administrative delays. The personal data will be protected by using frequently changed passwords. This protection scheme is viewed to be at least more safe than the present system of storing files in unlocked cabinets. None of New Haven's citizens have voiced any serious objections to this new computerized system.

*(6880)*70*ab*ba*bc*cd*da*dc*gf*hc*ia*ie*jf*mc*x1
"New Threats and New Defenses." BANKING, August 1970, pp. 69-70.

The author tries to convince the reader that most computer users, particularly banks, have very inadequate safeguards to protect against sabotage and vandalism. Actual and hypothetical examples are given of computer crimes that could be performed by unhappy employees, campus dissidents, or just plain "ding-a-lings". The example of tape vulnerability to magnets is greatly exaggerated. This article would be typical of those described by Mel Mandell in a NEW TORK TIMES article entitled "Computer Scare Talk: Sabotage Fears of 'Experts' Discounted".

*(6890)*69*ab*cc*fc*ff*mc
Newcomb, Lawrence. "The Bank Auditor's Role in EDP Design." BANKERS MAGAZINE, 3 November 1969, pp. 61-66.

*(6900)*72*ab*cc*fb
Newlin, C. "The Changing World of the Data Processing Administrator." DATA MANAGEMENT, February 1972, p. 38.

*(6910)*64*ab*cc*ff
Newman, M. S. "Internal Control and Data Processing." FINANCIAL EXECUTIVE, November 1964, p. 42.

*(6920)*70*ab*cc*ff
Nigra, A. L. "Auditing Acquisitions of Data Processing Equipment." THE INTERNAL AUDITOR, January 1970.

*(6930)*71*ac*ai*cb*da*es*md*x1
"No Basis for Assuming Software Can Ensure Confidential Systems." COMPUTERWORLD, 27 November 1971, p. 4.

This short article briefly summarizes some statements made by Sol Dolleck of the Census Bureau before the Fall Joint Computer Conference. Dolleck believes that there is no basis for assuming that an all-powerful software system can be designed that could take care of the problems of a national statistical data center if one were to be created. The problems of indirect disclosure and priorities have not yet been solved.

*(6940)*70*ac*ai*cb*da*eq
"'No Great Feat to Wiretap' Says Canadian Computer Professor." COMPUTERWORLD, 25 November 1970.

John M. Carroll describes a cryptographic system for protecting data privacy.

*(6950)*71*ad*ak*cb*eq*gh
Notz, W. A.; and Smith, J. L. "An Experimental Application of Cryptography to a Remotely Accessed Data System." RC-3508, IBM Corporation, White Plains, New York, 18 August 1971.

A hardware cryptographic device is described which was experimentally attached to an IBM 360/67 time-sharing computer. For more information see "The Design of Lucifer, A Cryptographic Device for Data Communication" by J. L. Smith.

*(6960)*69*ac*ai*bb*cc*db*fs*ia*mf
"Numbers Racket Used Data Cards." COMPUTERWORLD, 18 June 1969.

A computer operator used 80-column computer cards for operating a numbers racket.

*(6970)*68*ab*cb*cc*cd*dg*kd*mc*x1
O'Brien, James A. "The Computer and Banking's Protection." BANKING, September 1968, pp. 115-118.

The article explains how the introduction of computer systems has resulted in extensive changes in the susceptibility of banks to fraud, errors, and physical damage. It also shows how bank insurance and bank auditing have been affected. However, the article is largely obsolete and most of the ideas presented are now widely known.

*(6980)71*ae*ag*cb*da*db*dc*eb
O'Connell, M. L. "A File Organization Using Multiple Keys." AFIPS CONFERENCE PROCEEDINGS, Spring Joint Computer Conference, Vol. 38, 1971, pp. 539-544.

*(6990)*68*ac*bb*db
"On Computer Fraud." WALL STREET JOURNAL, 5 April 1968.

*(7000)*72*aa*al*cb*dg*ed*ei*el*gh*lb*ng
Oranick, Elliot I. THE MULTICS SYSTEM: AN EXAMINATION OF ITS STRUCTURE." MIT Press, 28 Carleton Street, Cambridge, Massachusetts 02139, 1972.

*(7010)*70*ab*cd*df*gd*jh
Ortiz, J. V. "Constant-Power System for Computers." ELECTRICAL CONSTRUCTION AND MAINTENANCE, January 1970, pp. 96-97.

A power backup system is described which makes use of kinetic energy from a flywheel.

*(7020)*71*ad*ak*cb*ea*ed*ef*ei*el*en*fd*gh*lb*nb*nc*nf*x4
"OS/MVT With Resource Security: General Information and Planning Manual." GH20-1058-0, IBM Corporation, White Plains, New York, December 1971.

The Resource Security System was initially designed for the World Wide Military Command and Control System and is largely based on 1968 military specifications. This manual is one of a set of four that describe the Resource Security features to OS/MVT. The other three manuals are listed immediately following this entry. The system is designed to provide control over users of the system, and the programs, data sets, and terminals to which they may desire access. The programs, data sets, terminals, and users are defined by a security officer as possessing certain characteristics and capabilities such as security level and access criteria. Characteristics are referred to as security profiles, and the interaction of these profiles determines the user's access to system resources. During OS/MVT operation the system dynamically accesses profiles, and on the basis of their comparison either allows access or terminates a user's job and logs the circumstances surrounding the attempted unauthorized access. The system is modular in design and provides numerous implementation options. The minimum security options will degrade OS/MVT Release 18 system performance 1% to 12%, and the maximum security options will degrade Release 18 performance 15% to 31%.

The following is a brief outline of this manual: basic concepts; systems features; security officer commands; identification and authorization of resources; system statistics; system description; machine configuration needed; performance; installation's responsibilities; planning considerations; selection of options; procedures for establishing security profiles and authorizations; and system design (appendix).

*(7030)*71*ad*ak*cb*ed*ef*gh*lb*nf*x2
"OS/MVT With Resource Security: Installation and System Programmer's Guide." GH20-1021-0, IBM Corporation, White Plains, New York, December 1971.

The Resource Security System is designed to provide security control over the users of a OS/MVT system and the programs, data sets, and terminals to which they may desire access. See the entry entitled "OS/MVT With Resource Security: General Information and Planning Manual" for more information.

*(7040)*71*ad*ak*cb*ed*ef*fq*gh*lb*x2
"OS/MVT With Resource Security: Security Officer's Guide." GH20-1057-0, IBM Corporation, White Plains, New York, December 1971.

The Resource Security System is designed to provide security control over the users of a OS/MVT system and the programs, data sets, and terminals to which they may desire access. See the entry entitled "OS/MVT With Resource Security: General Information and Planning Manual" for more information.

*(7050)*72*ad*ak*cb*fd*ea*ed*ef*ei*el*en*gh*lb*nb*nc*nf
*x3
"OS/MVT With Resource Security: System Description Manual." GH20-0967-0, IBM Corporation, White Plains, New York, March 1972.

The Resource Security System is designed to provide security control over the users of a OS/MVT system and the programs, data sets, and terminals to which they may desire access. See the entry entitled "OS/MVT With Resource Security: General Information and Planning Manual" for more information.

*(7060)*70*ac*bb*cc*db*md
Ottenburg, Miriam. "Electronic Tax Fraud Investigated at

IRS." THE EVENING STAR, Washington D.C., 24 June 1970, p. A-1.

Two examples of computer related tax fraud are given.

*(7070)*70*ab*cc*ff*fm
Otto, J. W. "Operational Auditing Applied to Data Processing Facilities." THE INTERNAL AUDITOR, May 1970.

*(7080)*71*ac*ai*bf*cd*df*jh
"Outages Rates a Leading Cause." COMPUTERWORLD, 12 May 1971, p. 2.

*(7090)*71*ae*ca*da*fe*ee
Owens, Richard C. Jr. "Evaluation of Access Authorization Characteristics of Derived Data Sets." ACM Special Interest Group on File Description and Translation (SIGFIDET) Workshop, 1971, pp. 263-278.

*(7100)*71*ad*al*ca*cd*ea*ed*ee*ef*fe*lb*ng*nn*x4
Owens, Richard C. Jr. "Primary Access Control in Large-Scale Time-Shared Decision Systems." Master's Thesis, MAC TR-89, MIT, Cambridge, Massachusetts 02139; or AD-728 036, National Technical Information Service, Springfield, Virginia 22151, July 1971, 93 pp.

Four primary dimensions of the access control problem are identified. They are: the physical level at which to apply control (files, records, individual data items); the fineness of distinction applied to the term "access" (yes or no, or more refined distinctions like read, write, append, execute); the meaning of the term "user identification" (names, passwords, signature recognition, etc.); and the degree of sophistication employed in automatically assigning restrictions to newly created data files (from no restrictions to a completely automated classification method which determines the sensitivity of data in a new file by knowing the access characteristics of the data input into this file). Within the context of MIT's Project MAC Advanced Interactive Management System (MacAIMS), the detailed design of an "interim access control system" is presented which takes positions along these four dimensions. The choice of positions along these dimensions determines the power and capabilities of the access control scheme. The proposed interim system can be easily modified along both the second and third dimensions of access control. The method of access control proposed is more general than that in any system in current use. The concepts of the "owner" of information, the "originator" of information, and the persons who may change access control restrictions to information can all be separated.

The author reviews all well known existing and proposed access control systems and concludes that none are adequate. He does like Hoffman's formulary model but is not convinced that the user would be sophisticated enough to write his own formularies. The MULTICS system is described, and Owens concludes that it does not have adequate access controls. Owens also concludes that Weissman's ADEPT-50 scheme of automatic classification of new files is too restrictive for non-military use. However, the proposed "interim system" does not solve all of the access control problems either. Several limitations are described and suggestions for further study are proposed. The author concludes that development of a system that conveniently and completely protects its user's rights will be a very difficult task.

*(7110)*70*ad*cb*dg*ed*ei*ej*el*en*gh*mh
"PACER Multi-Level Security Program Design Specifications." PRC-WP0115, Planning Research Corporation, November 1970.
This report describes the design specifications for PACER, a military intelligence analysis system which processes highly classified information and runs on a Honeywell 6000 series computer.

*(7120)*70*ac*ai*bd*be*cc*dd*de*nj
"Pacific Telephone Sued for Erroneous Billing." COMPUTERWORLD, 30 September 1970.
A California lawyer is suing Pacific Telephone Company for $7,000,000 for erroneous billing and loss of service when he refused to pay the incorrect bills.

*(7130)*69*ab*cc*dg*ff
Palmer, R. R.; and Duma, W. J. "Auditing with Computers." BANKER'S MONTHLY MAGAZINE, 15 January 1969.
The authors review several approaches to auditing and conclude that auditing must be done with the computer.

*(7140)*72*ab*ba*bb*cc*da*db*dc*ng*no*x2
Parker, Donn B. "The Antisocial Use of Computers." COMPUTERS AND AUTOMATION, August 1972, p. 22.
The author briefly discusses each of the following: three criminal cases; a few factors leading to criminal behavior; security measures being based on the value of what is being protected with little knowledge of real threats; misconceptions and lack of knowledge about computers by law enforcement agencies and the courts; and the current magnitude of computer related crime. Some interesting statistics were given on computer crime. Since 1966 less than eighty computer-related crimes have been authenticated although many more have been reported. IBM receives about three hundred reports per month of at least unethical acts occurring among its customer installations. The average financial loss of twenty authenticated cases recently studied was $670,000 per case with a range of $1,300 to $1,750,000. The author makes six specific predictions which he feels should be the goal of future exploratory research. The possible impact of these six predicted research goals on computer users, computer and software manufacturers, laws and Congress, and professional societies is briefly explained. However, three of these predictions appear to be questionable and the other three don't suggest anything unexpected.

*(7150)*72*ae*bg*cb*cc*cd*dg*ha*ja
Parker, Donn B. "The Nature of Computer Related Crime." INTERNATIONAL CONFERENCE ON COMPUTER COMMUNICATION

PROCEEDINGS, 1972, pp. 121-126.

A method of providing protection by means of threat analysis is presented. A brief history is given on computer-related crime. Likely future crime developments are also briefly discussed.

*(7160)*73*ac*ai*ba*cb*cd*da*hb*hd*jd*je*mh*x2

"Passive Entry 'Good Way' to Obtain Sensitive Data." COMPUTERWORLD, 16 May 1973, p. 4.

Commander Jan Prokop, director of the Navy's computer selection office, stated that wiretapping, electromagnetic pickup, and hidden transmitters can be good techniques for obtaining sensitive computerized information. He cited a test case in the Pentagon where a CRT was allegedly being read from its radiation signals by an unauthorized user several rooms away from the computer. He also claimed that a hidden wireless transmitter had been found inside a CPU at a security agency.

*(7170)*70*ad*ak*cb*da*db*dc*ed

Patrick, D. K. "File-Organization Security in a Real-Time System." IBM TECHNICAL DISCLOSURE BULLETIN, Vol. 13, No. 4, September 1970, pp. 1030-1031.

File security is achieved by matching all of the user's available processing options against his set of authorizations. Only if the match finds no conflicting demands will the user be allowed to proceed.

*(7180)*70*ab*bb*cb*cc*db*ff*fi*id*kb*mk*nf*nk*x2

Patrick, Robert L.; and Dahl, Albrey. "Voting Systems: Los Angeles Doesn't Have One." DATAMATION, May 1970, pp. 81-82.

A small team of research scientists served as "poll watchers" during a recent Los Angeles election. After viewing the extremely careless manner in which the ballots were processed and becoming aware of the fact that the IBM Votomatic system has absolutely no safeguards to protect against any type of fraud, they carefully and quietly raised the possibility of vote tampering. This lead to the formation of a blue ribbon investigation committee which unfortunately lacked sufficient computer knowledge. The committee's conclusions supported use of the Votomatic system in spite of several extremely serious Votomatic flaws pointed out in this article. Perhaps the committee's recommendations were the only politically practical ones since Los Angeles had just bought several million dollars worth of Votomatic equipment. The authors conclude by offering several recommendations for improving the integrity of a computerized vote-count system.

*(7190)*69*ab*cb*cc*fc*ff*nf

Pauley, Charles. "Audit Responsibilities in the Design of Computerized Systems." THE INTERNAL AUDITOR, July 1969.

The author explains why auditors must be involved in the design of computer systems.

*(7200)*69*ad*cb*ed*gh*lb*x1

"PDP-10 Programmer's Reference Manual: Time-Sharing Monitors." DEC-T9-MTZA-D, Digital Equipment Corporation, Maynard, Massachusetts, August 1969.

This manual describes one of DEC's efforts to provide file access control. The term "user" is separated into three categories: the file owner, persons on the same project as the owner, and everyone else. Access to a file may be restricted for each of these three groups by read protection, write protection, and protection by having the capability to change access control information. It is also possible to name files such that the monitor knows they are procedures. This can be used to enforce "execute" access control.

*(7210)*72*ae*cb*cc*cd*dg*ea*ec*ed*ei*ej*el*ep*fs*gf*gg *hd*ht*hu*hw*jd*nh*ni*nn*x2

Peck, Paul L. "Achieving Security and Privacy of Information in an On-Line Data Processing Environment." PROCEEDINGS OF ONLINE 72: International Conference on Online Interactive Computing, Online Computing Systems Ltd., Uxbridge, Middlesex, England, September 1972, pp. 107-129.

This paper is identical to another article by Mr. Peck entitled "Data Processing Safeguards" which was printed in the JOURNAL OF SYSTEMS MANAGEMENT.

*(7220)*72*ab*cb*cc*cd*dg*ea*ec*ed*ei*ej*el*ep*fs*gf*gg *hd*ht*hu*hw*jd*nh*ni*nn*x2

Peck, Paul L. "Data Processing Safeguards." JOURNAL OF SYSTEMS MANAGEMENT, October 1972, pp. 11-17.

The author briefly discusses five general threats to the integrity of computer information. They are: hardware and software malfunctions; unauthorized user attempts to examine, modify, or obtain information; unauthorized computer center personnel actions; insecure communications and electronic emanations; and negligence. Two EDP environments, a basic environment and a sophisticated environment, are then explained and twenty-five safeguards are discussed in the context of these two environments. The applicability of each of these twenty-five safeguards to the five general threat categories is shown in a summary table. The safeguards were also grouped into five functional areas: access controls, internal system controls, data transmission controls, violation controls, and other controls.

The remaining three-fourths of this article is devoted to describing in some detail the mechanization and capabilities of the following twenty-five safeguards: physical access control; user system entrance control; hardware and software terminal entrance and exit control; hardware protection of data in main memory; software protection of data in bulk storage; interrupt processing software; isolating parts of the executive system in read-only memory; restricting users to higher level languages; software management of hardware resources; utilization of secure communication techniques; electromagnetic shielding of the computer center; microprogrammed hardware checks; software integrity checks; hardware error data checks; operating procedures; software reaction to and procedures for responding to potential and actual security violations; software determination and marking of sensitive output; record keeping; safe and vault protection; personnel security programs; and procedures for certification and recertification.

*(7230)*72*ae*cb*cc*cd*dg*ea*ec*ed*ei*ej*el*ep*fs*gf*gg *hd*ht*hu*hw*jd*nh*ni*nn*x2
Peck, Paul L. "Protecting Corporate Computer Information." IDEAS FOR MANAGEMENT: Proceedings of the ASM International Systems Meeting, 1972, pp. 30-40.

This article is identical to another article by Mr. Peck entitled "Data Processing Safeguards" which was printed in the JOURNAL OF SYSTEMS MANAGEMENT.

*(7240)*71*ad*cb*cc*cd*dg*ea*ec*ed*ei*ej*el*ep*fs*gf*gg *hd*ht*hu*hw*jd*nh*ni*nn*x2
Peck, Paul L. "Survey of Applicable Safeguards for Insuring the Integrity of Information in the Data Processing Environment." AD-726 571, National Technical Information Service, Springfield, Virginia 22151, June 1971, 32 pp.

This paper is identical to another article by Mr. Peck entitled "Data Processing Safeguards" which was printed in the JOURNAL OF SYSTEMS MANAGEMENT.

*(7250)*71*ab*bc*cc*cd*dc*jf
Perham, John. "The Computer - A Target." DUN'S REVIEW, January 1971, p. 34.

*(7260)*71*ab*cc*cd*dc*fs*fu
"Personal Protection Urged." DATA PROCESSING MAGAZINE, April 1971.

*(7270)*67*ae*ag*cb*cc*ec*ed*ei*el*en*hd*kb*mh*x2
Peters, Bernard. "Security Considerations in a Multi-Programmed Computer System." AFIPS CONFERENCE PROCEEDINGS, Spring Joint Computer Conference, Vol 30,

1967, pp. 283-286.

The principles set forth in this paper have been generalized from the specific development of a specific military system which dealt with multiple levels of classified information. To obtain the security level which software can make possible, the following principles must be followed: the security monitor must be approved by an appropriate authority; adequate memory protect and privileged instructions must exist; certain key computer switches must have simple physical barriers to prevent undetected local override; and operating personnel must be cleared to appropriate levels and designed out of the operation as much as possible. A log of all significant events should be kept both by the computer and operating personnel; every user should be subject to common discipline and authority; and remote terminals should be able to vary their security level. The author briefly discusses the following attributes of an acceptable monitor: the security aspects of a monitor shouldn't increase overhead over ten percent; the monitor must perform all input/output without exception; monitor coding that can access any part of core without restriction should be kept to a few well-tested units; the monitor needs to be periodically tested; users' programs must be bound by memory protect while executing; all peripheral accesses must be authorized by the monitor; violating requests must be completely aborted; and security rules must not be suspended for program testing.

*(7280)*67*ae*cb*da*ed*ei*el

Peterson, H. E. "Protecting Privacy Within the Computer System." PROCEEDINGS OF AMERICAN SOCIETY OF INDUSTRIAL SECURITY: 13th Annual Seminar, September 1967, pp. 99-101.

*(7290)*67*ad*ae*ag*aj*cb*cc*da*db*ei*ej*el*eq*fi*hb*hd *jd*je*lb*nh*ni*nn*x2

Peterson, H. E.; and Turn, Rein. "System Implications of Information Privacy." AFIPS CONFERENCE PROCEEDINGS, Spring Joint Computer Conference, Vol. 30, 1967, pp. 291-300; or P-3504, RAND Corporation, Santa Monica, California 90406, April 1967, 40 pp.

This paper was quite valuable when first published. It is widely quoted by other authors. However, most of the ideas in it are now commonly known. The article still serves as a fairly good introductory paper for those unfamiliar with hardware and software aspects of computer security.

The paper presents a discussion of threats to information privacy in non-military information systems, applicable countermeasures, and system implications of providing privacy protection. The authors classify threats to information privacy as accidental, deliberate passive, and deliberate active. They then discuss each of the following threats: accidental (user error, system error); deliberate passive (electromagnetic pick-up, wiretapping, waste basket); deliberate active (browsing, masquerading, between lines entry, piggy-back entry, entry by systems personnel, entry via trap doors, core dumping to get residual information, and physical theft of removable files). Four of the deliberate active threats were originally introduced in this paper. "Browsing" is the use of legitimate system access to obtain unauthorized information. "Masquerading" is posing as a legitimate user after obtaining proper identification by subversive means. "Between-lines" entry consists of penetrating the system when a legitimate user is on a communications channel but not actively using the terminal. "Piggy-back" infiltration consists of intercepting user-processor communications and returning messages contrived to further the infiltrator's purposes.

Following the discussion of threats is a discussion of these countermeasures: access management (authorization, identification, authentication); processing restrictions; threat monitoring; cryptography; and integrity management (verification of system software, hardware, user programs, and later periodic checks). The applicability of each of these five countermeasures to the thirteen specific threats is shown in a summary table. Security implications of the above threats and countermeasures to communication lines, terminals, computerized files, and central processors are also presented.

*(7300)*70*ab*cb*dd*de*fh*eh*fi*na*x2
Peterson, N. D. "Error Control in EDP Systems." MANAGEMENT ACCOUNTING, November 1970, pp. 34-36.

This article is concerned with methods of computer detection and correction of errors in data attributable to both human and machine sources. The following methods were suggested for checking the validity of a data elements: test for blank entries, zero values, and negative values; include a check digit with each element and require the computer to recalculate the digit; check for data outside reasonable limits; set up an exhaustive table of all allowable codes for certain data elements; and determine data element reasonableness from other associated data. For checking the validity of data files, the following are recommended: hard copy printout of all program selected options; control totals of record counts and numeric entries; verify control totals between successive processing phases; verify that file records are correctly sorted; and check for logical discrepancies between similar files.

The author states that the user should not have to depend upon any programmer when exotic errors occur. He feels that it is desirable to consolidate most data validation functions into one program, and that data systems should be tested with data that includes a full range of errors and exceptions. The implementation and advantages of an audit trail are also briefly explained.

*(7310)*70*ab*cc*dd*fi*fz*hr
Peterson, N. D. "A Guide to Acceptance Testing of Computer Software." BUSINESS AND ECONOMIC DIMENSIONS, June 1970, pp. 5-11.

*(7320)*69*ae*cb*cc*cd*dg*nh
Pfoff, Alfred M. "Structuring the Data Security Problem." GUIDE 29 PROCEEDINGS, GUIDE International Corporation, 1 Illinois Center, 111 East Wacker Drive, Chicago, Illinois 60601, 1969.

*(7330)*71*ac*ai*cb*ep*hd*ii*je*lb*x2
"Phone 'Phreaks' Just Can't Tap Data Line Alone." COMPUTERWORLD, 20 October 1971, p. 3.

The article tries to persuade computer users that they don't have to worry about student-types using illegal multi-frequency tone-generators (blue boxes) to access data-system verification trunks and detect what is being transmitted. AT&T said that the connection of "blue box" users to verification trunks would require inside help. However, an ESQUIRE article claims that inside help isn't necessary.

*(7340)*72*ac*ai*cd*gc*jf*x2
Piasta, Frank. "SRI Researcher Says Danger of Magnets to Tape 'Hogwash'." COMPUTERWORLD, 16 February 1972, p. 1.

W. D. Tiffany, manager of the Security Research Program at Stanford Research Institute, has tried unsuccessfully to duplicate conditions under which tape files have reportedly been erased. He states that a magnetic field of 250 gauss (that of a small commercial magnet) would be needed directly at the surface of the tape to damage it. The strength of a magnet is inversely proportional to the cube of the distance from it. Tiffany concludes that even the thickness of a standard tape reel case is enough to prevent the vast majority of readily available magnets from affecting tapes. L. Conroy, director of Securitronics, disagrees with Tiffany's statements. See "Magnets: A Surface Issue" in the August 30, 1972 issue of COMPUTERWORLD for Conroy's counter arguments.

*(7350)*72*ab*cc*cd*dg
Pinkerton, J. A. "Is Your Computer Safe?" COMPUTER DECISIONS, June 1972, pp. 12-14.

*(7360)*67*ab*cd*ed*fv*kg*x1
"Plan for an Unwanted Reward." BUSINESS AUTOMATION, February 1967, pp. 36-39.

This article describes the file backup system used by Science Information Exchange (SIE) of the Smithsonian Institution in Washington, D.C.. For less than $3,000 annually, SIE maintains a disaster file for some 400 magnetic tapes and 15 disk packs.

*(7370)*70*ab*cc*cd*dd*df*hv
"Planning for Your New Computer." COMPUTER DECISIONS, December 1970.

Some installation considerations are given for installing a computer in a new facility.

*(7380)*71*ab*ba*da*hc*ii*lb*ma*nj*x1
"Plot Thickens in Plotting Program Theft." DATAMATION, 15 April 1971, p. 47.

A former Information Systems Design employee allegedly tapped that firm's computer over telephone lines to steal a plotting program valued at $15,000 to $25,000. The program was needed to win over an Information Systems Design customer to the suspect's new employer.

*(7390)*70*ac*ai*bc*cb*dc*gc*jg
"Plug-To-Plug Combustible." COMPUTERWORLD, 14 October 1970.

An electrical short in an IBM 2260 terminal caused a $50,000 fire loss at the Smithsonian Institution in Washington, D.C..

*(7400)*71*ab*cb*cc*dd*de*fx*hp
Polissar, J. "Generating Errors to Reduce Errors." MODERN DATA, May 1971, p. 60.

*(7410)*70*ac*ai*cd*dc*ga*gf*jg
"Poor Security Leaves DP Facilities Ripe for Sabotage." COMPUTERWORLD, 17 June 1970, p. 1.

This article discusses the need for better physical security, especially during the current period of dissent.

*(7420)*66*aa*cc*dg*ff*kd
Porter, W. T. Jr. AUDITING ELECTRONIC SYSTEMS. Wadsworth Publishing Company, 1966.

*(7430)*70*ab*cc*fm
Porter, W. T. Jr. "Control Considerations in Systems

Operations." DATA MANAGEMENT, September 1970, pp. 29-32.

*(7440)*69*ab*cb*ek*ff
Porter, W. T. Jr. "Generalized Computer Audit Programs." JOURNAL OF ACCOUNTANCY, January 1969.

*(7450)*65*aa*bb*cc*db*ff*hj*mc
Pratt, Lester A. BANK FRAUDS: THEIR DETECTION AND PREVENTION. The Ronald Press Company, 1965.

*(7460)*70*ab*bb*cc*db*de*ff*fy*hj*kb*kd*mc*ni*x2
Pratt, Lester A. "Loss Exposure Hazards Under Bank Automation." BURROUGHS CLEARING HOUSE, October 1970, p. 18.

When one realizes that scarcely a day passes without at least one bank embezzlement being brought to light, it becomes evident that employee dishonesty is one of the most serious hazards of the banking industry. EDP does not lessen in any way the need for an evaluation of the system of internal control. On the contrary, it is essential that internal controls be more carefully scrutinized to ascertain that they are effective. Throughout this seven page article, many different vulnerabilities to embezzlement are pointed out, and internal control recommendations are given for safeguarding against these vulnerabilities. An eleven item checklist is given to help the internal auditor determine the efficiency of his audit program. Specific problems associated with MICR inscribed numbers on checks are also discussed. The author states that verification of account figures is the most effective method of detecting embezzlements or honest errors. Although most of the internal control recommendations presented are widely known, the article still provides a valuable overview of the internal control problems in the banking industry.

*(7470)*70*ac*ai*cc*da*fe*hd*ka*mj*nm
"Precautions Preclude Misuse of Student Data." COMPUTERWORLD, 4 March 1970, p. 1.

*(7480)*70*ac*cc*dg*ff
Presnick, Walter. "Protecting Your Computer's Security." DATA SYSTEM NEWS, February 1970.

This is a brief interview with Joseph J. Wasserman, president of Computer Audit Systems.

*(7490)*72*ad*cb*cc*da*ea*ed*hd*he*ka*mb*md*mf*mg*mj*nd *ng*nm*no*x4
"The Privacy and Computer Task Force Report." Communications Canada, Information Services, 100 Metcalfe Street, Ottawa, Ontario, 1972, $2.50.

This report was prepared for the Canadian Departments of Communications and Justice. It presents the findings of an eighteen month study on the relationship of the computer and personal privacy. For a short summary of its contents read either "Snapshop 1971 - How Canada Organizes Information About People" by John M. Carroll or "Canadian Study Sees Role for United Nations in Privacy Issue" by E. Drake Lundell Jr.

*(7500)*70*ac*ai*cc*da*ka*nl*nm
"Privacy Commission Chairman Suggests Licensing Plan." COMPUTERWORLD, 11 November 1970.

*(7510)*71*ab*cc*da*ka*nm
"The Privacy Thing." BUSINESS AUTOMATION, May 1971.

*(7520)*69*ab*cc*dg*ff
"Problems and Potential Solutions in Computer Control." INDUSTRIAL SECURITY, April 1969.

*(7530)*70*ab*cc*df*dg*fz*ma*nj
"Problems of Liability for the EDP Security Industry." COMPUTERS AND AUTOMATION, September 1970.

*(7540)*68*ab*ba*da*hc*mi
"Program Plagiarism Alleged in U.K. Case." DATAMATION, June 1968, p. 91.

The case involves a BOAC airline reservation system program.

*(7550)*65*ab*ba*cc*da*fs*f1*hc*kb
"Proprietary Programs Progress: Ten Copyrights, One Jail Sentence." DATAMATION, October 1965, p. 11.

*(7560)*66*ab*cc*da*db*hb
"Protect Your Business Secrets." MODERN OFFICE PROCEDURES, May 1966.

*(7570)*00*af*cd*da*dc*gf
"Protecting Company Property Against Vandalism and Theft." Briefing No. 761, Retail Research Institute.

Various types of access control and alarm devices are described. Their advantages and disadvantages are discussed, and certain devices are recommended. A "where-to-purchase" guide is given for all the devices.

*(7580)*68*ad*cd*dc*ge
"Protection of Electronic Computer/Data Processing Equipment 1968." NFPA No. 75, National Fire Protection Association, 60 Batterymarch Street, Boston, Massachusetts 02110, 1968, 32 pp., $.75.

This pamphlet outlines the preplanning stage of fire protection for the computer room. Details of design, types of materials required, construction of hardware, air conditioning, coolant systems, and emergency power controls are discussed. Water, carbon dioxide, and Halon 1301 extinguishing systems are also discussed.

Other N.F.P.A. pamphlets include: #10 - Portable Fire Extinguishers ($1.00), #12 - Carbon Dioxide Extinguisher Systems ($1.50), #13 - Sprinkler Systems ($2.00), and #232 - Protection of Records ($1,00).

*(7590)*70*ad*cd*dc*ge

"Protection of Records 1970." No. 232, National Fire Protection Association, 60 Batterymarch Street, Boston, Massachusetts 02110, $1.00.

This pamphlet contains complete information on protection of paper-type records. Other NFPA pamphlets include: #75 - Protection of Electronic/Data Processing Equipment 1968 ($.75), #10 - Portable Fire Extinguishers ($1.00), #12 - Carbon Dioxide Extinguisher Systems ($1.50), and #13 - Sprinkler Systems ($2.00).

*(7600)*69*ab*cd*dc*dd*ga

"Providing the Right Environment." ELECTRONIC REVIEW, 28 November 1969.

*(7610)*66*ab*ba*da*je*x2

Purgslove, S. D. "The Eavesdroppers: 'Fallout' from R & D." ELECTRONIC DESIGN, 21 June 1966, pp. 35-43.

The placing of wiretaps on telephone lines, terminal boards, in manholes, or directly inside a telephone or data modem has become a sophisticated art. Detection of a tap on the external wires is extremely difficult by other than visual inspection.

*(7620)*71*ab*cd*da*gf*x1

"A Pushbotton Lock for Computer Room Security." THE OFFICE, March 1971, p. 161-163.

The article describes a pushbotton lock manufactured and sold by Simplex Lock Corporation in Collinsville, Connecticut. The lock offers two advantages. First, no control of keys is needed, and second, the combination can be easily and cheaply changed when an employee leaves or when the threat of labor trouble occurs. The lock is completely mechanical with prices starting at $35.00.

*(7630)*73*af*cc*cd*nm*np*x4
QUARTERLY BIBLIOGRAPHY OF COMPUTERS AND DATA PROCESSING. Applied Computer Research, 8900 North Central Avenue, Phoenix, Arizona 85020, 1971-, (Quarterly, with annual and semi-annual cumulations).

This subject-indexed annotated bibliography is designed primarily for individuals engaged in the practicing end of the computer profession, including computer users, consultants, time-sharing users and suppliers, software houses, etc.. The periodicals reviewed are primarily computer-related trade publications, general business and management periodicals, and computer-oriented and management-oriented professional societies. The more esoteric and academic literature is not reviewed.

The bibliography is intended to be thorough, but newspaper items are not included. 126 security articles were listed from January 1968 to January 1973. The first issue, April 1971, covers January 1968 to March 1971. Approximately 175 periodicals are reviewed along with pertinent books and reports. Because "security" is one of the bibliography's subject indices, relevant articles are easy to find. Almost all periodicals are annotated in one sentence. This bibliography is currently (May 1973) the best periodically-published reference work on computer security.

*(7640)*68*ab*cc*da*db*dd*de*ff*ni
"Questionnaire for Evaluation of Internal Control in Data Processing." AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTS, 1968.

Although interesting, this article is somewhat out-of-date. For a more up-to-date publication see COMPUTER CONTROL GUIDELINES by the Canadian Institute of Chartered Accountants, or "AFIPS System Certification Would Help Protect Public" by Edward J. Bride.

*(7650)*70*ac*ai*cd*dc*gf
"Radical Rumblings Heeded, Centers Increase Security." COMPUTERWORLD, 14 October 1970.

Many midwest EDP installations are adding closed circuit TV, additional guards, etc., to provide additional protection against violent demonstrations and sabotage.

*(7660)*71*ab*cc*cd*fv*ge*gf*mi*no*x2
"Railroads Outline Their Approaches to Computer Security." RAILWAY AGE, 13 September 1971, p. 68.

This article summarizes the findings of a computer security survey taken by RAILWAY AGE. The survey was only concerned with physical access control, data file protection, and data file backup. Some of the safeguards taken by Louisville & Nashville, Seaboard Coast Line, Union Pacific, Southern, and Southern Pacific are briefly described. Unfortunately, the article only presents the positive aspects of the survey. It appears that most of these railroads use extensive physical access control procedures and provide quite satisfactory off-site file backup where frequently updated files are stored in large secure safes. However, most of the railroads did not have any standby computer hardware or equipment backup facilities. They planned to utilize service-bureaus in case of equipment failures.

*(7670)*68*ad*cb*dg*ed*ef*ei*el*fe*gh
Ramirez, J. "Problems in Protection of Information in a Multiuser On-Line System." Master's Thesis, Moore School of Electrical Engineering, University of Pennsylvania, Philadelphia, Pennsylvania, May 1968.

The Moore School's Problem Solving Facility is described in detail. Methods of preventing "conflict-request" problems when two or more users are simultaneously sharing a file are discussed. For more information read "A File System for a Problem Solving Facility" by David K. Hsiao.

*(7680)*71*ab*cc*dg*fx*ni
Ramsgard, W. C. "Evaluate Your Computer Installation." MANAGEMENT SERVICES, January 1971, pp. 37-41.

*(7690)*73*ab*cb*dg
Rapoport, R. "Electronic Alligators." SATURDAY REVIEW OF THE SCIENCES, March 1973, pp. 35-38.

*(7700)*72*ab*cc*ff*fx
Rau, P. "Evaluating the EDP Function." DATAMATION, September 1972, pp. 72-73.

*(7710)*aa*cc*ff*fp*fv*x1

Rauseo, Michael J. MANAGEMENT CONTROLS FOR COMPUTER PROCESSING. American Management Association Inc., 135 West 50th Street, New York, New York 10020, 1970, 272 pp., $12.00.

The main purpose of this book is to present fundamental technical concepts and applications of basic management principles that apply to the computer systems area. The book doesn't presume the reader has any understanding of general EDP methods or computer techniques. The five chapters are entitled: (1) How to Identify Potential Computer Applications, (2) What a Manager Should Know About Computer Programming, (3) Management Methods and Feasibility Studies, (4) Management Control of Computer Processed Information, and (5) Organizing and Managing the Computer Department. Only chapter 4 is concerned with computer security. Controls are mentioned for programming errors, operator errors, hardware errors, and protection of files. Tape library control systems, retention plans, reconstruction plans, and the effect of the computer on the audit trail are also discussed.

*(7720)*73*af*cc*np*x1

READERS' GUIDE TO PERIODICAL LITERATURE. The H. W. Wilson Company, New York, 1900-, (Monthly, with annual cumulations).

This guide is a cumulative author/subject index to periodicals of general interest published in the United States. Desired articles can be found under the subject index "Electronic Data Processing (now 'Computers') - Security Measures". Each annual publication contains several computer security articles, but most of these, plus additional security articles, can be easily located in the BUSINESS PERIODICALS INDEX.

*(7730)*70*ac*ai*bg*dg

"Real DP Crime May Blossom." COMPUTERWORLD, 25 November 1970.

*(7740)*72*af*cc*df*fm

"Recognition of EDP Operational Problems." LYBRAND NEWSLETTER, September 1972.

*(7750)*70*ad*bc*cc*cd*dc*fs*ga*gd*ge*jg

"Recommended Good Practices for the Protection of Electronic Data Processing and Industrial Automation." Factory Insurance Association, Hartford, Connecticut, 1970.

This is a good comprehensive booklet on physical security and fire prevention. Some of the safeguards discussed are: location selection, elimination of combustibles, control of ignition sources, smoke removal systems, fire detection and extinguishment, backup power, and operating procedures. Several checklists on construction details are also given.

*(7760)*68*ab*cc*cd*da*dc*fp*fv
"Records Protection in the Age of EDP." THE OFFICE, October 1968.

*(7770)*67*ab*cc*fk
"Record Retention Timetable." MODERN OFFICE PROCEDURES, April 1967.

This article discusses the length of time that records should be kept before they are destroyed.

*(7780)*73*ae*ag*ca*da*ep*er*es*x2
Reed, I. S. "Information Theory and Privacy in Data Banks." AFIPS NATIONAL COMPUTER CONFERENCE PROCEEDINGS, Vol. 42, 1973, pp. 581-587.

This paper relates the security of data records in computerized retrieval systems with Shannon's information-theoretic treatment of secrecy systems for natural language messages in communication systems. The reader must be familiar with the mathematics of communication theory to adequately understand this paper. First, the analogy between retrieval systems and certain communication channels is explained. The requirements of a privacy system are not as stringent as those of a secrecy system, because personal records can be sufficiently distorted to make inferences about them nonunique and yet allow their use in statistical analysis. Distortion measures are presented which will achieve maximum privacy (although less than perfect) for a given allowable degree of distortion.

*(7790)*69*ab*cb*ep*eq
Reed, I. S.; and Turn, Rein. "A Generalization of Shift-Register Sequences." P-3698, RAND Corporation, Santa Monica, California 90406, January 1969; or JOURNAL OF THE ACM, July 1969, pp. 461-473.

Circuits based on the feedback shift-register concept appear especially suitable for cryptology applications.

*(7800)*71*af*cc*fu
Reeder, James A. "Security Education and Training: Prevention Against Compromise." DEFENSE INDUSTRY BULLETIN, Winter 1971.

*(7810)*69*ab*cc*ff
Reeve, J. T.; and Johnson, R. E. "Practical Use of Computer in Auditing." THE INTERNAL AUDITOR, January 1969, p. 15.

*(7820)*71*ab*cb*ek*ff

Reid, G. F.; and Demcak, L. A. "Audit Implementation with General Purpose Software." JOURNAL OF ACCOUNTANCY, July 1971, pp. 35-36.

*(7830)*70*ab*cc*fm
Reid, H. V. "Problems in Managing the Data Processing Department." JOURNAL OF SYSTEMS MANAGEMENT, May 1970, pp. 8-11.

*(7840)*71*ab*cc*cd*dg*fa*fb*ff*fh*fo*fq*fv*nf*x3
Reider, Harry R. "Maintaining the Security of Computer Records." BURROUGHS CLEARING HOUSE, February 1971, p. 28.

Many desirable control procedures are presented for use in data processing installations. The same control procedures that were exercised over clerks, bookkeepers, and accountants in conventional systems, must be exercised over programmers, systems analysts, and computer operators in computer systems. In the design of an effective EDP organization plan, the following factors should be considered: definition of individual responsibilities for all functions; preparation of formal job descriptions; separation of functions and duties; installation of internal processing control and external checking functions; and establishment of standards of performance for personnel. Data Processing documentation can serve to provide material for supervisory review, system and program revision, inquiry response, new personnel instruction, and internal control evaluation. Documentation should include an installation standards manual, system documentation, program run books, operators run books, keypunch manuals, and clerical procedures manuals. Input controls must be established where data are: created; converted to machine form; entered into the computer; handled, moved, or transmitted in the organization; and rejected in processing. Output controls must assure only those authorized to see the data receive it, and feedback mechanisms must exist for reporting errors. Processing controls should include: overflow condition error tests; operator message controls; check-point controls; and reasonable limit, crossfooting, control total, and edit tests. File protection involves a combination of: physical controls (environment control, fireproof vaults); procedural controls (tape and disk labeling, off-site storage); and a retention plan (grandfather-father-son concept).

*(7850)*72*ab*cc*cd*dg*fa*fb*ff*fh*fo*fq*fv*nf*x3
Reider, Harry R. "Safeguarding Computer Records." MANAGEMENT CONTROL, October 1972, pp. 245-248.

This article is identical to another article by Reider entitled "Maintaining the Security of Computer Records" in the February 1971 issue of BURROUGHS CLEARING

HOUSE,

*(7860)*70*ac*ai*cd*ge
"Reservations Center Prefers 'Wet Look'." COMPUTERWORLD, 14 October 1970.

Pacific Southwest Airlines has installed a water sprinkler system in its computer center.

*(7870)*72*ac*cb*nb*ng*nk*x2
"Responsibilities Assigned in IBM Security Study." ELECTRONIC NEWS, 21 August 1972, p. 26.

IBM's $40 million, five year research program to develop hardware and software data access safeguards in computer systems is briefly outlined. The following four sites were selected to participate in the study: the Federal Systems Division in Gaithersburg, Maryland; MIT in Cambridge; the State of Illinois in Springfield; and TRW Systems in Redondo Beach, California. The Federal Systems Division will coordinate and integrate activities of the other sites, provide programming support, and train personnel involved in the study. MIT will check out various hardware through which information can be shared, determine how access can be controlled, and study the effect of the user environment to control access to systems. Illinois will investigate the cost to users of achieving different levels of data security. TRW will attempt to develop definitions of systems security and measurement techniques needed to determine levels of security.

*(7880)*68*ab*cb*cc*em*na
"Restart and Recovery." EDP ANALYZER, October 1968.

*(7890)*72*ab*ak*cc*fm
Rettus, R. C.; and Smith, R. A. "Accounting Control of Data Processing." IBM SYSTEMS JOURNAL, January 1972, pp. 72-92.

*(7900)*70*ac*ai*bc*dc*jf
Revolutionary-Force Bombs IBM Office." COMPUTERWORLD, 18 March 1970, p. 1.

*(7910)*71*ab*bb*cd*da*db*dc*ga*gf*hk*ho*if*ii*mc*x1
Reynolds, Jayne H. "Computer Misuse: A look at Vulnerable Areas." BEST'S REVIEW: Life/Health Edition, May 1971, p. 76; or BEST'S REIVEW: Property/Liability Edition, May 1971, p. 70.

This article is primarily concerned with physical security. It attempts to persuade the reader that most organizations have very inadequate safeguards. Several actual and hypothetical examples of computer misuse by disgruntled employees and saboteurs are discussed. In one example, a supervisor, who was passed over for department head when his boss retired, spent several months trying to discredit his new boss by feeding misinformation into the computer. Physical security safeguards implemented by several unnamed insurance companies are also described.

*(7920)*71*ab*cc*da*hd*ka*nm
Robinson, Stanley. "The National Crime Information Center (NCIC) of the FBI: Do We Want It?" COMPUTERS AND AUTOMATION, June 1971, pp. 16-19.

The author has doubts about the NCIC. He feels it may contain the ingredients of a police state.

*(7930)*68*ae*cb*cc*fv*gf
Rofes, William. "Disaster Recovery." PROCEEDINGS OF SHARE 31 AND GUIDE 27; SHARE Inc., 25 Broadway, Suite 750, New York, New York 10004; or GUIDE International Corporation, 1 Illinois Center, 111 East Wacker Drive, Chicago, Illinois 60601, October 1968, Sect. 5, pp. 55-70.

The protection needed for vital computerized business records is discussed.

*(7940)*70*ae*cb*cc*fv*gf
Rofes, William. "Vital Records Protection." GUIDE 30 PROCEEDINGS, GUIDE International Corporation, 1 Illinois Center, 111 East Wacker Drive, Chicago, Illinois 60601, 1970.

*(7950)*72*ab*cc*df*fm*ni
Romberg, B. W. "Eyeball Your Computer Operations Today." INFOSYSTEMS, December 1972, pp. 30-31.

*(7960)*69*aa*cc*da*de*fe*fh*fk*fj*hd*ka*mb*md*nl*nm
Rosenburg, Jerry Martin. THE DEATH OF PRIVACY. Random House, New York, New York, 1969, 236 pp.

The capability of the computer to control huge data banks and to pose as a threat to personal privacy are examined. The author believes that the individual should have the opportunity to: refute stored personal information, determine what is collected, and maintain a permanent check on how data on him is used. Other data privacy laws and regulations are also proposed. The book is only remotely concerned with technical and operating procedure safeguards for data security.

*(7970)*68*ab*cc*fa
Rosner, M. N. "Organizing for Management Information." SYSTEMS & PROCEDURES, November 1968, pp. 35-37.

*(7980)*65*ab*cc*ff
Ross, F. E. "Internal Control and the Audit of Real-Time

Digital Systems." JOURNAL OF ACCOUNTANCY, April 1965, pp. 46-55.

*(7990)*72*ab*cc*de*df*fb*hv*x2
Ross, Joel E. "Computers: Their Use and Misuse." BUSINESS HORIZONS, April 1972, pp. 55-60.

The problem of how to make computers pay off is analyzed. Most failures can be traced to four mistakes: thinking an information system can substitute for a management system; lack of top-management involvement; a communications gap between management and computer personnel; and failure to organize properly.

Here is a list of recommendations suggested by the author: design your own turnkey operation; save some money for new applications and development; don't let DP managers make all computer decisions; don't install a management information system without a management system; scrap systems that don't perform; don't underestimate development costs; eyeball output reports for outrageous mistakes; check the technical, economical, and operational feasibility of proposed projects; determine what you want MIS to do; set objectives, identify constraints, determine information needs, specify all output; and avoid automatic bill payment.

*(8000)*68*ab*cc*fa
Rossner, M. N. "Organizing for Management Information." SYSTEMS AND PROCEDURES JOURNAL, November 1968, pp. 35-37.

*(8010)*66*ab*cc*ff
Rothery, B. "Information and the Auditor." DATA PROCESSING MAGAZINE, August 1966, pp. 58-59.

*(8020)*72*ae*ag*cb*cc*dg*hd*ig*ih*ka*lb*mf*nl*nm*x2
Rothman, Stanley. "The Protection of Privacy and Security in Criminal Offender Record Information Systems." AFIPS CONFERENCE PROCEEDINGS, Fall Joint Computer Conference, Vol. 41, 1972, pp. 423-424.

This paper singles out those aspects of the problem of protecting privacy and security in information systems that are special to law enforcement. The rule that any computer participating in the FBI's remote access National Crime Information System must be either dedicated to law enforcement or under law enforcement control is causing considerable debate. The development of a commercially available secure operating system is vital to resolving this debate. By far the most common threat is bribery of systems employees and police officers by private detectives, bank officers, newspaper reporters, employees, etc.. Since most law enforcement agencies must manage personnel within civil service regulations, proper pre-employment screening and firing

employees for security violations are difficult. The Law Enforcement Assistance Act has developed through project SEARCH, a model act for state government, and administrative regulations for the protection of privacy in computerized criminal-history systems. However, there is no guarantee that the states will approve this recommended model act.

*(8030)*68*ae*cb*ed*gh*mh
"RYE, CAPRI, COINS, OCTOPUS, SADIE, Systems." Network of Computers Workshop, National Security Agency, October 1968.

*(8040)*70*ac*ai*dc*hg*jf
"Sabotage Course Shows Action May Have Bad Effect on Society." COMPUTERWORLD, 25 November 1970, p. 1.
A humanities course at Syracuse University on nonviolent sabotage of computers has discovered that society as a whole can be hurt by computer sabotage.

*(8050)*70*ac*ai*cb*dc*gc
"Safe Source Says Some Safes are Safer." COMPUTERWORLD, 21 October 1970.
The differences between EDP media storage and regular paper storage are discussed. One difference is that paper can withstand a 350 degree temperature while magnetic tape starts to deteriorate at less than 200 degrees. The information on magnetic tape vulnerability may now be somewhat obsolete.

*(8060)*68*ad*cc*cd*dc*fw*gd*ge*jf*no
"Safeguard Data Processing Files and Programs." RETAIL RESEARCH INSTITUTE - EDP INFORMATION SERVICE, July 1968.
This article presents the results of a survey of 20 large retail stores regarding their practices in safeguarding data processing files and programs, and in preventing serious disruption of computer operations in the event of serious urban riots. The survey questioned the stores on: storage, updating, microfilming, source data storage, alarm systems for fire and smoke, backup agreements, auxiliary power, alternatives to phone service, employee safety, skeleton staff in time of riot, and receipt of mailed data.

*(8070)*67*ab*cb*cc*ea*lb
"Safeguarding Time-Sharing Privacy - An All-Out War on Data Snooping." ELECTRONICS, 17 April 1967.
A large part of this article is devoted to a discussion of the 1967 Spring Joint Computer Conference on data security.

*(8080)*00*ad*dc*jg*na
"Salvaging and Restoring Records Damaged by Fire and Water." RP-2, Federal Fire Council, Washington, D.C. 20405.

*(8090)*67*ab*cb*eq
Savage, J. E. "Some Simple Self-Synchronizing Digital Data Scramblers." BELL SYSTEMS TECHNICAL JOURNAL, February 1967, pp. 448-487.

*(8100)*70*ab*cc*mf*x1
Scaletta, Phillip J. Jr. "The Computer and the Administration of Justice." DATA MANAGEMENT, December 1970, pp. 34-39.
The use of computers in the field of law is

discussed. This article is the third part of a four part series on the legal ramifications of the computer age. Although this article isn't concerned with computer security considerations, the other three parts of the series are concerned with security.

Courts are now using computers for: accounting, sorting, scheduling, and printing of material; collecting parking violation fines, maintaining case name indexes, automatic case docketing, calendar control, and jury selection. Law firms are beginning to use computers for: timekeeping; fee billing; payroll and expense accounting; attorney productivity reports; attorney availability reports; unbilled time analysis; and financial condition analysis. Legislators are using computers to store and display existing laws and proposed bills, and for legislative redistricting. The use of computers for retrieving relevant case and statuate law is also discussed.

*(8110)*71*ab*cc*da*de*hd*ka*nm*x1
Scaletta, Phillip J. Jr. "The Computer as a Threat to Individual Privacy." DATA MANAGEMENT, January 1971, pp. 18-23.

This article is a basic introduction to computers and the privacy problem. Some general problems associated with the Federal Data Center proposal are discussed. Although the U.S. Constitution does not specifically guarantee the right to privacy, the courts are more frequently taking the position that an individual has the right to control information about himself. A number of common ways that information could be illegally obtained from time-sharing computers are presented. Out of carelessness, maliciousness, or sheer stupidity, much damage can be done by administrators who introduce errors into records. The author feels that Congress must pass some privacy legislation, but he doesn't give any specific recommendations.

*(8120)*70*ab*cc*dd*de*nj*x2
Scaletta, Phillip J. Jr. "The Legal Ramifications of the Computer Age: Part 1 - Suing a Computer: Printout as Evidence." DATA MANAGEMENT, October 1970, pp. 12-15.

This article discusses legal problems that have resulted from the unique characteristics and uses of computers. In most computer cases there will probably be no witnesses. Assuming a malfunction is found, what is the standard of conduct against which the defendant's conduct may be measured? How does one resolve a common jury misconception that computers are nearly infallible? What happens if the computer retrieves the wrong credit reference from its memory and a customer is wrongfully denied credit? Should the injured plaintiff bear the burden of proving specific acts of negligence? Do accidents involving computers normally occur in the absence of negligence? Under what circumstances can the board of directors be sued for not using a computer to stay competitive or for using a computer in untested and potentially dangerous situations?

The author doesn't want to wait for a case-by-case development of tort law to answer these questions. He recommends legislation placing strict liability on the user and the manufacturer of computers for any damage or injury caused by computer malfunction or mishap.

*(8130)*70*ab*cc*df*dg*fz*ma*x2
Scaletta, Phillip J. Jr. "The Legal Ramifications of the Computer Age: Part 2 - Contracts, Patents, and Copyrights." DATA MANAGEMENT, November 1970, pp. 20-22.

The following problems should be resolved in an agreement for computer services. The written contract should carefully spell out an obligation of the data processor to provide for security of the data entrusted to him. Liquidated damages should be mutually agreed upon which would compensate the user for loss which he would have if his data or its secrecy was lost. The contract should clearly specify who is responsible for errors and what error detecting procedures the processor must use. Requirements for service availability under unexpected circumstances also need consideration. A lawyer must carefully word the contract since many computer words and terms have no precise legal definition.

The discussion on copyrights and patents is obsolete. See "Legal Protection of EDP Software" by David Goldberg for a more recent and more informative discussion of copyrights and patents.

*(8140)*70*ac*ai*ba*da*ma
"Scandinavia's First Data Theft Occurs at Service Bureau." COMPUTERWORLD, 18 November 1970.

*(8150)*72*ab*cc*fm
Schefer, E. A. "Management Control of the Corporate Computer Activity." DATA MANAGEMENT, September 1972, pp. 45-56.

*(8160)*72*ae*cb*ed*ei
Schell, Roger R. "Summary of Remarks for Panel Discussion on Privacy and Protection in Operating Systems." ACM NATIONAL CONFERENCE, 1972.

*(8170)*70*ab*cc*da*db*ft*nm
Schiedermayer, P. L. "The Many Aspects of Computer Security." THE POLICE CHIEF, July 1970, p. 20.

This article describes various aspects of computer theft, fraud, and privacy invasion. Its purpose is to acquaint police personnel with computer related crimes. The author believes that honest EDP personnel are the best insurance against computer crimes.

*(8180)*73*ac*cc*da*ka*nl*nm*x4
Schmeck, Harold M. Jr. "A Federal Panel Urges New Laws to Protect the Privacy of Personal Records." NEW YORK TIMES, 1 August 1973, p. 17.

A government advisory committee has just recommended a new code for "fair information practice", backed up by law, to protect individual privacy in this age of computers. The committee's panel of experts presented a 346 page report which is the result of their year-long study. Casper Weinburger, current Secretary of Health, Education, and Welfare, said that he agrees with the general principles of the report. The report advocates strong criminal and civil laws for the following five principles: there must be no secret personal data record-keeping systems; there must be a way for an individual to find out what information is kept on him and how it is used; there must be a way for an individual to prevent information about him obtained for one purpose from being used for other purposes without his consent; there must be a way for an individual to correct or amend a record about himself; and any organization creating, maintaining, using, or disseminating personal records must insure the reliability of these records for their intended use, and take precautions to prevent misuse. The report opposes the establishment of a standard universal identifier, and recommends that constraints be placed on the use of Social Security numbers as identifiers.

*(8190)*72*ad*aj*al*ca*dg*ee*eh*ng
Schroeder, Michael D. "Cooperation of Mutually Suspicious Subsystems in a Computer Utility." Ph.D. Dissertation, MAC TR-102, Electrical Engineering Department, MIT, Cambridge, Massachusetts 02139, September 1972.

Practical protection mechanisms are described that allow mutually suspicious subsystems (like independently compiled programs and databases) to cooperate in a single computation and still be protected from each other. These mechanisms are based on the division of a computation into independent domains of access privilege, each of which may encapsulate a protected subsystem.

*(8200)*72*ab*ae*ah*cb*dg*ec*ee*ef*ei*lb*x2
Schroeder, Michael D.; and Saltzer, Jerome H. "A Hardware Architecture for Implementing Protection Rings." PROCEEDINGS - THIRD ANNUAL ACM SYMPOSIUM ON OPERATING SYSTEMS PRINCIPLES, October 1971; or COMMUNICATIONS OF

THE ACM, 3 March 1972, pp. 157-170.

This paper describes a set of hardware precessor access control mechanisms that were devised as part of the second iteration of the hardware base for the MULTICS system. MULTICS is a general purpose, multiple user, interactive computer system developed by Project MAC of MIT in a joint effort with the Cambridge Information Systems Laboratory of Honeywell Information Systems Inc. and, until 1969, the Bell Telephone Laboratories. MULTICS in currently implemented on a modified Honeywell 645 computer system. The 645 computer was the first attempt to define a suitable hardware base for a computer utility. It was recently modified to include an improved and expanded set of access control mechanisms which implement protection "rings" almost completely in hardware.

In a system which uses segmentation as a memory addressing scheme, protection can be achieved in part by associating concentric rings of decreasing access privilege with a computation. The hardware processor mechanisms for implementing these rings of protection are described in detail in this paper. They allow cross-ring calls and subsequent returns to occur without trapping to the supervisor. Automatic hardware validation of references across ring boundaries is also performed. A call by a user procedure to a protected subsystem (including the supervisor) is identical to a call to a companion user procedure. A segment is the smallest unit of information that can be protected.

The paper begins by establishing the general need to control access to stored information in a computer utility and by presenting several criteria for comparing different sets of access control mechanisms. Relevant aspects of the organization of segmented memories were then sketched, and the processor mechanisms for implementing protection rings were described. The paper concludes by illustrating how rings can be used and by evaluating the impact of a hardware system.

*(8210)*70*ab*bb*cc*db*fq*hj*kb*kd*mc*x1

Schweisheimer, W. "Embezzlement by Computer." BANKERS MONTHLY, June 1970, pp. 291-292.

A few examples of embezzlement by computer are described. Many executives have the misconception that they must throughly understand computers before they can ask intelligent questions concerning computer operations and security worthiness. The author states that executives can and must ask questions about a computer's security even though they don't understand computers. Most computer experts believe that implementation of the following four steps will prevent a large majority of all embezzlements: don't let programmers operate the computer; segregate check authorizing and check writing operations; frequently rotate the duties of programmers and operators; and frequently perform computer audits of the financial records.

*(8220)*69*ad*ae*cd*dc*ga
Scoma, Louis Jr. "Catastrophe Prevention in the Computer Complex. Environmental Factors: How Vulnerable Are You?" American Management Association Conference on Security and Catastrophe Prevention Management of the Computer Complex, November 1969; or Data Security Inc., 15 Spinning Road, Hinsdale, Illinois 60521.

*(8230)*71*ae*cc*cd
Scoma, Louis Jr. "Protecting the Cost of Technology: Security and the Data Center." AMA 17TH ANNUAL SYSTEMS MANAGEMENT CONFERENCE, American Management Association, New York, New York, March 1971, 5 pp.

Several basic considerations are discussed for operating a secure computer center.

*(8240)*71*ab*bc*cd*dc*x1
Scoma, Louis Jr. "Protecting Your EDP." THE OFFICE, September 1971, pp. 53-54.

The author briefly lists twelve actual examples of computer destruction by disgruntled employees or saboteurs, and the resulting losses. His statement that a small quarter-size magnet can erase 50,000 tapes in minutes is preposterous. Other security experts claim such a magnet would be lucky to erase one tape. (Read an article entitled "Magnets: A Surface Issue" in the August 30, 1970 issue of COMPUTERWORLD.) Scoma lists the following ten commandmends of EDP security. Thou shalt: not take security for granted, provide for adequate personal clearances, establish restricted areas, provide fire control and prevention measures, provide for theft detection, provide for sabotage detection, establish riot and mob controls, not overlook backup equipment requirements, generate backup databases, and be security minded in the physical planning of computers.

*(8250)*70*ab*bc*cd*dc*x1
Scoma, Louis Jr. "Security in the Computer Complex." COMPUTERS AND AUTOMATION, November 1970, p. 10.

The author cites six examples of computer and computerized data destruction caused by student saboteurs and disgruntled employees. He then briefly makes the following recommendations: take time to adequately plan your facility and regularly review your existing facility; plan the complex to meet the particular neeeds of your firm; train all operating personnel in fire reporting and fire fighting procedures; be prepared for the disgruntled employee; security check all new DP personnel; and provide adequate air-conditioning and power backup to avoid a major business interruption. However, Scoma's statement that a quarter-size magnet can destroy up to 50,000 tapes in a matter of minutes is preposterous. Some authors doubt that a quarter-size magnet can destroy anything. (See "Magnets: A Surface Issue" in the August 30, 1072 issue of COMPUTERWORLD.) Scoma's articles are typical of those discussed by Mel Mandell in an article entitled "Computer Scare Talk: Sabotage Fears of 'Experts' Discounted" in the May 9, 1971 issue of the NEW YORK TIMES.

*(8260)*72*ad*cb*da*eq*nn

"Scrambling and Unscrambling Files for Security." PB-213 899/3, National Technical Information Service, Springfield, Virginia 22151, November 1972, 102 pp., $12.50.

The article proposes a method for encoding and decoding data files based on a one-time pad used just before and after transmission. This method supposedly gives better protection than previous data scrambling techniques. A short survey on previously attempted scrambling techniques is also given.

*(8270)*67*ab*ad*cb*cc*cd*dg*nm

SDC MAGAZINE: July 1967. System Development Corporation, 2500 Colorado Avenue, Santa Monica, California 90406.

The entire issue of the magazine is concerned with computer security and data privacy. The privacy issue is discussed at length, but the security issue is given much less coverage.

*(8280)*69*ab*cb*cc*db*mc*nl*x1

"SEC Closes in on Computers." BUSINESS WEEK, 9 August 1969, p. 82.

Up until recently, the Securities and Exchange Commission hasn't stretched its authority to cover Wall Street's new computer networks serving giant institutional traders. However, the commission has now proposed rules that could require automated trading system users to submit details on how they plan to guard against price-rigging, fraud, and manipulation, and how they intend to keep unauthorized interests out while giving the SEC access. Two trading systems that will be most affected, Autex and Instinet, are briefly described. The New York Stock Exchange's block automation system and the National Association of Securities Dealer's automated quote system will be exempt from the proposed rules.

*(8290)*71*ab*cb*da*ep

"Secure Communications." THE COMMUNICATIONS USER, January

1971.

*(8300)*73*ac*ai*cb*cc*db*dd*de*mk*ne*no*x3
"Secure and Accurate? Most Vote Officials Seem Content." COMPUTERWORLD, 9 May 1973, p. 1.

Although there have been many recent stories about inaccuracies and security breaches in computerized vote counting systems, most county election officials seem to be unconcerned about the problem. This was the conclusion drawn from a survey of county election systems prepared a year ago and just released by Systems Research Inc.. County election officials using punched card systems rated their equipment as 100% accurate and secure, while those using paper ballots rated their system as only 83% accurate and 75% secure. Officials apparently still find it easy to have blind faith in the computer.

The survey also found that punched card voting systems are more expensive than lever-type voting systems. The average cost per registrant for lever, punched card, and paper ballot systems was found to be $1.39, $1.90, and $2.05 respectively. Only 7% of the counties presently use punched card systems, although 16% use computers to maintain registration lists.

*(8310)*70*ad*cb*cc*da*ed*gh*ka*mf*nm
"Security and Privacy Considerations in Criminal History Information Systems." Report No. 2, Project SEARCH, California Crime Technological Research Foundation, Sacramento, California, July 1970.

*(8320)*70*ac*ai*bc*cc*cd*dc*jf*mj
"Security Cut Damage from DP Center Blast." COMPUTERWORLD, 23 December 1970, p. 1.

A bomb explosion at the University of Kansas Computer Center caused minor damage thanks to recent security improvements at the center.

*(8330)*69*ab*cd*da*ep*gf*hb*kb*x1
"Security Defenses for the Computer Room." OCCUPATIONAL HAZARDS MAGAZINE, December 1968; or MANAGEMENT REVIEW, May 1969, pp. 67-68.

This article briefly summarizes a few techniques that can be used to provide safeguards against espionage. They are: guard patrols, ultrasonic alarms, scrambling of telephone transmitted information, and cables that sound an alarm if punctured.

*(8340)*70*ab*cb*da*ep
"Security in Communications, Excerpts from 15th Annual Seminar." INDUSTRIAL SECURITY, Vol. 14, No. 4, pp. 20-29.

*(8350)*73*ab*ak*cc*dg
"Security in Data Processing." DATA PROCESSOR, IBM Corporation, February 1973, pp. 12-14.

*(8360)*73*af*bg*cc*cd*dg*gg
SECURITY LETTER. 475 Fifth Avenue, New York, New York 10017, (Biweekly Newsletter).

This is a biweekly newsletter about security problems. The letter often mentions problems associated with computers. In the August 9, 1971 issue, a two page supplement listed forty commonly found deficiencies in the security of computer centers.

*(8370)*70*ab*bc*cd*da*dc*gf*jf*nd*x1
"Security Men Thrive on the Wages of Fear." BUSINESS WEEK, 20 June 1970, pp. 112-114.

Security service companies and security equipment manufacturers are doing a booming business despite the current business slump. Large corporations such as Westinghouse have entered the market, but so have some questionable fast-buck operators. The article is primarily concerned with security alarms for commercial and home use, and the companies that manufacture or sell them. A few computer security problems and a double-door access control device, marketed by Louis Scoma of Data Processing Security Inc., are briefly discussed.

*(8380)*69*ad*cb*dg*ed*gh*hb*kb*mh*nq
"Security of Classified Information in the DIS ANSRS System." DIA: C-3663/MS5, Defense Intelligence Agency, 14 February 1969, (Classified).

*(8390)*70*af*cb*cc*cd*dg*lb
"Security of Computer Systems as Major Problem for 1970's." GOVERNMENT SECURITY AND LOYALTY, Bureau of National Affairs, Washington, D.C., 25 September 1970.

Dr. Maurice Hellmer, of the Defense Intelligence Agency, discusses six major threats to time-shared computers. They are: personnel, physical security, software, hardware, remote terminals, and administrative procedures.

*(8400)*71*ab*cd*da*dc*fg*fk*fz*ge*gf*ii*jf*jg*jh*x2
"Security of the Computer Center." EDP ANALYZER, December 1971, pp. 1-13.

This report focuses on the following physical protection aspects of the computer complex: physical access control (guard system, man-trap entrance, color coded and magnetic badges, keys, electronic push-button locks, building design); automatic smoke detection (under-floor and above-ceiling sensor arguments, air flow considerations); automatic fire suppression (Halon 1301, carbon dioxide, and water system advantages and disadvantages); building design and maintenance (limit room size, water drainage, water-proof ceilings); magnetic and radar interference (destructive capabilities); air conditioning, electrical power, and lighting backup (power blackout frequencies, protection alternatives); and bomb threat procedures, evacuation plans, and security training of personnel (bomb threat emergency procedure checklist, fire drills). Although nothing new is presented, this report gives a good brief summary on most aspects of physical protection.

*(8410)*71*ad*cb*cc*cd*dg*gg*gh*nb*ng*nh*no*x4
"Security of the TACC Data Base Study (Description of Automatic Data Base Security Techniques)." ESD-TR-71-370-vol-1, Hughes Aircraft Company, Fullerton, California; or AD-735 728, National Technical Information Service, Springfield, Virginia 22151, October 1971, 149 pp., $3.00.

The results of a survey of hardware, software, and procedural techniques used in current and proposed computer systems are presented. The security requirements, system environment and function, and safeguards used are described for each of the 20 government and 14 commercial systems that were examined. A total of 35 hardware, 41 software, and 20 procedural safeguard techniques were found. Some data is also given on the relative cost of developing, using, and maintaining each of these 96 techniques. Qualitative cost estimates were made for some techniques when quantitive estimates were not obtainable. An attempt was made to categorize the 34 systems by their security requirements and the 96 techniques by their applicability to the security requirements."

*(8420)*70*ab*cb*cd*gf*gh
"Security Products Survey." THE OFFICE, August 1970, pp. 44-45.

A wide variety of security devices are briefly mentioned.

*(8430)*70*ac*ai*cc*cd*da*dc*fp*gc*jf*jg
"Security Protection for EDP Files Seen Crucial." COMPUTERWORLD, 26 August 1970, p. S-6.

*(8440)*00*ad*cb*cc*mh
"Security Requirements for Automatic Data Processing." 5200.28, Department of Defense, Arlington, Virginia.

*(8450)*00*ad*cd*ge*gf*nd
"Security Systems." Predicasts Inc., 1101 Cedar Avenue, Cleveland, Ohio 44106, $250.00.

This is a study on firms specializing in providing security services and on security products designed for financial investors. Each product is analyzed as to its advantages, disadvantages, and value. (That's right! It can be yours for only $250.00.)

*(8460)*70*ac*ai*be*cc*de*ma*mc*nj
"Service Bureau Head Gets $85,000 in Bank Suit." COMPUTERWORLD, 11 November 1970, p. 12.

A Minnesota service bureau was awarded $85,000 in its suit against American National Bank. The suit was filed against the bank because the bank failed to provide the bureau with a general ledger bookkeeping system.

*(8470)*49*ab*ca*ep*eq*x2
Shannon, C. E. "Communications Theory of Secrecy Systems." BELL TELEPHONE SYSTEMS TECHNICAL JOURNAL, October 1949, pp. 656-715.

In this classic paper, a mathematical theory of secrecy systems is developed, as well as methods for measuring secrecy system effectiveness. Examples of different types of ciphers are shown. The basic weak points and desirable characteristics of secrecy systems are discussed. Incompatibility among the desirable characteristics are also analyzed. Shannon proved that the necessary and sufficient condition for a cryptographic transformation to be totally unbreakable is that the key must be truly random, at least the same length as the message, and only used once. The theory of cryptology has been significantly improved since this article was written . The paper is highly mathematical and requires a good knowledge of probability theory and modern algebra to be understood.

*(8480)*69*ab*cc*ff
Sheffield, R. J. "EDP Audit Techniques." THE INTERNAL AUDITOR, November 1969.

*(8490)*69*ab*cb*cc*db*fm
Shelton, L. B.; and Reid, E. W. "Unauthorized Intervention in Computer Processing." THE INTERNAL AUDITOR, July 1969, p. 59.

*(8500)*69*ab*ah*cb*ec*ed
Shoshani, A.; and Bernstein, A. J. "Synchronization in Parallel Accessed Data Base." COMMUNICATIONS OF THE ACM, November 1969, pp. 604-607.

*(8510)*72*ac*cc*da*nl*nm*x1
Shuster, Alvin. "British Panel Calls for Legislation to Protect Privacy." NEW YORK TIMES, 13 July 1972, p. 4.

A British government committee proposed a series of measures to safeguard individual privacy. Their 10,000 word report dealt with bugging, computers, secret dossiers, private detectives, and industrial espionage. On computers, the committee recommended a voluntary code by users to guard against abuses. These recommendations were judged inadequate by the National Council on Civil Liberties. The government plans to hear the public's reaction before it acts on the proposal.

*(8520)*00*ad*bc*cd*dc*jf*kb*mh
Siler, James W. "Data Center Disaster." Business Information Services, 690 Building, Dow Chemical Company, Midland, Michigan.

This article describes the computer center disaster experienced by Dow Chemical Company when war protestors invaded its computer complex. Over 1,000 tapes were permanently destroyed.

*(8530)*68*aa*cb*eq
Sinkov, A. ELEMENTARY CRYPTANALYSIS, A MATHEMATICAL APPROACH. Random House, New York, 1968.

*(8540)*70*af*cb*eq
Skatrud, Ralph O. "Computers and Cryptography." In- PRIVACY: LEGAL AND TECHNICAL PROTECTION IN THE COMPUTER AGE, University of California, Berkeley, California, October 1970, 26 pp.

This article gives a basic description of the terms, history, and techniques of cryptography. Many of the techniques described take advantage of computer processing. It is similar to another article by Skatrud entitled "A Consideration of the Application of Cryptographic Techniques to Data Processing" in the 1969 Fall Joint Computer Conference proceedings.

*(8550)*69*ae*ag*cb*da*eq*x3
Skatrud, Ralph O. "A Consideration of the Application of Cryptographic Techniques to Data Processing." AFIPS CONFERENCE PROCEEDINGS, Fall Joint Computer Conference, Vol 35, 1969, pp. 111-117.

First, a brief history is given on the development of cryptographic techniques from the 15th thru the 20th centuries. Then two digital cryptographic techniques which may have potential applications in data processing systems are described in detail. The first is a method of digital substitution analogous to a Vernan double tape system. It uses a controlled combination of data and the contents of two memories. The second method uses a digital route transposition matrix that employs a combination of row and column transposition under memory control.

The author describes these two cryptographic techniques in sufficient detail to enable the reader to clearly understand how they would be implemented in hardware or software. He presents in mathematical terms the probability of each method being deciphered without knowledge of the cryptographic key or contents of the message. Both methods are theoretically unbreakable if one follows the author's restrictions on maximum message length and maximum time between necessary changes of the keyword. Possible ways of achieving key leverage in each ciphering process are also explained.

*(8560)*70*ab*cb*da*eq*x3
Skatrud, Ralph O. "Cryptographic Techniques in Data Processing." COMPUTER SERVICES, July 1970, p. 13.
This article is similar to another article by Skatrud entitled "A Consideration of the Application of Cryptographic Techniques to Data Processing" in the 1969 Fall Joint Computer Conference proceedings.

*(8570)*73*ac*ai*bb*bd*cc*db*dd*mk*x3
Smalheiser, Marvin. "Accuracy of L.A. Vote System Challenged." COMPUTERWORLD, 9 May 1973, p. 5.
The accuracy of the Los Angeles computer punched card voting system has been challenged by Baxter Ward, who was elected to the L.A. County election board of supervisors last fall. He wants an extensive manual recount to check against the computer count. Ward became suspicious when a check of the votes he received in the primary election last year showed thirty-four instances where identical vote totals were reported for successive precincts by the computer. In some cases, he said, two precincts in a row reported an identical total for him or his opponent. In some cases three precincts in a row and in one case four in a row reported the same figures. The mathemetical probability of a four in a row sequence was determined to be less than one in a million. A check of another contest in an earlier 1970 election showed a similar unique coincidence of identical figures.

*(8580)*73*ac*ai*cc*dg*fc*ff*kd*x2
Smalheiser, Marvin. "Auditors Get Word - Gain Management's Confidence." COMPUTERWORLD, 20 June 1973, p. 3.
This article presents some of the recommendations made at the first National EDP Auditor's Conference. Joseph J. Wasserman of Computer Audit Systems called EDP auditors "the world's worst salesmen". He told them they must start selling themselves to management, and get needed resources to work with, or else continue to be severely inhibited in their efforts to monitor computer operations. The need for standards for EDP auditors was another basic theme of the conference. William H. Murry of IBM urged auditors to independently access the risk of

fraud, recommend action, and provide visibility of the level of risk. Another speaker warned auditors against getting too technically involved.

*(8590)*73*ac*ai*ba*cb*cc*cd*dg*fx*x2
Smalheiser, Marvin. "Be Safe - Try to Break Your System." COMPUTERWORLD, 6 June 1973, p. 1.

Last year Jerry N. Schneider stole more than $1 million worth of electronic equipment from Pacific Telephone and Telegraph Company simply by pushing the right beep-tones on his touch tone telephone, and picking up the equipment at PT&T's shipping docks early in the morning before warehouse crews arrived. He pleaded guilty to one count of grand theft (other charges were dropped), served forty days of a sixty day sentence, was released on probation for three years, and is now a systems consultant for EDP Security Inc., a company he helped organize. Schneider believes that the best way to develop confidence in a system is to try to break it. He recommends the following precautions: establish a frame of mind that you are going to tighten security; look around, talk less, and listen more; make sure there is adequate physical security; be assured of the integrity of employees; provide a system of checks and balances to insure the integrity of both the input and output data; and use a data scrambler to stop unauthorized data taps. Schneider also suggests the use of host computers or minicomputers, set up alongside a computer, to watch the programs and control accesses.

*(8600)*72*ac*ai*ba*cb*cc*cd*da*hn*ii*kf*lb*x1
Smalheiser, Marvin. "Computer 'Accomplice' in Thefts." COMPUTERWORLD, 16 February 1972, p. 1.

Jerry Schneider, a 21-year-old UCLA engineering student, studied Pacific Telephone and Telegraph's computer system and learned enough to place commercial orders for equipment simply by punching the right beep-tones on his own touch tone phone. He then illegally ordered over $1 million worth of electronic equipment and sold it through a dummy firm operated by ten associates. The equipment and bills of lading were picked up at PT&T's shipping docks early in the morning before warehouse crews arrived.

*(8610)*73*ac*ai*ba*bb*bf*da*db*df*hd*hj*ic*ih*kd*md*me
*no*x2
Smalheiser, Marvin. "DP Crime - Who Does It?" COMPUTERWORLD, 30 May 1973, p. 2.

This article quotes testimony by Donn B. Parker of Stanford Research Institute before a State Assembly committee hearing. Parker did a study on 24 recent computer crime cases involving local, state, and federal governments. The study indicates that the computer criminal is likely to be a white collar male, 18 to 30 years old, highly rational, and deviating only in small ways from his peers. A high frequency of collusion among perpetrators was also found. The type of crimes that were studied are: vandalism - 4, address list theft - 5, check manipulation - 4, payroll manipulation - 3, confidentiality violation - 4, illegal sale of EDP services - 2, and vote counting fraud - 2. The perpetrators were: 16 EDP employees, 2 elected officials, 2 citizens, a private businessman, a claims manager, a welfare employee, and a policeman.

*(8620)*73*ac*ai*bb*cc*db*mc*nj*x1

Smalheiser, Marvin. "Equity Investor Suit Says IBM Safeguards Lacking." COMPUTERWORLD, 16 May 1973, p. 1.

This article presents some of the charges made in a class action suit, filed by five Los Angeles residents, which seeks over $4 billion in damages resulting from the Equity Funding scandal. The suit charges that IBM contributed to the Equity Funding scandal by failing to design mechanical and procedural means of detecting fraudulent inputs into their equipment. Alvin B. Green, the attorney who filed the suit said, "Were it not for the equipment being manufactured as presently constituted and IBM failing to advise the public of the problem, fraud would never have arisen."

Almost every charge in this suit is preposterious. Either the plaintiffs are incredibly ignorant, or they are hoping the jury who decides their suit can be convinced to believe these absurd charges. For some actual facts on the scandal, read two articles by Alan Taylor in the April 25 issue of COMPUTERWORLD.

*(8630)*73*ac*ai*cc*db*fs*kd*nl*x2

Smalheiser, Marvin. "Safford Summons User Group to Rally Against DP Fraud." COMPUTERWORLD, 20 June 1973, p. 1.

Herbert B. Safford, international president of the Data Processing Management Association (DPMA), believes that the time has arrived for computer professional associations to speak out on computer assisted fraud and promote efforts to prevent it. Enforcement will have to come either through a strongly enforced code of ethics, where members found responsible for fraud are censured by all associations throughout the industry, or through licensing of DP personnel backed by legal prosecution. Safford favors the latter approach providing it is well thought-out. He also suggested that computer user associations can assist EDP auditors by advising them on how to protect computers, programs, and data. These associations should also develop guidelines for top management review of EDP installations.

*(8640)*73*ac*ai*bc*cd*fv*gc*jg*me*na*x2
Smalheiser, Marvin. "Water Damage Avoided: Plastic Protection Proves Worth in Fire." COMPUTERWORLD, 10 January 1973, p. 1.

A $1,200 investment in plastic covers protected about $15 million worth of computer equipment during a fire which partially destroyed a block-square building in Sacramento, California. The building was occupied by the California National Guard and the State Department of Motor Vehicles. The computer equipment was located on the second floor. Covers were put on the equipment before water was able to seep through the ceiling. The fire was on the fifth floor of the six-story building. Computer data files were removed from the building when it appeared that the entire building might be lost. Four days after the fire normal operations resumed.

*(8650)*73*ab*cc*fm*nb
Smith, Hendrick S. "Cost Control for Computers, Applying Bread-and-Butter Principles." BUSINESS HORIZONS, February 1973, p. 73.

*(8660)*71*ad*ak*cb*eq*gh
Smith, J. L. "The Design of Lucifer, A Cryptographic Device for Data Communications." RC-3326, IBM Corporation, White Plains, New York, 15 April 1971.

For more information See "An Experimental Application of Cryptography to a remotely Accessed Data System" by W. A. Notz and J. L. Smith.

*(8670)*71*ad*ak*cb*ep
Smith, J. L. "Hardware Implementation of a Cryptographic System." IBM TECHNICAL DISCLOSURE BULLETIN, Vol. 14, No. 3, August 1971, pp. 1004-1008.

This article describes a cryptographic system developed by IBM. It is designed to provide enciphering and deciphering of messages between a remote terminal and the computer. Both software and specially designed hardware are used to mechanize the system.

*(8680)*72*ae*ak*cb*ep
Smith, J. L.; Notz, W. A.; and Osseck, P. R. "An Experimental Application of Cryptography to a Remotely Accessed Data System." PROCEEDINGS OF THE ACM, 1972, pp. 282-298.

A cryptographic system developed by IBM is described. It is designed to provide enciphering and deciphering of messages between a remote terminal and the computer. Both software and specially designed hardware are used to mechanize the system.

*(8690)*68*ab*cc*df*dg*ff*fg*fh*fk*fl*fu*fo*fp*fq*kd*x3

Smith, Troy J. "Internal Auditing of Controls for Data Processing Department." THE INTERNAL AUDITOR, May 1968, pp. 44-50.

This paper discusses balancing controls for off-line computer systems. Balancing controls are essential internal controls needed to assure receipt of all data, accuracy of processing, reliability of completed reports, reduction of rerun costs, and efficiency of operations. There are two significant control features: physical control over the physical movement of data, and record (paper) control over the movement of data. With respect to physical movement of data, controls should include: a record of input data received from source, issued to operations, returned from operations, returned to source; and a record of output data received from operations and distributed to users. Some commonly used types of program controls for output are: columnar totals, hash totals, and record counts. For error controls: cross footing, limit checks, check points, zero balances, sequence checks, and audit checks are commonly used. Document counts, and control totals of hours, rates, etc. are most frequently used for data input control.

Working from the above externally established controls, an independent data control center should: develop complementary records which will trace physical and machine movement of data; develop methods of verifying the accuracy of data as it is processed from program to program; schedule and release source data to operations for processing; verify return of source data, output data, records, and reports from operations when processing has been completed; maintain records of output users and verify delivery of output to these users; maintain complete documentation records of machine programs and operations; release programmed computer instructions, punched card files, and magnetic tape files to operations only when needed to process current data; index, label, and sort all card files, tape files, and programmed instructions in a secure library facility; develop retention schedules for all tape and card files; and provide personnel to assist operations in resolving machine, program, or data difficulties. The author also presents a list of ten questions that should be answered to test whether or not a data control system provides adequate protection. Although this article is somewhat out-of-date, most of the controls discussed are still very useful.

*(8700)*69*ab*cc*dg*ff*hk*hp*kb*kd

Smith, Troy J. "Internal Controls for Data Processing." COMPUTERS AND AUTOMATION, November 1969.

Audit and control methods for input data, and optimal check points for controlling work flow are discussed.

*(8710)*69*ab*cc
Smith, Troy J. "Workable DP Controls." COMPUTERS AND AUTOMATION, November 1969.

*(8720)*70*ac*bb*be*cc*dg*ff*hm*kd*ne*x1
Smith, William D. "Controls Haven't Caught Up to Boom in Computers." NEW YORK TIMES, 22 February 1970, Sect. 3, p. 11.

When the celebration of the New York Mets baseball championship had passed, many businessmen discovered that enthusiastic employees had tossed valuable computer tapes and punched cards out office windows in a tribute to their heros. This and other examples demonstrate inadequate control over most business computers. One reason for the gap between desire and performance is that most traditional auditing personnel have no knowledge of computers while most computer personnel are ignorant of auditing. Joseph Wasserman, president of Computer Audit Systems, recommends: keeping unauthorized personnel out of the computer room, off-site file backup, and definite separation of duties among employees.

*(8730)*71*ac*cc*da*f1*hc
"Software Protection: Trade Secret Laws, Not Patents, May Be Way." ELECTRONIC NEWS, 15 November 1971, Sect. 2, p. 34.

*(8740)*70*ab*cc*da*db*de*ft
Sohn, D. "Screening for Drug Addiction." PERSONNEL, July 1970.

*(8750)*71*ab*cd*df*gd*jh
"Some Quick Tips for Surviving Brownouts." FACTORY, May 1971, p. 26.

*(8760)*70*ab*cc*cd*x1
"Some Tips on Computer Security." INDUSTRY WEEK, 3 August 1970, p. 22.

This brief article presents several security recommendations by Richard F. Cross, security officer of Bank of New York. They are: be certain that remote terminals have controlled access to the computer; install self-contained air conditioning; only allow authorized personnel in the computer room; conduct extensive pre-employment interviews; set up an emergency plan for immediate securing of all tapes, programs, and other valuables; and review your insurance coverage to consider insuring against business losses resulting from computer problems.

*(8770)*72*ab*cb*cc*cd*dg*eh*fv*fw*hc*nb*nf*x3

Sorensen, J. L. "Common Sense in Computer Security." JOURNAL OF SYSTEMS MANAGEMENT, April 1972, pp. 12-14.

Suddenly everyone is concerned about computer security. The risk is very real, but more common sense and less panic on the part of management are needed today. It's almost impossible to protect against intentional destruction of computer equipment and computerized data files. It is beginning to appear that employees are becoming the biggest security risk. Unfortunately, most of the steps toward greater security involve significant cost. For large computer installations, substantial expenditures are appropriate, but for the majority of small and medium size installations less expensive alternatives are needed.

The author suggests a two step approach for implementing a security program. First, assess the installation's security status; identify measures needed to provide fairly complete security; evaluate each in relation to the risk protected against and the cost involved; and select those with obvious justification on a common sense approach. Second, develop detailed contingency procedures for quick recovery in the event computer equipment or files are destroyed. Recovery procedures do not have to be expensive. Usually it is not difficult to locate other installations in the vicinity with compatible equipment and work out a backup agreement. However, this is not enough. A backup system must be periodically tested to insure that it is truly compatible, and that it can handle the extra workload.

The author also made a few flexible recommendations to prevent and detect theft. A file owner should scramble information in valuable data files that have a significant risk of being stolen. It is useful to insert "decoy" names in important name and address files. Unauthorized direct mail solicitations to the "decoy" addresses will indicate that the file was stolen.

*(8780)*72*ac*ai*bb*cc*db*fh*hk*if*ka*mf*nj*nl*nm*x2

Sorkin, Michael D. "State Sued on Data Bank: Privacy Invasion Charged." COMPUTERWORLD, 27 September 1972, p. 1.

A class action lawsuit has been filed in Des Moines, Iowa aimed at prohibiting all Iowa law enforcement officials from keeping either computerized or manual identification files on arrested persons with no criminal convictions. The suit claims that Iowa criminal identification records are sent to the FBI where they are classified and exchanged with law enforcement agencies, other government agencies, and several classifications of private employers including railroads, banks, and insurance companies. Once the identification records leave the FBI's possession, there is no restriction on their use. Computerization of Iowa's criminal records has become controversial because LENCIR, a Des Moines subsystem of the state computer network, has been keeping secret files on "persons of interest" and labeling the suspects as "known criminals" even though many have never been convicted or charged with a crime.

*(8790)*72*ac*ai*cc*da*db*hd*ka*nl*nm*x3

Sorkin, Michael D.; Lundell, E. Drake; and Bride, Edward J. "Privacy Issues Grow More Lively." COMPUTERWORLD, 20 December 1972, pp. 1-2.

This is one of the most recent articles describing what is occurring in the areas of personal privacy and government regulation of computer data banks. Sorkin discusses a freeze asked on LEAA funds, Lundell describes a newly formed Canandian Data Bank Committee, and Bride reveals that the use of the Social Security number as a universal identifier is doubtful.

A report by the Lawyers Committee for Civil Rights Under Law, said the Law Enforcement Assistance Administration (LEAA) of the U.S. Justice Department should halt its spending on criminal justice information systems until legislation providing privacy safeguards is adopted. Several serious privacy abuses by the LEAA are revealed.

The Canadian government has established a special interdepartmental committee charged with drawing up privacy-protection rules for computerized databanks and is considering use of an ombudsman to make sure that these rules are enforced. The rules will first be applied to the government's own databanks.

A U.S. government committee is leaning toward the conclusion that the Social Security number would not make a good universal identifier number. It is neither unique or universal. Many migratory people have several SS numbers and cases of two or more people having the same number aren't that uncommon. The very existence of a universal identifier being in the public's interest is also being questioned.

*(8800)*68*ab*cc*ff

Soudler, I. J. "Plain Talk About Auditing in an ADPS Environment." JOURNAL OF ACCOUNTANCY, April 1968, pp. 43-47.

*(8810)*68*ab*cc*da*es*ka*mb*nm

Sprague, C. R.; and Ness, David N. "Privacy and a National Data Bank." BANKING, June 1968, pp. 50-51.

The authors discuss how databanks do not necessarily entail an invasion of privacy.

*(8820)*68*ab*cc*da*es*ka*mb*nm

Sprague, Richard E. "Personalized Data Systems." BUSINESS AUTOMATION, October 1969, p. 47.

*(8830)*70*ab*cc*da*ka*mb*nm
Sprague, Richard E. "The Invasion of Privacy and a National Information Utility for Individuals." COMPUTERS AND AUTOMATION, January 1970, pp. 48-49.

The author concludes that the invasion of privacy problem can only be prevented by forming a national information utility for individuals.

*(8840)*00*af*cc*dg*fy
"The St. Paul Data Processing Policy." St. Paul Insurance Companies, 385 Washington Street, St. Paul, Minnesota 55102.

*(8850)*73*ae*ag*cb*da*eq*x3
Stahl, Fred A. "A Homophonic Cipher for Computational Cryptography." AFIPS NATIONAL COMPUTER CONFERENCE PROCEEDINGS, Vol. 42, 1973, pp. 565-568.

Computational cryptography, which deals with the storage and processing of sensitive information in computers, is distinguished from communication cryptography. The major difference between these two types of cryptography is that computational cryptography must allow the normal editing functions of deleting, inserting, and moving strings of information to occur within the enciphered file without going through a deciphering and reenciphering process for the entire file after every edit. Because computational cryptography techniques must have this additional editing capability, they can't provide the extremely high security of communication cryptography techniques.

The author states that most computation cryptography techniques are either too computationally complex to be implemented or provide ciphers that are too easily broken. He then describes a homophonic cipher that is extremely easy to implement and provides good security by destroying almost all frequency information of the message. The security of the cipher can easily be varied, but more securely encoded messages require greater amounts of storage space. Unfortunately, the homophonic cipher is quite vulnerable to the problems of limited message syntax and partially known messages.

*(8860)*70*ac*ai*bd*be*cc*dd*de*hv*me*mk*nj
"State Bans Punched Card Voting as City Sues Vendor, Even Weather a Problem." COMPUTERWORLD, 30 December 1970, p. 3.

*(8870)*70*ab*cc*fs
Stephan, R. W. "Setting Up a Manual of Policies and

Procedures." DATA MANAGEMENT, September 1970, pp. 93-95.

*(8880)*69*ab*cb*cc*cd*da*hw
"Sticking Up a Computer." INNOVATION MAGAZINE, No. 7, 1969.
Rapid growth in the computerization of business operations has caused EDP personnel to give little concern to the security of their systems.

*(8890)*70*ab*cb*cc*da*db*mc*ng
Stiefel, Rudy C. "A 'Checkless' Society or an 'Unchecked' Society?" COMPUTERS AND AUTOMATION, October 1970, pp. 32-25.
It will be very difficult for computers to automate the monetary aspects of our lives. It is now technically feasible to build a system that would make a cashless and checkless society possible, but inadequate computer safeguards against theft and fraud will probably prevent such a system from being developed.

*(8900)*70*ad*cb*cc*da*db*mc*ng
Stiefel, Rudy C. "Proceedings of Carnahan Conference on Electronic Crime Countermeasures." PB-190 589, National Technical Information Service, Springfield, Virginia 22151, 16 April 1970.
The author believes that it will be very difficult for computers to automate the monetary aspects of our lives. It is now technically feasible to build a system that would make a cashless and checkless society possible, but inadequate computer safeguards against theft and fraud will probably prevent such a system from being developed.

*(8910)*71*ab*cc*ff
Stolle, C. D. "Computer-Based Audits." MANAGEMENT ADVISOR, May 1971, pp. 38-43.

*(8920)*68*ad*cb*ed*ef*gh*x1
Stone, M. G. "TERPS: File Independent Inquiries." THE COMPUTER BULLETIN, March 1968, pp. 286-289.
This article describes the TERPS system which allows protection at the record level within files. A descriptor with each file contains a security code for the fields. The term "access" is divided only into "yes" or "no" capabilities. Access restrictions are based on terminal location, security level, and password.

*(8930)*71*ae*ca*cb*eb
Strnad, Alois J. "The Relational Approach to the Management of Data Bases." IFIP Congress, 1971.

*(8940)*69*ac*ai*bc*cc*cd*dc*jf*mj
"Students Demolish Computer Center." COMPUTERWORLD, 26

February 1969, p. 1.
The destruction of the Sir George Williams University's computer center is described.

*(8950)*71*ac*ai*bc*cd*dc*jf*mj
"Students Protest Lads, Occupy Center." COMPUTERWORLD, 24 February 1971, p. 4.

*(8960)*70*ad*cb*da*ep*md
"Study of Electronic Handling of Mail." AD-715 124, National Technical Information Service, Springfield, Virginia 22151, June 1970, 83 pp.
Possible security techniques in transmitting information electronically from one site to another are analyzed.

*(8970)*72*ab*cc*df*dg*nb*nf*x3
"Subtle Problems - Human Error, Accidents, Responsive Controls - May Be the Most Critical for EDP Installation, Says Diebold Executive." MANAGEMENT ADVISOR, September 1972, pp. 10-11.
Theodore J. Freiser, senior vice president of John Diebold & Associates (a management consulting firm), believes that human error, accidents, and lack of responsive controls are just as lethal security problems as are the well publicized examples of sabotage, embezzlement, and theft. He recommends the following procedure for implementing or improving a security program. First, determine what inherent risks exist. Second, establish the company's potential vulnerability to these risks. Third, estimate the cost and business implications of the materialization of these risks. The money spent to reduce a particular risk should be closely related to the product of the above two steps. Fourth, determine the practical opportunities that exist to reduce the vulnerability to these risks. This last step includes estimating the cost implications of proposed measures to increase security, and the development of a time-phased implementation plan specifying action, personnel, and equipment involved.

*(8980)*70*ac*ai*cc*da*nj
"Suit Hinges on Programs." COMPUTERWORLD, 16 December 1970.

*(8990)*70*ab*cb*cc*da*hd*nm
"Summary of Recommendations on Operation of Data Banks re Privacy." DATA PROCESSING DIGEST, October 1970, p. 34.

*(9000)*71*ab*cd*df*gd
Summers, Garth E. "Providing Reliable Power for Computer Systems." PLANT ENGINEERING, 7 January 1971.

*(9010)*70*ae*cc*dc*fv*fw
Supp, Robert J. "Catastrophe Prevention Management of the Computer Complex." 6373-60, American Management Association Briefing Session, 13 April 1970.

A disaster protection program for protecting data records is described.

*(9020)*70*ad*cb*ed*ei*el*gh*no
"Survey and Analysis of Major Computing Operating Systems." Comtre Corporation, AD-704 138, National Technical Information Service, Springfield, Virginia 22151, January 1970.

*(9030)*69*ad*cb*eb*ed*gh*no
"A Survey of Generalized Data Base Management Systems." CODASYL Systems Committee Report, May 1969.

*(9040)*73*ac*ai*cc*dg*fa*ff*fg*fi*kd*x1
"System Protection Depends on Well Educated Auditor." COMPUTERWORLD, 28 March 1973, p. 8.

This article presents some comments made by Harvey S. Gellman, president of DCF Systems Ltd., in a speech before the Toronto chapter of the Institute of Internal Auditors. It is necessary to provide good education for the internal auditor to equip him for his role in protecting the security of computer systems. In addition to fraud, the internal auditor must protect his company from loss of availability of its computer. He can best meet his responsibilities if he can review computer programs in the design stage. He should also perform a cost versus benefit analysis to determine the appropriate security for different sets of data. Gellman maintains that a separate audit control group, not under the EDP department, is necessary for adequate separation of duties and controls.

*(9050)*70*ad*cb*cc*dg*ed*ej*el*em*ff*fi*fn*kb*kd*nf*ni
"Systems Auditing and Control: Software and Management Series." S10, Diebold Computer Planning and Management Service, April 1970, 77 pp.

The following four main audit areas are discussed in detail: editing routines to check input validity; controls to disallow concurrent updating of files; logging accesses to files; and restart procedures. Detailed recommendations are also given for developing a good systems and procedures manual. The appendix includes a comprehensive auditing checklist which has many interesting and valuable questions.

*(9060)*70*ab*cc*ff*fu
Tagen, W. G. "Educating the Internal Auditor in EDP." THE INTERNAL AUDITOR, January 1970.

*(9070)*69*ab*cb*cc*dg
Tassel, Coleman J. "Information Security in a Computer Environment." COMPUTERS AND AUTOMATION, July 1969.

*(9080)*73*ac*ai*bb*cb*cc*db*ff*hj*hk*hm*if*kd*mc*x3
Taylor, Alan. "Auditor Negligence, Fear of DP Called Keys to Fraud." COMPUTERWORLD, 25 April 1973, p. 3.

This article and another article in this issue, also by Taylor, provide an excellent detailed description of the computer's role in the great Equity Funding Life Insurance fraud. A few highlights are presented below. Four separate sets of fraudulent actions were being routinely entered on the computerized books, but none of them involved the production of specialized programming by the DP staff until a final attempt to stave off rediscovery was made. These four fraudlent uses were: (1) reopening the previous year's books and adding new input to match corporate aims; (2) accepting falsified input from user departments which created and maintained bogus policies; (3) preparing test files at the instructions of the actuarial department, officially for use in insurance-selling simulation studies, but actually used to create falsified input describing bogus policies; and (4) accepting about thirty-five sets of falsified input documents which resulted in dead policies being revived and their $3,000 to $5,000 value being cashed in through dummy accounts. The last of the above four fraudulent actions was apparently the work of some unknown independent entrepreneur, and not related to the big company-sponsored fraud.

The computer played two important roles in making the fraud possible. It assisted in implementing the fraudulent figures, and the auditor's fear of the computer was used by the conspirators to prevent the normal level of auditing from taking place. Equity encouraged auditors to request hard copies of computerized records they wanted to inspect the next day. The auditors turned over these lists the preceeding evening which gave the conspirators overnight to produce fake documents. The fraud had been in successful operation for over three years. An employee finally exposed the fraud which auditors were never able to detect. Over $1 billion in bogus insurance policies was involved.

*(9090)*70*ac*ai*cc*fz*nj
Taylor, Alan. "Directors' Fortunes Being Risked by DP Department." COMPUTERWORLD, 23 December 1970.

This article reports on a discussion between the author and Roy Freed and Robert Bigelow, two lawyers who specialize in the computer field. The increase in legal suits between manufacturers and users, legal contract forms, and the liability of management and corporate directors are briefly discussed.

*(9100)*73*ac*ai*bb*cb*cc*db*ff*hj*kd*mc*x3
Taylor, Alan. "The Great Fraud: DP or Not DP?" COMPUTERWORLD, 25 April 1973, p. 1.

This article and another article in this COMPUTERWORLD issue, also by Taylor, provide an excellent detailed description of the computer's role in the great Equity Funding Life Insurance fraud. The purpose of this article is to show that the fraud, which has been called the "first great computer fraud in history", is really not a computer fraud. Many stories in several national journals implicitly or explicitly condemned the data processing department as guilty of fraud and/or criminally incompetent. This article analyzes the WALL STREET JOURNAL and NEWSWEEK stories in detail, and convincingly shows that the Equity DP department was most likely not guilty of any fraudulent activity. It appears that inadequate auditing procedures were mostly responsible for the fraud's success. The handling of major bogus insurance policies was not integrated into the computer operations until two years after the fraud started. Special programming to support the fraud was only used to stave off the fraud's rediscovery. Although, the DP department could have easily been used to support and promote the fraud, the roof had fallen in on Equity before this occurred.

*(9110)*73*ac*ai*cc*db*fb*fs*kd*nl*x2
Taylor, Alan. "Must In-House DP Be Banned as Too Open to Fraud?" COMPUTERWORLD, 13 June 1973, p. 19.

The author is concerned about the possibilities of computer fraud initiated and controlled by corporate executives who oversee the DP operations. He is especially concerned because he feels that executive-controlled computer fraud is extremely difficult to detect. The Equity Funding fraud is an excellent example. Taylor states that DP personnel must become more professional and not let their loyalty to the firm affect the way data processing is handled. The only other alternative, and a less desirable one, is to ban in-house DP and require all DP to be done by service bureaus or some other independent DP organizations.

*(9120)*73*ac*ai*cb*cc*dg*el*ff*kd*ng*x3
Taylor, Alan. "Two Instruction Streams Can Enhance Auditability." COMPUTERWORLD, 11 July 1973, p. 11.

Computers with two instruction streams (Burroughs 5000 and Control Data 6600) can provide better managed and controlled programs. The second instruction stream can be used to provide an audit trail of the first stream, which is used for executing programs. Until recently, the cost of devoting one of the instruction streams solely to providing an audit trail was prohibitive. However, about a month ago Control Logic Inc. introduced a mini-computer, based upon a central processor on a chip, which can provide the needed second instruction stream for only $2,000. This mini-computer instruction stream can provide audit trails on a program's instruction sequence without interfering with the program's functions in any way.

*(9130)*70*ab*cb*cc*gg*lb*mb
Taylor, R. L.; and Feingold, R. S. "Computer Data Protection." INDUSTRIAL SECURITY, August 1970, pp. 20-29.

The authors discuss the lack of data security, particularly that related to remote-access, time-shared computers. They conclude that these security problems will be technically solved within the next five years, and that the solution will lead to the establishment of a national databank.

*(9140)*00*ad*cb*cc*dg*fx*mh
"Techniques and Procedures for Implementing, Deactivating, Testing and Evaluating Secure Resource-Sharing ADP Systems." 5200.28-M, Department of Defense, Arlington, Virginia.

*(9150)*71*ab*ba*cb*da
"Telephone Used in Computer Theft." BUSINESS AUTOMATION, 1 April 1971.

*(9160)*70*ab*bb*cc*db*hj*kd
"The Thief Inside." THE OFFICE, August 1970, pp. 12-15.

Common types of embezzlement are discussed, and a program of preventative measures is given for both small and large companies. Many actual embezzlement cases are presented. However, there is little material on computer-related embezzlements.

*(9170)*70*ab*cb*cc*cd*da*hb*kb*mf
"The Thief Outside." THE OFFICE, August 1970, pp. 35-38.

The security program at Sargent and Greenleaf, a lock manufacturer, is discussed. This company uses very elaborate precautions to protect their files, records, and computer. Some security recommendations are given.

*(9180)*69*ab*cc*df*nc
Thomas, D. R. "On Reliability Strategy in Electronic Data

Processing." MANAGEMENT ACCOUNTING, January 1969, pp. 39-42.

*(9190)*71*ab*cc*dg*ed*eh*ej*el*ff*fh*fl*kd*lb*ni*x3
Thorne, Jack F. "Internal Control of Real-Time Systems." DATA MANAGEMENT, January 1971, pp. 34-37.

This article discusses aspects of internal control which relate to input controls, processing controls, stored data controls, and output controls, and are peculiar to real-time processing. The author suggests the following data input controls: each terminal user has his own key, code, or card for access control and identification; all transactions are checked for validity by the computer and all errors are reported; and a listing of all transactions is sent to a supervisor for his review and approval. Programmed checks may be used to: detect loss or nonprocessing of data; determine that arithmetic functions are performed correctly; determine that all transactions are posted to the proper record; and ensure that all detected errors are corrected. Stored data controls should include: periodic printing of files on a surprise basis; documentation of all file changes; restriction of file changes to specified terminals; use of test transactions to establish the integrity of files; and verification of data in files by checking appropriate data maintained outside the system. For output control, a permanent record of all types of output created (an output log) is desirable. This also applies to data displayed on terminal cathode ray tubes. The author concludes by presenting an internal control checklist applicable to real-time systems only. The checklist contains sixteen questions which imply similar to the ones described throughout this article. The checklist is to be used in conjunction with, rather than a replacement for, checklists on batch processing systems.

*(9200)*72*ab*cb*dc*gc*jf*x3
Tiffany, W. D. "Are Computer's Files Vulnerable to Magnets?" THE OFFICE, September 1972, p. 51.

The author, manager of the security systems research program at Stanford Research Institute, presents his research findings on the vulnerability of magnetic tapes to magnets. The results show that all small magnets (200-2000 gauss) and almost all large magnets must be held within one inch of a magnetic tape to sufficiently distort data to cause computer malfunctions. Even the smallest magnets can destroy magnetic tapes, but only if held at the surface of a tape. A magnet's field of intensity varies inversely with the cube of the distance from the magnet. For these reasons, the author believes that the tape's canister will protect it from all but quite large magnets. The stories about small magnets being able to quickly erase entire tape libraries are definitely untrue.

*(9210)*67*ab*ah*cb*cc*da*mf*nm*x1
Titus, James P. "Security and Privacy." COMMUNICATIONS OF THE ACM, June 1967, pp. 379-380.

Highlights of the 1967 Spring Joint Computer Conference are presented. However, many of the problems discussed at this conference are now obsolete or require additional considerations. The protection of communication lines was considered to be the number one technical problem. (Today's major technical problem is access control of shared files.) Harold E. Peterson and Rein Turn, of RAND Corporation, presented an interesting paper describing various methods of penetrating a time-shared computer system. Bernard Peters, of the National Security Agency, described a software security system that was just being implemented in NSA's multiple-access message-switching system. Robert Galati, director of the New York State Identification and Intelligence System, discussed problems of protecting individual privacy in criminal information systems. Alan Westin also discussed problems of individual privacy protection.

*(9220)*71*ae*cb*dc*dd*em*fv*lb
Tonik, A. B. "Recovery of On-Line Data Bases." PROCEEDINGS OF THE ACM, 1971, pp. 103-111.

*(9230)*69*ad*ak*cb*ed*gh*lb*x1
"TSS/360 Quick Guide for Users." X28-6400-0, IBM Corporation, White Plains, New York, May 1969.

One of IBM's efforts to provide file access control is presented. The system allows specification of access restrictions on a user-by-user basis with modes: read, read/write, unlimited, and restricts.

*(9240)*70*ad*ak*ca*da*eq
Tuckerman, Bryant. "A Study of the Vigenere-Vernam Single and Multiple Loop Enciphering Systems." RC 2879, IBM Corporation, White Plains, New York, 14 May 1970.

*(9250)*72*ad*aj*ca*cb*cc*nn*x1
Turn, Rein. "A Brief History of Computer Privacy/Security Research at RAND." AD-748-917, National Technical Information Service, Springfield, Virginia 22151; or P-4798, RAND Corporation, Santa Monica, California 90406, March 1972, 9 pp.

This report briefly describes the research efforts of RAND employees in computer security and privacy since 1953. RAND scientists made significant pioneering contributions in 1963 to 1967 by delineating the data security/privacy problem and formulating technical safeguards. Mr. Ware organized the first session on data privacy/security ever held at a computer conference (AFIPS - 1967 SJCC). Peterson and Turn presented one of the first papers on technical aspects and systems implications of data security. RAND also established much on the vocabulary of this subject. Harrison produced two well known annotated bibliographies on computers and privacy. Other researchers demonstrated the practicality of system-penetration as a tool for evaluating security safeguards. Currently, theoretical and technical aspects on the protection of privacy in "personal information" databanks are being investigated.

*(9260)*73*ae*ag*cb*da*ep*eq*er*nb*x3
Turn, Rein. "Privacy Transformations for Databank Systems." AFIPS NATIONAL COMPUTER CONFERENCE PROCEEDINGS, Vol. 42, 1973, pp. 589-601.

This paper briefly reviews relevant characteristics of the following classes of privacy transformations: compression, monoalphabetic substitution, polyalphabetic substitution, transposition, and composite transformations. Irreversible privacy transformations for statistical databank systems are also briefly described. The suitability of a particular class of privacy transformations for application in a communication network or in the files of a databank depends upon: the relevant characteristics of the particular application; the inherent characteristics of the class of privacy transformations used; and the technical characteristics of the system that implements the application and the privacy transformation. All these characteristics are listed and briefly discussed. Characteristics of different natural languages and computer languages which affect the security of privacy transformations are also presented.

Next, a brief discussion is given on determining the secureness of a given privacy transformation. This is followed by a discussion on initial and recurring cost considerations. Major differences are shown in the application of privacy transformations to communication links and to data files. The author concludes by stating that, "Measures of the amount of security provided by different mechanisms, measures of the value of information, and the tools for tradeoff analysis, are now beginning to crystalize into a discipline of data security engineering. It is likely that in the next few years the design of data security systems will be much less of an art." Although this paper discusses many privacy transformation considerations in detail, it is not mathematical and is easily readable.

*(9270)*70*ad*aj*cb*da*ea*el*ep*eq*ha*ii*je*lb*x2

Turn, Rein; and Peterson H. E. "Security of Computerized Information Systems." P-4405, RAND Corporation, Santa Monica, California 90406, July 1970, 9 pp.; or AD-709 366, National Technical Information Service, Springfield, Virginia 22151.

The first half of this paper discusses the vulnerabilities of remotely accessed computers, while the second half presents a good brief discussion on cryptographic techniques for protecting information stored in files or transmitted over telephone lines. First, each of the following are discussed in a few paragraphs: basic tasks of the operating system; persons masquerading as authorized users; wiretapping; circumvention of operating system controls; physical penetration of computer center; improving the operating system; real-time monitoring; positive identification; and protected communication lines. Then two types of cryptographic transformations are described, followed by discussions on: the needed hardware for encoding or decoding; weak points that enable encrypted messages to be broken; properties of computer languages that make breaking the encrypted message easier or more difficult; work factors; and synchronization and communication control-word problems.

*(9280)*72*ad*ae*ag*aj*cb*cc*da*db*dc*eq*fd*ka*lb*nb*nc *nf*ng*nh*x4

Turn, Rein; and Shapiro, Norman. "Privacy and Security in Databank Systems - Measures of Effectiveness, Costs, and Protector-Intruder Interactions." AFIPS CONFERENCE PROCEEDINGS, Fall Joint Computer Conference, Vol 41, 1972, pp. 435-444; or P-4871, RAND Corporation, Santa Monica, California 90406, July 1972, 36 pp.

During the last several years a variety of techniques have been developed for protecting sensitive information against unauthorized access or modification. However, systematic procedures for cost-effective implementation of these safeguards are still lacking. This paper attempts to contribute to the formulation of "data security engineering" in the area of personal information databank systems. A model is presented for a personal information databank system which includes the following elements: databank, subject, controller, custodian, collector, user, intruder, and society. The elements of this model need not be unique since multiple roles and overlap in functions are common. Arrows are drawn between certain elements to show that some form of interaction normally occurs between these elements. The right of privacy involves interaction between the subject and the collector or controller elements, while data security involves interaction between the intruder and the databank elements. Threats to data privacy, confidentiality, and security may arise from all elements of this model.

The authors state that databanks can be classified along the following dimensions: public - private, statistical - dossier, centralized - decentralized, dedicated - shared, and off-line / on-line. These classifications permit ranking of databank systems in order of the complexity of their security problems. The authors then develop a rather simple mathematical model which describes economic considerations for database protectors and intruders. The analytic or empirical expressions for this mathematical model are presently difficult to determine, and are often quite sensitive to the particulars of a databank security system and the information protected. However, some advice is given for determining the needed expressions for: the value of information to the potential intruder, -to the subject, and -to the protector.

The objectives of a security system are: to deter a profit-seeking intruder by raising the intrusion cost to a level that reduces his expected profits to an unacceptable level, and to prevent access by intruders not economically motivated through effective access and threat monitoring. Design criteria for security systems must include effectiveness, economy, simplicity, and reliability. Security techniques can be functionally classified as: denying information about the security system (not always desirable), preventing physical or electronic access, detecting intrusion attempts, and maintaining databank integrity. The article concludes by presenting a short discussion on several cryptographic methods, and giving some representative cost figures on a few data access and cryptographic protection techniques.

*(9290)*70*ac*ai*bc*cd*dc*jf*mj

"Twenty Students Take Over DP Center, Promise They Don't Plan Any Damage." COMPUTERWORLD, 25 November 1970.

Twenty students took over the Salem State College computer center in Massachusetts. They held it for ransom until obtaining a satisfactory response from the administration to their list of forty-two demands.

*(9300)*72*ab*cb*da*eq*gh

Twigg, T. "Need to Keep Digital Data Secure?" ELECTRONIC DESIGN, 9 November 1972, pp. 68-71.

A three stage code generator which produces pseudorandom bit sequences is described. The device can provide numerous, easily changed codes, and is easily mechanized with integrated circuits.

*(9310)*70*ac*ai*bc*cd*dc*jf*mj

"Two Arrested in Threat to Destroy DP Center." COMPUTERWORLD, 12 August 1970, p. 1.

Two New York University faculty members were arrested for allegedly threatening to destroy the school's computer center if they were not paid $100,000. Shortly before the threat was made, 150 students had taken over the center. The money was allegedly to be used for bail to free a member of the Black Panther organization.

*(9320)*71*ab*cc*ff

Tyrnauer, S. "Computerized Auditing Methods: An Evaluation." THE INTERNAL AUDITOR, January 1971.

*(9330)*72*ab*cc*dd*de*em*fm

Tyrnauer, S. "Information Processing: Management Control of Job Failures and Related Reruns." THE INTERNAL AUDITOR, May 1972.

**(9340)*71*ac*ai*bc*dc*gc*jg*mj*x2
"University Fire: Terminals Beat Heat." COMPUTERWORLD, 21 April 1971, p. 1.

Five Sycor computer terminals survived fire, smoke and water in a University of California administration building at Santa Cruz. The units were taken from the scene of fallen timbers, water, and total destruction to the computer center where they were plugged in and worked. All units had their paint blistered from the heat.

*(9350)*70*ac*ai*bc*cd*dc*jf*mj
"University of Wisconsin Computer Center Bombed; Damage Studied." COMPUTERWORLD, 9 September 1970, p. 6.

*(9360)*71*ac*ai*bd*be*cc*dd*de*ka*mf
"U.S. Marshall Releases Federal Fugitive Because of Incomplete Data in Computer." COMPUTERWORLD, 20 January 1971, p. 2.

*(9370)*69*ad*al*ca*dg*eb*ee
Vanderbilt, D. "Controlled Information Sharing in a Computer Utility." AD-699 503, National Technical Information Service, Springfield, Virginia 22151; or MAC-TR-67, Project MAC, MIT, Cambridge, Massachusetts 02139, October 1969, 172 pp.

An abstract model for structuring and controlling shared information is described. Much of this model is based on work by Jack B. Dennis and E. C. Van Horn discussed in an article by them entitled "Programming Semantics for Multiprogrammed Computation".

*(9380)*69*ab*ah*cb*da*eq*x2
Van Tassel, Dennis. "Advanced Cryptographic Techniques for Computers." COMMUNICATIONS OF THE ACM, December 1969, pp. 664-665.

Several unique characteristics of computer files are briefly described which make cryptographic methods of little use. Computer files usually offer an enemy cryptanalyst a large amount of data to work on; in computer files all records are usually similar; and supposedly the enemy would know what type of information is in the stolen file. The article then discusses some basic advantages and disadvantages of transposition, substitution, and addition cryptographic methods.

*(9390)*70*ae*ag*ba*bb*da*db*ha*hc*hj*ic*if*ig*kd*kf*mc*md*x2
Van Tassel, Dennis. "Computer Crime." AFIPS CONFERENCE PROCEEDINGS, Fall Joint Computer Conference, Vol. 37, 1970, pp. 445-450.

Twenty actual, well publicized cases of computer related fraud are described. About half of the cases are the result of criminals modifying old embezzlement techniques to cope with computer processing. The other half are unique to the computer field. The resulting losses varied from $1,500 to $2,700,000 with the average being over $200,000. Examples of computer sabotage, accidents, and errors were not discussed.

*(9400)*72*aa*bg*cc*cd*dg*ea*ej*el*eq*ff*fg*fk*fo*fp*fq*ft*fu*fv*fx*fy*fz*gg*ha*hk*hl*hm*hq*hr*ja*jc*jf*jg*kb*kd*la*lb*ma*nf*ni*nl*nm*nn*np*x4
Van Tassel, Dennis. COMPUTER SECURITY MANAGEMENT. Prentice-Hall Inc., Englewood Cliffs, New Jersey 17632, April 1972, 220 pp., $10.50.

This book covers computer security in a fairly complete and easily readable manner. It is especially ideal for the individual who knows little about computers or computer security and would like to become broadly acquainted with the subject without having to read many separate sources. Because the book is quite comprehensive, it should also be valuable to a firm's security personnel in determining any missing links or weak spots. A checklist of security questions is included at the end of most chapters.

The book is essentially an attempt by the author to integrate about 200 magazine articles dealing with various aspects of computer security. Although the book is fairly comprehensive, it does not go into much depth on any particular aspect of computer security. Most of the book is concerned with management controls and operating procedures. Only one chapter is concerned with physical aspects of computer security. Methods of designing security into production-accounting type programs are discussed in some detail. Except for several basic requirements, little is said about the safeguard needs of an operating system security monitor. No technical aspects of hardware or software are discussed.

The book is divided into seventeen chapters with the following titles: Computer Crime, Computer Security, Embezzlement: Detection and Control, EDP Control, Auditing, Programmer Error, Operator Error, Operator Fraud, Programmer Fraud, Software Protection, Fire Protection, Disaster and Catastrophe Protection, Insurance, Cryptographic Techniques, Service Bureaus, Time Sharing, and Computer Privacy. There are four appendices: a list of four computer security firms, a record retention time-table, a sample data processing insurance policy, and an annotated bibliography of 190 articles. The bibliography is valuable, but it is limited in scope. Most of the articles in the bibliography are annotated in one sentence, and almost all are primarily concerned with management controls and operating procedures.

*(9410)*71*ab*bc*cc*fc*fv*fw*x2

Van Tassel, Dennis. "A Contingency Plan for Catastrophe." DATAMATION, 1 July 1971, pp. 30-33.

The author first discusses the need for contingency plans and gives four examples of actual computer disasters. Because many accidents and disasters occur when critical personnel are unavailable, the implementation of preplanned wait periods is recommended where the amount of time delay before initiating expensive recovery action depends on the seriousness of the problem. Organizations that are highly dependent on their computer's continued operation for survival should have at least one full-time person with responsibility for developing emergency guidelines. Off-site backup is usually very desirable. Backup hardware and software need periodic checking to assure that they will meet the requirements specified in the contingency plans. Some backup arrangements can also be made when negotiating the normal maintenance contract with a vendor. Insurance for the actual information, the value of supporting software, the cost of reconstructing destroyed files, the loss of revenue, and the cost of carrying on normal business while files are being reconstructed should be investigated by all computer users. Although well planned bombings and hurricanes are almost impossible to defend against, a good backup and contingency plan will lessen the resulting recovery expenses.

*(9420)*69*ae*ag*cb*da*eq*x2

Van Tassel, Dennis. "Cryptographic Techniques for Computers." AFIPS CONFERENCE PROCEEDINGS, Spring Joint Computer Conference, Vol. 34, 1969, pp. 367-372.

This article provides a brief and easily readable introduction to cryptography. It should be especially useful for those completely unfamiliar with the subject. Several cryptographic terms are defined, and some basic methods are presented for using transposition and substitution encoding schemes. The article concludes by noting the following advanced cryptographic schemes: combining two or more cryptographic encoding schemes; transmitting random digits when the system is not being used; sending an encoded message over two or more transmission paths; and combining bits with a string of random numbers.

*(9430)*70*ab*cb*da*eq

Van Tassel, Dennis. "Cryptographic Techniques for Computers: Substitution Methods." INFORMATION AND STORAGE RETRIEVAL (Great Britain), June 1970, pp. 241-249.

Substitution cryptographic techniques such as the Caesar, bilinear, homophonic, Vigenere, and playfair methods are discussed in this article. An example is given of each method as well as information on the securness of each. Although some of the methods could be used to protect computer files, it is generally recognized that binary number strings are more efficient, secure, and flexible.

*(9440)*69*ab*cb*cc*da*db*ej*fd*fl*ft*x1

Van Tassel, Dennis. "Information Security in a Computer Environment." COMPUTERS AND AUTOMATION, July 1969, pp. 24-28.

The author briefly discusses a wide range for safeguards to protect sensitive information from unauthorized access. Some of his recommendations are: classify information according to its sensitivity value; keep audit lists on all sensitive information in controlled storage areas; dispose of obsolete, sensitive information in a secure manner using paper shredders or multiple write-over procedures for magnetic media; on every operating shift there must be at least one appropriately cleared individual who is able to enforce all security regulations; insure that adequate memory protect and privileged instructions exist; keep a computer generated log on all significant events; use frequently changed or one-time passwords for remote user identification; if possible restrict users to high level languages; periodically test the security system by trying to break it; and use cryptographic techniques if a significant amount of sensitive information is periodically transmitted over outside telephone lines.

*(9450)*69*ab*cb*da*eq*x1

Van Tassel, Dennis. "Keeping Confidential Information Confidential." JOURNAL OF SYSTEMS MANAGEMENT, February 1969, pp. 14-15.

The following recommendations are made for keeping information confidential: decide what information is to be kept confidential and concentrate protection efforts on this information; inform employees as to what information is confidential and what is expected of them; give confidential information to only those with a definite need-to-know; have special storage facilities for safeguarding confidential information; and have well planned procedures for destroying obsolete confidential information. The author states that very simple cryptographic techniques are adequate for protecting most stored data from unauthorized use. He then briefly describes three basic cryptographic techniques. They are addition, table look-up, and sorting.

*(9460)*70*ab*cc*dc*fy*x2

Verba, Joseph. "Protecting Your EDP Investment." MANAGEMENT SERVICES, September 1970, pp. 37-40.

Management's first step should be the elimination or reduction of the risk of loss resulting from damage to EDP equipment and records. The following protective measures are recommended: keeping vital records in fireproof safes, duplicating valuable records, developing a disaster plan, and working out backup arrangements with users of similar equipment. The author then explains coverage offered by the following, currently available types of business insurance: standard fire contents form, office contents special form, valuable papers and records form, accounts receivable form, special data processing policy - equipment, special data processing policy - media, business interrupting insurance, extra expense insurance, and data processing extra expense form. Coverage offered by the special forms is considerably broader than that offered by the standard forms.

*(9470)*71*ab*cc*ff*fu
Vergari, J. V. "EDP and the Internal Audit Function." THE MAGAZINE OF BANK ADMINISTRATION, March 1971, pp. 26-39.

*(9480)*71*ab*cc*dg*ff
Verger, J. V. "EDP and the Internal Audit." BANK ADMINISTRATION, March 1971.

*(9490)*70*ac*ai*bc*cd*dc*jf*x2
"Violence by Rebels Threatens Centers." COMPUTERWORLD, 7 October 1970, p. 1.

FBI reports indicate that in the last 15 months, 4,330 bombings resulted in 40 deaths, 380 injuries, and $25 million in physical damage. The Students for Democratic Society organization is now advocating the destruction of computer centers.

*(9500)*71*ab*ah*cb*da*db*dc*ea*gf
"Voiceprint Concept Supported by Government Sponsored Tests." COMMUNICATIONS OF THE ACM, June 1971, pp. 434-435.

*(9510)*71*ac*ai*bf*cd*df*gd*jh
"Voltage Unit Solves Firm's DP Troubles." COMPUTERWORLD, 13 January 1971, p. 24.

*(9520)*65*ae*ag*cb*el*gh*ht*hu*lb*x1
Vyssotsky, V. A.; Corbato, F. J.; and Graham, R. M. "Structure of the MULTICS Supervisor." AFIPS CONFERENCE PROCEEDINGS, Fall Joint Computer Conference, Vol. 27, 1965, pp. 203-212.

This paper is a preliminary report and was written before the MULTICS system was implemented. Several desirable "supervisor" capabilities are discussed. The operating system was written in PL-1, so it could be easily modified and also be largely machine independent. The system is designed to automatically compensate for temporary loss of one or more hardware modules. The system assumes that it is more efficient to serve a few users at a time, and do it well, than it is to serve all users poorly at once. Dynamic linking; trap handling; creation, blocking, and termination of files; and protection against machine errors are also briefly discussed.

*(9530)*69*ab*cc*fc*ff
Wagner, J. W. "EDP and the Auditor of the 1970's." THE ACCOUNTING REVIEW, July 1969, pp. 600-604.

*(9540)*72*ac*ai*be*de*fh*hp*mf*x2
"Wales Nabs Wrong Man." COMPUTERWORLD, 12 January 1972, p. 2.

James H. Gray was held for ten days by Washington, D.C. police because he was confused with another James Gray wanted on a burglary charge. The error occurred because someone had not entered enough identification information into the District's computer system. Before he was able to convince a probation officer of the error, Gray lost his job and was evicted from his apartment.

*(9550)*72*ac*ai*bb*db*hc
"Ward Pleads Guilty to Trade Secret Theft." COMPUTERWORLD, 15 November 1972, p. 1.

Mr. Hugh J. Ward of University Computing Company pleaded guilty to stealing a trade secret after being charged with illegally accessing Information Systems Design's time-sharing computer and stealing a proprietary program. Ward was able to access ISD's computer because both ISD and UCC had a common customer who was assigned the same password by both companies.

*(9560)*70*ad*aj*cb*cc*da*dd*de*eh*el*gh*hd*ka*lb*mb*md
*nl*nm*x4
Ware, Willis H. "Computer Data Banks and Security Controls." P-4329, RAND Corporation, Santa Monica, California 90406, 17 pp.; or AD-703 281, National Technical Information Service, Springfield, Virginia 22151, March 1970.

The author believes that there is no substantial intrinsic motivation for a database operator to surround his databank with a complete set of information safeguards. Moreover, an operator may be technically ignorant of the risks in his system or may be unaware of the ease with which it can be penetrated. For these reasons, the author argues that strong government intervention and control is necessary to protect the privacy of individuals. First, the following suggestions for controls are made: adequate physical protection, ideally - encrypted communications, bounds registers, interrupt and memory protect features, privileged instructions, software access control, audit trails, unusual event alarms, self-test mechanisms, and administrative and management controls. Then the following government rules and regulations are proposed: (1) databank licensing where the operator must state: purpose of databank, source of information, user of information, all safeguards used, validity checks used, audit trails used, mechanisms where individuals can review their dossiers, and tests used to insure the system is operating correctly; (2) periodic audit by government; (3) database operator or user made liable for willfully or negligently handling an individual's information; (4) no anonymous data sources; and (5) positive written certification, to those affected, that errors have been corrected.

*(9570)*67*ad*ae*ag*aj*db*dd*hl*hm*hn*hu*id*ie*ih*ii*lb *nh*ni*x2
Ware, Willis H. "Security and Privacy in Computer Systems." AFIPS CONFERENCE PROCEEDINGS, Spring Joint Computer Conference, Vol. 30, 1967, pp. 279-282; or P-3544, RAND Corporation, Santa Monica, California 90406; or AD-650 810, National Technical Information Service, Springfield, Virginia 22151, April 1967.

This article outlines some of the major vulnerabilities which exist in modern time-sharing computer systems. The following vulnerabilities were briefly discussed: processor (radiation; failure of hardware protection circuits such as bound registers, memory read/write protects, and privileged mode; failure of software protection features such as access control, bounds control, and user identification); communication lines (radiation, wiretaps, crosstalk); switching center (failure to connect proper line, cross coupling between lines); remote terminals (attachment of bugs or recorders); files (theft, copying, unauthorized access); operator (replace the protection monitor with non-protective one, reveal protective measures); maintenance man (disable hardware protective devices, use stand-alone utility programs to access files); systems programmer (disable software protective features, provide private "ins", reveal protective measures); and user (identification, authentication, and subtle modifications to software system).

*(9580)*67*ad*ae*ag*aj*cb*cc*dg*mh*x3
Ware, Willis H. "Security and Privacy: Similarities and Differences." AFIPS CONFERENCE PROCEEDINGS, Spring Joint Computer Conference, Vol 30, 1967, pp. 287-290; or P-3544, RAND Corporation, Santa Monica, California 90406.

The title of this article is deceiving because the author gives the terms "security" and "privacy" special meanings which are different from their most common meanings. "Security" is used to refer to computer systems which handle classified military information, and "privacy" is used to refer to computer systems which handle only non-military information. The purpose to this paper is to identify and briefly discuss the differences and similarities between computer systems operating with classified military information and computer systems handling private or sensitive information.

The following nine conclusions are discussed: (1) the problem of controlling user access to the time-sharing computer system is similar in both situations; (2) the incentive to penetrate the system is present in both situations; (3) the computer hardware requirements appear to be the same in both situations; (4) the file access and protection problem is similar under both circumstances; (5) the philosophy of the overall system organization will probably have to be different in the non-military situation; (6) the certifying authority is certainly different in the two situations; (7) deliberate penetrations must be anticipated in both situations, but the military espionage threat is more serious; (8) both situations require secure communication circuits; and (9) the level of communication protection needed will usually be greater for the military situation. The author concludes by noting the all important difference that users of non-military systems may not be subject to a common authority or discipline. This difference indicates that a computer network designed to safely protect classified military information will not automatically provide adequate protection for non-military information systems.

*(9590)*70*ad*aj*cb*cc*cd*fx*nn*nq
Ware, Willis H. (ed). "Security Controls for Computer Systems." R-607, RAND Corporation, Santa Monica, California 90406, February 1970, (Classified Confidential).

The report is supposedly very comprehensive. It includes a checklist on how to test the security of a computer installation.

*(9600)*70*aa*da*mb*md*mg*nl*nm*np*x2
Warner, Malcolm; and Stone, Michael. THE DATA BANK SOCIETY: ORGANIZATIONS, COMPUTERS, AND SOCIAL FREEDOM. George Allen and Unwin Ltd., Ruskin House, Museum Street, London, England, 1970, 244 pp.

This book studied the effects on private citizens of the concentration of massive information by large organizations. The problem is examined from a social and broadly political standpoint in the knowledge of technical potentials and limitations. Only one sixteen page chapter of this book deals with computer security issues. In this chapter, several protective measures are discussed and recommended both for the computer manufacturer and computer user. That chapter, like the rest, is very non-technical and can be easily understood by those who know nothing or very little about computers. The book is more valuable to those interested in the computer's affect on individual privacy. An annotated bibliography of sixty articles is included, but only ten of these entries are concerned with security issues.

*(9610)*70*ac*ai*bf*cc*df*kd*mi*nj
"Washington Airport Shuttle Crippled by Driver Strike." COMPUTERWORLD, 5 August 1970, p. 1.

Washington, D.C. bus drivers went on strike when their paychecks were forty-five minutes late. The bus firm has its paper tape reader repossessed by a service bureau which it was having financial difficulties with. No other automatic means of payroll processing were available for backup, so the checks had to be manually processed.

*(9620)*68*ab*cc*dg*ff*kd
Wasserman, Joseph J. "Auditing the Computer." MANAGEMENT REVIEW, October 1968.

This article discusses changes that are occurring in audit trails due to electronic data processing. It is a condensed version of another article by Wasserman entitled "The Vanishing Trail" and published in BELL TELEPHONE MAGAZINE.

*(9630)*69*ab*cc*ff*kd
Wasserman, Joseph J. "Bridging the Computer-Auditor Gap." BANKING, December 1969, pp. 83-85.

*(9640)*72*ab*cc*dg*ff*kd
Wassermen, Joseph J. "Computer Audit Packages." DATA MANAGEMENT, September 1972, pp. 71-72.

This paper discusses several audit functions which should be considered when evaluating a generalized audit program. Some of these functions are: extraction, surveying, mathematics, totaling, sampling, aging, bypass invalid data, and user exit.

*(9650)*70*ab*cc
Wasserman, Joseph J. "Control in an EDP Environment." THE INTERNAL AUDITOR, September 1970.

*(9660)*69*ab*bd*be*cb*cc*db*dd*de*en*fc*ff*fg*fh*fj*fm
*fp*fq*fv*fx*hp*hq*hr*kd*x2
Wasserman, Joseph J. "Plugging the Leaks in Computer Security." HARVARD BUSINESS REVIEW, September 1969, pp. 119-129.

This article describes many computer auditing and control concepts, and shows how a company can use them for detecting and preventing unintentional human errors. Fraud and natural disaster threats are only very briefly discussed because losses from them are dwarfed by losses resulting from honest mistakes. Some error control concepts discussed are: parallel testing of old and new systems; checking by using a test deck of fictitious transactions; checking control totals as records are converted; establishing a quality control unit to sample the accuracy of data both before and after computer processing; an input section which maintains positive controls over all transactions it receives; an output section which controls the distribution of data and ensures its reasonableness, timeliness, and completeness; a built-in method of error analysis; complete and current written instructions for all machine operations; an EDP library which requires authorized access for removal of tapes; limiting the number of personnel who are authorized to change production programs and data files; classifying information as to its sensitivity; allowing only authorized personnel access to the computer room; duplicating all vital files and storing them in a remote location; using recovery/restart procedures for large processing jobs; file reconstruction and disaster insurance; separation and rotation of duties; ensuring computer systems are auditable; using a "mini-company" testing procedure which passes fictitious test transactions through the computer system simultaneously with regular live data; 100% comparison of program calculations; statistical sampling of records; extracting specific records for analysis; and checking mathematical calculations made by the computer.

*(9670)*70*ab*cc*fc*x1

Wasserman, Joseph J. "Protecting Your Computer's Security." DATA SYSTEMS NEWS, February 1970, p. 17.

The author states that security is a problem because most users ignore the subject until it becomes a problem. He believes that auditors should have enough understanding of data processing to be able to participate in system design. Programmers and operations personnel should view their jobs in relation to the goals of the business - one of which is security.

*(9680)*68*ab*cc*dg*ff*kd

Wasserman, Joseph J. "The Vanishing Trail." BELL TELEPHONE MAGAZINE, July 1968.

Changes that are occurring in audit trails due to electronic data processing are discussed.

*(9690)*68*ab*cc*da*ka*nm*x1

Watterson, Lynn. "Data Banks Can Protect Privacy." BANKING, January 1968, p. 56.

The author believes, but does not convincingly prove, that current computer technology is capable of preventing unauthorized access to sensitive data. She feels that the real problems are in developing standards and laws to control what information is to be collected and who is to have authorized access to this information. A consumer credit system is proposed where files are kept only on individuals that wish to participate in the system. A business can access an individual's credit file only by getting the individual's permission. All individuals would have the right to review their complete file if they pay a small fee.

*(9700)*70*ab*cc*cd*fw*ga*gf*mc*x1
Wearstler, Earl W. "Computer Center is for Safety, Not for Show." BANKING, April 1971, p. 70.

Continuous operation of the computer center is essential for most banks. Therefore, the computer center needs good physical protection from fire, storms, and sabotage. Several common methods are briefly described for controlling physical access to the computer room and providing protection from fire. Off-site storage for duplicates of master and grandfather files, and a disaster plan with detailed procedures for all contingencies are recommended.

*(9710)*70*ab*cb*ek*ff*gh
Webb, R. "Audassist." JOURNAL OF ACCOUNTANCY, November 1970, pp. 53-58.

*(9720)*00*ad*ca*da*db*dc*ea
Wegstein, J. H. "A Computer Oriented Single Fingerprint Identification System." NBS Technical Note 443, National Bureau of Standards.

*(9730)*68*ad*ca*da*db*dc*ea
Wegstein, J. H. "Matching Fingerprints by Computers." NBS Technical Note 466, National Bureau of Standards, July 1968.

*(9740)*73*ac*ai*cd*df*gd*jh*x2
Weinstein, Michael. "Backup Power: Who Needs It and at What Price?" COMPUTERWORLD, 23 May 1973, p. 21.

The initial cost of installing an uninterruptible power supply system can be estimated with the simple rule of $1 for every watt of power required. Most battery-based systems are designed to keep the computer operating for one hour or less while motor generator backup systems are used to provide power for periods from one hour to several days. Short term battery systems are always used in conjunction with motor generator systems because the generators can not be started instanteously when a power fault occurs.

*(9750)*72*ac*ai*cb*db*dc*ea*ih*x1
Weinstein, Michael. "Who Accesses What on Remote Terminal?

DP Managers Must Have Stricter Control." COMPUTERWORLD, 6 December 1972, p. 24.

Some common methods of identifying and authenticating remote terminals and remote terminal users are briefly discussed. The computer must be able to identify all terminal addresses. Privileged terminals should have terminal addresses preceding each input and output. Various password schemes, badges, cards, keys, and voice and fingerprint identification may be used to identify individual terminal users. Unattended terminal problems can be solved by requiring identification if terminal communication has not occurred for a specified time.

*(9760)*69*ab*cd*dc
Weiser, A. L. "ADP Physical Installation Considerations." COMPUTERS AND AUTOMATION, November 1969, pp. 44-49.

*(9765)*70*ab*cc*ff
Weiss, Harold. "Computers and Auditing - A Conference Report." DATAMATION, 15 July 1970, pp. 108-113.

*(9770)*69*ab*bc*cc*cd*dc*ga*jg*x2
Weiss, Harold. "Danger of Total Corporate Amnesia." FINANCIAL EXECUTIVE, June 1969, pp. 63-68.

The author feels that most organizations are dangerously lax in their disaster prevention and recovery planning. He attempts to throughly convince the reader that the high concentration of vital computerized information in a small area makes possible the total destruction of corporate records by natural disaster or sabotage. The problems of equipment unavailability, file and program protection, and fire detection and prevention are discussed in some detail. Various types of data processing insurance are also briefly described. The author concludes by recommending that higher level management review its organization's vulnerability to data processing disaster and initiate a crash program to reduce risk and assure the capability of efficient recovery.

*(9775)*72*ab*cc*fm
Weiss, Harold. "EDP Operations: The Forgotten Third." JOURNAL OF SYSTEMS MANAGEMENT, July 1972, pp. 18-21.

*(9780)*69*ae*cc*cd*dc*hg*jf*jg
Weiss, Harold. "Reducing the Risk of Destruction." DATA PROCESSING MANAGEMENT ASSOCIATION CONFERENCE PROCEEDINGS, Vol. 14, 1969, p. 417.

Several methods for reducing the possibility of destruction to critical data and equipment are discussed.

*(9785)*71*ab*cc*fc*ff
Weiss, Harold. "Reflections on Computers and Auditing in the 1970's." THE INTERNAL AUDITOR, July 1971.

*(9790)*67*ab*cb*cc*cd*dg
Weiss, Harold. "The Week the Computers Stopped." DATAMATION, April 1967.

The vulnerability of typical computer installations is described.

*(9795)*67*ab*cc*fy*nb
Weissman, Clark. "Programming Protection: What Do You Want to Pay?" SDC MAGAZINE, Systems Development Corporation, 2500 Colorado Avenue, Santa Monica, California 90406, July 1967, pp. 30-31.

The author believes that adequate security for computing systems is available with today's technology. All that is needed is an informed market with the willingness to put its money where it wants its privacy and protection. A system can have adequate protection if the cost to subvert the security system is significantly greater than the cost to maintain the needed protection. Where this cost relationship can not adequately be met, an insurance policy may be the most economical means of protection.

*(9800)*69*ad*ae*ag*ca*da*db*ea*ee*ei*el*gh*hb*he*hi*ih *lb*mh*nc*x3
Weissman, Clark. "Security Controls in the ADEPT-50 Time-Sharing System." AFIPS CONFERENCE PROCEEDINGS, Fall Joint Computer Conference, Vol. 35, 1969, pp. 119-133; or SP-3342, Systems Development Corporation, Santa Monica, California 90406, 29 May 1969.

Implementation of security in the ADEPT-50 Time-Sharing System is described in detail, as are other features such as: initialization of security profiles; the LOGIN decision procedure; security audit trails; security integrity checks; security residue control; automatic file classification based on the cumulative security history of referenced files; once-only passwords; and the "security umbrella" of the ADEPT job. Approximate design and operation costs, and a list of security command words are also discussed.

The ADEPT-50 system identifies four types of security objects - users, terminals, jobs, and files; and three types of security properties - authority, franchise, and category. The authority property relates to levels of security classification such as: unclassified, confidential, secret, and top secret. The category property restricts access by project and area. It can have up to sixteen values assigned by the using agency. The franchise property corresponds to a need-to-know constraint. There are three types of files: public, private, and semi-private. Only the semi-private files have need-to-know lists. Control at the file level also includes: read only, write only, read and write, and read and write with ability to override lockout of simultaneous use. The ADEPT-50 security system overhead cost is approximately two percent. It was implemented on an IBM 360/50 computer with no special hardware modifications.

*(9805)*70*ab*ad*cb*cc*nb*ng*x3
Weissman, Clark. "Trade-Off Considerations in Security System Design." DATA MANAGEMENT, April 1972, pp. 14-19; or SP-3548, System Development Corporation, 2500 Colorade Avenue, Santa Monica, California 90406, 10 September 1970.

The major difficulty in security system design is the inability to quantify trade-off considerations. This article concentrates on system software aspects of security. The security goals, strategies, and safeguards selected for the ADEPT-50 Time-Sharing System are discussed throughout this article.

Security goals can be selected by carefully looking at the security problem, the issues surrounding it, the user community, the goals of the system itself, and seeing if security goals are implied. Another method of goal selection, called threat analysis, is to hypothesize system failures and resulting consequences, and then envision ways of reducing system vulnerability. System software security design involves a trade-off between granting the user different levels of access to raw computer power, and providing different levels of sophisticated and expensive safeguards to protect against the user's capability to subvert the system. Several different levels of access control, residue control, and integrity control are presented and discussed in some detail. The control levels designed into the ADEPT-50 system are also noted. The author also identifies and briefly discusses five common protection strategies used in modern society: isolation (isolating the valuable object and controlling access to it); confusion (camouflage, disguise, cryptography); deterrence (profit/loss relation, laws); wager (insurance); and delegation (use of service bureaus). The article concludes by briefly discussing two major problem areas of the future - metrics and certification.

*(9810)*71*ab*cb*cc*cd*dg
Welke, L. A. "What About Security? - On Centers." MODERN DATA, September 1971, p. 34.

*(9815)*72*ab*cc*ff

Welke, W. R.; and King, K. G. "Using the Computer as an Audit Tool." THE CPA JOURNAL, November 1972, pp. 930-935.

*(9820)*70*ab*cc*df*dg*fz*ma*nj
Wessel, Milton R. "Computer Services and the Law." BUSINESS AUTOMATION, November 1971, pp. 48-50.

The liability problems for EDP service bureaus will significantly increase during the next ten years. Those service bureaus that fail to recognize their expanding liabilities will face a much larger risk of not remaining in business. This article is exactly the same as another article by Wessel entitled "Problems of Liability for EDP Service Industry" which appeared in COMPUTERS AND AUTOMATION.

*(9825)*65*ab*cc*da*fy*f1
Wessel, Milton R. "Legal Protection of Computer Programs." HARVARD BUSINESS REVIEW, March 1965.

*(9830)*70*ab*cc*df*dg*fz*ma*nj
Wessel, Milton R. "Problems of Liability for EDP Service Industry." COMPUTERS AND AUTOMATION, September 1970.

The liability problems for EDP service bureaus will significantly increase during the next ten years. Those service bureaus that fail to recognize their expanding liabilities will face a much larger risk of not remaining in business. This article is exactly the same as another article by Wessel entitled "Computer Services and the Law" which later appeared in BUSINESS AUTOMATION.

*(9835)*71*ab*cd*dc*fv*ga*ge*gf*gh*jf*nd*x2
Wessler, John; Myers, Edith; and Gardner, W. David. "Physical Security - Facts and Fancies." DATAMATION, 1 July 1971, pp. 34-37.

The article describes physical security measures taken by these organizations: RCA, New England Telephone, Bank of California, City of Los Angeles, an unnamed midwest machine tool manufacturer, GTE's Sylvania Lighting Products Group, and MIT. The protection provided ranged from poor to excellent. Several well known companies that offer computer security consulting services are also mentioned.

*(9840)*67*ae*ag*cc*da*ka*mb*nl*nm
Westin, Alan F. "Legal Safeguards to Insure Privacy in a Computer Society." Speech Presented at AFIPS CONFERENCE PROCEEDINGS, Spring Joint Computer Conference, 18 April 1967.

The author discusses the problem of data surveillance, where an individual's behavior is kept track of by periodically collecting data on him and monitoring it with a computer. Current American law is not very adequate for controlling misuse of personal information. Technological safeguards and legal controls are recommended to balance the conflicting demands between the right to individual privacy and society's right-to-know. Positive action must begin now if rational solutions are to be developed.

*(9845)*69*ab*ad*ak*cb*cc*da*ka*md*nl*nm
Westin, Alan F. "New Laws Will Protect Your Privacy." THINK: An IBM Corporation Magazine, May 1969, pp. 27-31.

This article discusses general trends and events in the development of technical, administrative, and legal means to protect individual privacy. Two recent Supreme Court decisions are cited which broke the legal stalemate in the privacy area and resulted in federal legislation on wiretapping and eavesdropping. However, a lot of events have occurred in the last four years to make this article somewhat obsolete.

*(9850)*67*aa*cc*da*hd*ka*md*nl*nm*nn*np*x4
Westin, Alan F. PRIVACY AND FREEDOM. Atheneum Press, New York, 1967, 487 pp.

This is a classic book on privacy. It is an in-depth analysis of the history of privacy since 1776. However, it was written in 1967 and is somewaht out-of-date on current computer activity. The book is divided into four parts entitled: The Functions of Privacy and Surveillance in Society, New Tools for Invading Privacy, American Society's Struggle for Controls - Five Case Studies, and Policy Choices for the 1970's. Each part is copiously documented. The first part analyzes the sociological, psychological, and political dimensions of privacy. The second part describes present surveillance techniques and what the future is likely to bring. The last part discusses the history of law relating to privacy and makes specific legal recommendations to insure the right to privacy in the future. An extensive bibliography is also included. This book should definately be read by those seriously interested in the general problem of privacy.

*(9855)*72*aa*cb*cc*cd*da*dd*de*fd*fe*fh*fp*fs*hd*ka*ng *nl*nm*no*x4
Westin, Alan F.; and Baker, Michael A. DATABANKS IN A FREE SOCIETY. Quadrangle Books, 330 Madison Avenue, New York, New York 10017, 1972, 522 pp., $12.50.

This book is the most ambitious study of record-keeping and privacy to date. It is the result of a three year effort by a team of scholars drawn from the social sciences, computer sciences, law, psychology, and mathematics, and led by Alan F. Westin, a Columbia University professor who is the ranking authority on constitutional aspects of data collection and civil liberties. The study was conducted for the National Academy of Sciences. Its major conclusion is that vast, centralized computer databanks simply do not exist, despite a widespread conviction to the contrary by the public and press. Most of the mid-1960 databank plans later proved either impossible to achieve, economically bankrupting, or useless from a business or administrative viewpoint. The study is based on questionnaires from more than 1,500 organizations, both public and private, and site visits to 55 of the most advanced users of computerized information. These site visits were made in 1970 and 1971. Another major conclusion of the study is that social and legal policies with built-in safeguards need to be hammered out before the inevitable development of vast, centralized computer databases does occur.

The book is written with scholarly rigor and avoids dramatizing the material. Fourteen very detailed profiles are given on the following computerized organizations: The Social Security Administration; The FBI's National Crime Information Center; New York State's Department of Motor Vehicles; Kansas City Police Department; New Haven, Connecticut; Santa Clara County, California; Bank of America; TRW - Credit Data Corporation; Mutual of Omaha; R. L. Polk and Company; MIT; The American Council on Education; The Church of the Latter-Day Saints; and The Kaiser-Permanente Care Program. The book is organized into five sections: a brief introductory chapter on records, computers, and civil liberties; the previously mentioned 14 profiles; site findings of the 55 organizations visited; and two summary chapters entitled "Future Directions in Computer Technology" and "Implications for Public Policy".

Before purchasing or reading this book, one may want to read one or both of the following 1300-word reviews: "A Myth-Destroying Study of Computers" by Ephraim A. Lewis in the January 13, 1973 issue of BUSINESS WEEK, or the book review section in the April 1973 issue of DATA PROCESSING DIGEST. A similar study of Canadian Organizations can be found in an article by John M. Carroll entitled "Snapshot 1971 - How Canada Organizes Information About People" in the 1972 Fall Joint Computer Conference Proceedings.

*(9860)*71*ab*cd*dd*df*jh

"Westinghouse Warns of Power Fluctuations' Effect on EDP Units." MANAGEMENT ADVISER, July 1971, p. 13.

*(9865)*69*ae*cc*dg*em*fi*fp*fx*f1*hc*hm*hr*nj

Whelan, Thomas. "Software Security." American Management Association Session Briefing on Catastrophe Prevention and Security Management of the Computer Complex, 17

November 1969.

Program design, program changes, testing procedures, checkpoint recovery routines, environmental protection, and legal protection of software are all discussed.

*(9870)*70*ab*cc*da*nm

"Who Watches the Watchers." DATA SYSTEMS NEWS, December 1970.

*(9875)*71*ab*cc*da*fs*ft*hc*jc

"Why Employees Steal." U.S. NEWS AND WORLD REPORT, 3 May 1971, pp. 78-82.

*(9880)*71*ab*cc*dd*de*nm

"Why the Public Dislikes Computers." COMPUTERS AND AUTOMATION, May 1971, p. 7.

*(9885)*71*ab*cc*da*fh*ka*nl*nm*x2

Wiesner, J. B. "The Information Revolution and the Bill of Rights." COMPUTERS AND AUTOMATION, May 1971, p. 8.

The author, President of MIT, feels there is a great danger that we, the public, could become "information bound" because each step in the development of an "information tyranny" appeared to be constructive and useful. Data-centralization and manipulation can be expected to grow at an ever increasing rate. At the same time, effective information gathering, record keeping, and data processing are essential to a modern society. To keep modern technology from dominating the public, very strict legal controls must be adopted on - who can do what with private information. These controls must be adopted soon, before their deployment is contrary to the special interests of large groups of people. Technology alone cannot provide adequate safeguards.

The author outlines several specific needs: the establishment of a watchdog authority to review information gathering and processing activities and to report to Congress; the setting of rigid limitations on permissible surveillance activities, perhaps by amending the constitution; the outlawing of free exchange of information and requiring disclosure to individuals of data kept on them; and the development and required use of technical means of safeguarding data.

*(9890)*68*ab*cb*ec*lb

Wilkes, M. V. "Time-Sharing Computer Systems." AMERICAN ELSEVIER, 1968.

*(9895)*72*ab*cc*ff

Will, H. J. "Computer Based Auditing." CANADIAN CHARTERED ACCOUNTANT, February 1972.

*(9900)*72*ab*cd*dc*ga*ge*nd*x2
Willis, John A. "Is Your Computer Center Safe?" COMPUTER DECISIONS, June 1972, pp. 12-14.

A few basic suggestions are given concerning proper location of the computer room, physical access control, and fire detection and prevention. A sample checklist of fifteen questions is also presented. The article concludes by presenting a list of names, addresses, and telephone numbers of twelve companies offering computer security surveys.

*(9905)*69*ab*cd*dd*gb*jh
Wilson, T. "Air Conditioning in the Computer Room." DATA PROCESSING, March 1969, pp. 167-168.

*(9910)*71*ab*ak*cb*cc*dg*fe*em*ff*ma
Wimbrow, J. H. "A Large-Scale Interactive Administrative System." IBM SYSTEMS JOURNAL, November 1971, pp. 260-282.

This article describes a nationwide network of terminals used by over 20 major businesses which share a single large and varied data base. Part of the article discusses user authorization, data-base reconstruction considerations, and auditing.

*(9915)*69*ac*ai*bc*cd*dc*gc*jf*mj
"Wirecutters, Acid Used on Computer." COMPUTERWORLD, 9 April 1969, p. 7.

Student destruction of the Boston University computer center is described.

*(9920)*71*ad*cc*cd*np*x2
Witzer, Harold. "Computer Security Bibliography." AVCO Computer Services, 201 Lowell Street, Wilmington, Massachusetts 01887, January 1971, 133 pp., $3.50.

This partially annotated bibliography contains 330 entries. 120 of these are primarily concerned with privacy issues. The annotations are short and average about 30 to 40 words. Approximately 30 of the security entries and 90 of the privacy entries are not annotated, and approximately 60 of the entries are from COMPUTERWORLD newspaper. Almost all of the entries are concerned with physical security, or management controls and operating procedures. Entry numbers 144 through 164 are a list of 20 pre-1968 books dealing with privacy issues. Keyword and author indices are provided for accessing the 330 entries. Also included is a list of 66 firms that sell locks, surveillance systems, alarms, and guard services.

*(9925)*71*ab*cc*fm
Wofsey, Marvin M. "EDP Systems Controls." DATA MANAGEMENT, September 1971, pp. 71-76.

*(9930)*72*ab*bf*bg*cc*cd*df*dg*eg*el*fb*fw*fz*ga*ge*gf *nb*nf*nj*x2

Wofsey, Marvin M. "Data Security." DATA MANAGEMENT: Conference Issue, September 1972, pp. 80-86.

First, the need for data security is demonstrated by a brief discussion of these threats: fire; explosion; natural disaster; sabotage; social protests; environmental problems; power difficulties; loss of programs and data due to misoperation or environment difficulties; external radiation; operator error; data theft; fraud; illegal selling of computer time; and law suits for computer errors or poor service. Over twenty actual cases were cited when discussing these threats. Next, a large number of very common physical, procedural, and legal preventive measures are listed.

The author states that the computer manager should recognize potential dangers and prepare a cost/value analysis which includes the following elements: hazard, degree of damage, probability of occurrence, consequences, possible dollar damages, measures recommended, cost comparison of probable damages and costs of measures recommended, alternative measures considered, and costs of alternative measures considered. The completed cost/value analysis should be given to top management who must make the final decision as to what security measures are to be implemented.

*(9935)*71*ab*cd*dc*ge*nb

Wood, J. A. "Fire Protection for Computer Installations: A Cost-Effective Comparison." INSTRUMENTS AND CONTROL SYSTEMS, June 1971, pp. 129-131.

*(9940)*73*ac*ai*be*de*hp*kd*me*x1

Wright, Bob. "Human Error Found Cause of Overpayment in Weekly Paycheck." COMPUTERWORLD, 18 April 1973, p. 9.

A data input error resulted in a Durham, North Carolina city employee receiving a salary of $31 per hour when he was authorized to receive only $3.12 per hour. The error went undetected for two months until a year-end annual audit found the error. The computer did not check hourly rates because the city employed many daily and part-time workers who were not paid hourly rates.

*(9945)*71*ac*ai*bc*cd*dc*jf
"Yippies Convene, Discuss Methods of DP Sabotage." COMPUTERWORLD, 14 April 1971, p. 2.

*(9950)*72*ab*cc*da*f1*nj*nl
Young, M. L. "Precarious Path to Adequate Legal Protection of Software." DATA MANAGEMENT, August 1972, pp. 10-13.

*(9955)*67*ab*cc*ff
Young, R. "Internal Control in Electronic Data Processing." CPA JOURNAL, January 1967, pp. 45-50.

*(9960)*70*ab*cc*cd*dg
"Your Computer: How Secure?" CHEMICAL ENGINEERING, November 1970.

*(9965)*71*ab*bd*dd*nj*x1
"Your Firm Could Pay for a Computer Error." INSURANCE, 15 March 1971, P. 72.

This short article describes a case involving Ford Motor Credit Company and one of its customers. On three separate occasions the company's computer refused to acknowledge prompt automobile installment payments by a customer. The customer proved he had made the payments on the first two occasions but refused to go through the troublesome procedure on the third occasion. Ford promptly repossessed his automobile. A lawsuit followed, and Ford Credit Company was required to pay $5,000 in punitive damages plus the fair market value of the car. The jùdge held that a business is responsible to its customers for correct operation of its computer system.

*(9970)*72*ab*cb*dg*ha*lb
Yourdon, Edward. Reliability of Real-Time Systems," MODERN DATA, (A six part series of articles), January-June 1972.

This series of articles explores why and how systems fail. A book with the same title also exists.

*(9975)*70*ac*ai*ba*da*hd
"Youth Indicated in Data File Copying." COMPUTERWORLD, 11 November 1970, p. 3.

An 18-year-old was indicted on charges of interstate transmission of stolen property by wire, and unauthorized access on a time-shared computer network.

*(9980)*72*ab*cc*df*dg*fz*x2
Zaiden, Dennis J. "Some Legal Aspects of EDP." MANAGEMENT ACCOUNTING, July 1972, pp. 51-52.

The author discusses several items that should be included in a contract with a equipment vendor or service bureau. For a equipment vendor the contract should include: detailed specifications of the system telling what the system can and cannot do; physical requirements of the installation; details as to what programs and compilers will be provided; details of implementation assistance including technical personnel of vendor, employee training, user's manuals to be furnished, and period of assistance; and details as to who will do what, with specific roles stated for vendor and customer personnel. For contracts with service bureaus, a different set of items must be considered. They are: the bureau's responsibility for training, instruction manuals, etc.; maximum acceptable turn-around time; required provisions for assuring the integrity and privacy of programs and data; hardware and software maintenance; and insurance responsibilities.

*(9985)*72*ab*cc*df*dg*fy*x2
Zaiden, Dennis J. "Special EDP Insurance: Who Needs It." DATA PROCESSING MAGAZINE, Spring 1972, pp. 31-34.

The article first shows that conventional insurance policies do not provide adequate protection for EDP equipment and operations. It is suggested that a company prepare a complete list of all hazards it is exposed to, estimate the dollar value of probable losses resulting from these hazards, and then see an insurance representative. Since the St. Paul Fire and Marine Insurance Company currently provides one of the most versatile multiple peril data processing policies, its policy is discussed and analyzed in detail. The article concludes by giving some advice on avoiding coverage of equipment in both general insurance policies and special EDP policies, and on determining whether any deficiencies in coverage exist which should be compensated for.

*(9990)*72*ab*cc*cd*dg*ni
Zaiden, Dennis J. "Steps You Can Take to Protect Your Computer Operation." LKHH ACCOUNTANT, No. 2, 1972, pp. 29-35.

V. FIRMS SELLING COMPUTER SECURITY SERVICES OR EQUIPMENT

Of the thirty-four firms listed below, only about eight (numbers 50,60,100,120,160,170,230, abd 250) are service companies specializing in the field of computer security. Six are primarily manufacturers of security equipment, and the rest offer computer security investigations along with many other services. Source number 2010 in the annotated bibliography was used to obtain information on about half of these firms. The other firms were found from sundry sources.

10. ANALYTICS INC., 179 Washington Lane, Jenkintown, Pennsylvania 19046, (215) 885-9424.
Performs computer security surveys.

20. ASSOCIATED COMPUTING SERVICES INC., 12011 San Vicente Boulevard, Suite 350, Los Angeles, California 90049, (213) 476-6515.
Provides services in consulting, auditing, and data processing standards. Established in 1966. Had eighteen employees in 1972.

30. BAKER INDUSTRIES INC., 8 Ridgedale Avenue, Cedar Knolls, New Jersey 07927, (201) 267-1600.
Performs computer security surveys.

40. BELDEN MENKUS: CONSULTANT, 7 Blauvelt Avenue, Bergenfield, New Jersey 07621, (201) 385-0383.
Provides services in computer security evaluation, and design or improvement of information systems. Established in 1971. Had two employees in 1972.

50. BRADFORD SECURITY SYSTEMS INC., 300 East 52nd Street, New York, New York 10022, (212) 832-0459.
Provides consulting services in the area of computer security, reliabibity, and integrity. The firm will determine: specific computer system security requirements; vulnerability to fire, flooding, human errors, vandalism, fraud, sabotage, etc.; and cost effective safeguards to satisfy requirements. Established in 1969. Robert V. Jacobson is the firm's

president.

60. BURNS INTERNATIONAL SECURITY SERVICES INC., Briarcliff Manor, New York 10510, (914) 762-1000.
Will survey computer for security requirements.

70. CERTIFIED MANAGEMENT SERVICES INC., 3810 Wilshire Boulevard, Suite 1405, Los Angeles, California 90010, (213) 388-3415.
Offers systems and procedures services, and performs feasibility studies. Established in 1968. Had six employees in 1972.

80. COLLEGE COMPUTER CORPORATION, College Plaza, Collegedale, Tennessee 37315, (615) 396-2950.
Manufactures and sells security systems and related equipment. Also provides batch and time-sharing computing services, systems analysis, communications conuslting, and courses in computer science. Established in 1967. Had ten employees in 1972.

90. COMPUTER ASSISTANCE INC., 298 Park Road, West Hartford, Connecticut 06119, (203) 233-9848.
Provides services in facilities management, security audits, proprietary software, programming, and systems analysis. Established in 1967. Had forty employees in 1972.

100. COMPUTER AUDIT SYSTEMS INC., 725 Park Avenue, East Orange, New Jersey 07017, (201) 676-8320.
Specializes in computer auditing, controls, and security. Established in 1969. Had five employees in 1972. Joseph J. Wasserman is the firm's president.

110. COMPUTER MANAGEMENT CORPORATION, 3121 Euclid Avenue, Cleveland, Ohio 44115, (216) 881-9180.
Provides services in facilities management, systems design, software development, data input, documentation, and general consulting. Also manufactures and sells microfilm supplies and viewers. Established in 1969. Had thirty-five employees in 1972.

120. COMPUTER SECURITY INVESTIGATIONS, 7315 Wisconsin Avenue, Bethesda, Maryland, (301) 656-1144.
Offers security surveys and investigations.

130. CRAMER DIVISION OF CONRAC CORPORATION, Mill Rock Road, Old Saybrook, Connecticut 06475, (203) 388-3574.
Manufactures and sells security systems and equipment, digital cassettes, and cassette tape

transports. Established in 1936. Had approximately 400 employees in 1972.

140. DAN B. McDEVITT AND ASSOCIATES, 5019 East 38th Place, Tulsa, Oklahoma 74135, (918) 627-1181.

Provides services in facilities management, programming, systems design, debugging, and cost reduction. Established in 1962. Had twenty-nine employees in 1972.

150. DATA DEVELOPMENT INC., 1090 Highway A1A, P.O. Box 2089, Satellite Beach, Florida 32937, (305) 773-0332.

Provides services in academic, scientific, financial, bank data processing, and management areas. Also provides programming and general consulting services. Had twenty-five employees in 1972.

160. DATA PROCESSING SECURITY INC., 15 Spring Wheel Road, Hinsdale, Illinois 60521, (312) 325-2105.

Provides consulting services in areas of fire protection, electrical power backup, theft, sabotage, off-site record storage recovery plans, facilities, personnel, and physical hardware. Lewis Scoma Jr. is the firm's president.

170. DATAGUARD SYSTEMS, 700 West Campbell Avenue, Phoenix, Arizona 85013, (602) 277-7434.

Specializes in the field of computer security.

180. DATALOCK ELECTRONICS CORPORATION, 2550 Oaks Boulevard, Sacramento, California 95825, (916) 488-0180.

Sells electronic access controls for computer rooms. Established in 1970. Had eight employees in 1972.

190. DIEBOLD INC., 818 Mulberry Road, Canton, Ohio 44711, (216) 453-4592.

Manufactures and sells: alarms for protecting computer installations; information storage and retrieval systems; and protection and storage devices for EDP data. Established in 1859. Had 6000 employees in 1972.

200. FENWAL INC., 400 Main Street, Ashland, Massachusetts 01721, (617) 881-2000.

Manufactures fire detection and suppression systems. Will analyze your computer center for fire protection. Established in 1935. Had 700 employees in 1972.

210. ICM COMPUTER CORPORATION, P.O. Box 7220, Tulsa, Oklahoma 74105, (918) 587-2333.

Sells complete operating systems. Also designs and operates communications systems and management information systems. Established in 1969. Had 100 employees in 1972.

220. ICM INDUSTRIES, 4141 North Miami Avenue, Miami, Flordia 33127, (305) 758-1528.

Provides services in facilities management, batch processing, data communications, and customized programming. Also leases EDP equipment. Established in 1969. Had fifty employees in 1972.

230. INTELLIGENCE SERVICES INC., 6500 Jericho Turnpike, Syosset, New York 11791, (516) 433-0122.

Will Perform computer security surveys.

240. KELTRAN CORPORATION, 225 Crescent Street, Waltham, Massachusetts 02154, (617) 394-0525.

Manufactures and sells monitoring systems, security alarms, and digital printers. Established in 1960. Had forty-five employees in 1972.

250. MANAGEMATICS INC., 2 Penn Plaza, New York, New York 10001, (212) 594-7199.

Provides services in systems and facilities security, recovery procedures, preformance evaluation, management information systems development, and mathematical modeling. Established in 1968. Had ten employees in 1972.

260. PERMALOC SECURITY DEVICES INC., 627 Sligo Avenue, Silver Spring, Maryland 20910, (301) 589-9318.

Manufactures and sells access control systems for computer rooms. Established in 1968. Had four employees in 1972.

270. PINKERTON'S INC., 100 Church Street, New York, New York 10007, (212) 233-3144.

Will analyze computer installations for security requirements.

280. PYROTRONICS INC., 8 Ridgedale Avenue, Cedar Knolls, New Jersey 07927, (201) 267-1300.

Manufactures and sells fire and smoke detection systems for computers. Will analyze your computer room for fire protection needs. Had 200 employees in 1972.

290. RETAIL OPERATING SYSTEMS COMPANY, P.O. Box 7220, Tulsa, Oklahoma 74105, (918) 587-2333.

Designs, implements, and operates retail operating systems. Also offers software, hardware, and personnel services.

300. RICHARD L. BERRY: MANAGEMENT CONSULTANTS, 714 Landmark Two, Cherry Hill, New Jersey 08034, (609) 423-7542.

Provides services in systems consulting, personnel testing, recruitment evaluation, and staffing. Established in 1959. Had ten employees in 1972.

310. SABER LABORATORIES, 1150 Bryant Street, San Francisco, California.

Provides information security consulting services.

320. SIERRA RESEARCH CORPORATION: DATA SYSTEMS DIVISION, 217 Middlesex Turnpike, Burlington, Massachusetts 01803, (617) 273-0900.

Provides systems for machine monitoring and control, and data collection. Also manufactures and sells terminals. Established in 1960. Had sixty-nine employees in 1972.

330. URBAN SYSTEMS AND SERVICES COMPANY, 3400 Montrose Boulevard, Suite 216, Houston, Texas 77006, (713) 526-6243.

Provides services and consulting in facilities management for municipal governments, law enforcement systems, tax systems, and municipal water systems. Also manufactures and sells communication equipment. Established in 1969. Had twenty-five employees in 1972.

340. WESTINGHOUSE SECURITY SYSTEMS, 1725 Washington Road, Pittsburgh, Pennsylvania 15241, (412) 341-7672.

Offers datacenter security surveys.

VI. REFERENCES AND BIBLIOGRAPHIES FOR SECURITY AND PRIVACY ARTICLES

*(0310)
Anderson, Ronald E.; and Fagerlund, Ed. "Privacy and the Computer: An Annotated Bibliography." COMPUTING REVIEWS, November 1972, pp. 551-559.

*(0770)
Bergart, Jeffery G. "Computer Security, Access Control, and Privacy Protection in Computer Systems." Master's Thesis, Moore School of Electrical Engineering, University of Pennsylvania, Philadelphia, Pennsylvania, August 1972, 87 pp.; or "An Annotated and Cross-Referenced Bibliography on Computer Security Access Control in Computer Systems." AD-755 225, National Technical Information Service, Springfield, Virginia 22151, November 1972, 57 pp., $4.50.

*(1370)
Browne, Peter S. "Computer Security - A Survey." DATABASE: Quarterly Newsletter of ACM's Special Interest Group on Business Data Processing (SIGBDP), Vol. 4, No. 3, Fall 1972, pp. 1-12.

*(1480)
BUSINESS PERIODICALS INDEX. The H. W. Wilson Company, New York, New York, 1958-, (Monthly, with annual cumulations every June).

*(1940)
COMPUTER ABSRACTS. Technical Information Company, Martins Bank Chambers, P.O. Box 59, St. Helier, Jersey, British Channel Islands, 1957-. (Monthly, with annual cumulative index).

*(1950)
COMPUTER AND CONTROL ABSTRACTS. Institution of Electrical Engineers and Institute of Electrical and Electronic Engineers Inc., 345 East 47th Street, New York, New York 10017, 1966-, (Monthly, with semi-annual cumulations).

*(2080)
"Computer Security, Backup, and Recovery: A Selected Bibliography." Canning Publications Inc., 925 Anza Abenue, Vista, California 92083, 20 January 1972, 8 pp.

*(2170)
COMPUTERWORLD. Computerworld Inc., 797 Washington Street, Newton, Massachusetts 02160, 1967-, (Weekly).

*(2200)
COMPUTING REVIEWS. Association for Computing Machinery, 1133 Avenue of the Americas, New York, New York 10036, 1960-, (Monthly, with annual cumulative index).

*(2510)
DATA PROCESSING DIGEST. Data Processing Digest Inc., 6820 La Tijera Boulevard, Los Angeles, California 90045, 1955-, (Monthly, with annual cumulative index).

*(3580)
FUNK AND SCOTT INDEX OF CORPORATIONS AND INDUSTRIES: SECTION 1 - INDUSTRIES AND PRODUCTS. Predicasts Inc., 200 University Circle Research Center, 11001 Cedar Avenue, Cleveland, Ohio, 1962-, (Annually).

*(4270)
Harrison, Annette. "The Problem of Privacy in the Computer Age: An Annotated Bibliography." RM-5495-PR/RC, RAND Corporation, Santa Monica, California 90406, December 1967, 125 pp.

*(4280)
Harrison, Annette. "The Problem of Privacy in the Computer Age: An Annotated Bibliography - Volume 2." RM-5495/1-PR/RC, RAND Corporation, Santa Monica, California 90406, December 1969, 148 pp.

*(4560)
Hoffman, Lance J. "Computers and Privacy: A Survey." COMPUTING REVIEWS, June 1969, pp. 85-103.

*(4970)
IEEE TRANSACTIONS ON COMPUTERS. Institute of Electrical and Electronic Engineers Inc., 345 East 47th Street, New York, New York 10017, 1968-, (Monthly, with annual cumulative index).

*(5530)
Koung, Javier F. COMPUTER SECURITY, AUDITING AND CONTROLS - A BIBLIOGRAPHY. Management Advisory Publications, P.O. Box 151, Wellesley Hills, Massachusetts 02181, 1973, $7.50.

*(7630)
QUARTERLY BIBLIOGRAPHY OF COMPUTERS AND DATA PROCESSING. Applied Computer Research, 8900 North Central Avenue, Phonix, Arizona 85020, 1971-, (Quarterly, with annual and semi-annual cumulations).

*(7720)
READER'S GUIDE TO PERIODICAL LITERATURE. The H. W. Wilson

Company, New York, New York, 1900-, (Monthly, with annual cumulations).

*(----)
TRW Systems Group: Computer Bibliography. (Unpublished).

*(9400)
Van Tassel, Dennis. COMPUTER SECURITY MANAGEMENT. Prentice-Hall Inc., Englewood Cliffs, New Jersey 17632, April 1972, 220 pp., $10,50.

*(9600)
Warner, Malcolm; and Stone, Michael. THE DATA BANK SOCIETY: ORGANIZATIONS, COMPUTERS, AND SOCIAL FREEDOM. George Allen and Unwin Ltd., Ruskin House, Museum Street, London, England, 1970, 244 pp.

*(9920)
Witzer, Harold. "Computer Security Bibliography." AVCO Computer Services, 201 Lowell Street, Wilmington, Massachusetts 01887, January 1971, 133 pp., $3.50.