Bibliography

This bibliography of computer security documents was prepared by the National Computer Security Association. Corrections and additions will be appreciated. Please write us at Suite 309, 4401-A Connecticut Avenue, NW, Washington DC 20008. Or call voice at (202) 364-1304. Our BBS number: (202) 364-8252.

Access Control/Fence Industry Monthly Newsletter From Communication Channel Inc. 6255 Barfield Road Atlanta, GA 30328 (404) 256-9800 $26.95 This newsletter provides a listing of products and suppliers for the access control industry.

Adler, Stacy "7 Myths of Computer Security." Security vol 24 no. 1 January 1987 pp. 50-52 This article covers consultants that clear misconceptions about data protection software.

Armstrong, James R. "Protecting the Corporate Data." Data Processing & Communications Security vol 9 no. 4 March/April, 1985 pp. 16-17 This article discusses how most alternative off-site lack the environmental control, security and accessibility needed. Includes a discussion on things to consider in selecting an off-site storage facility.

American Society for Industrial Security, Washington, D.C. Chapter Newsletter Monthly Newsletter From American Society for Industrial Security 1655 N. Ft. Myer Drive Suite 1200 Arlington, VA 22209 (703) 522-5800 Free to members only. This newsletter provides current information on industrial security.

Anon. "Computer "Hacking" is No Longer Just a Lark." Office vol 102 no. 3 September 1985 pp. 90-95 Computer hackers will use computers to obtain information and resell it, use it for blackmail, extortion, and espionage. This article discusses techniques for preventing hackers from getting on a system, and monitoring them if they are discovered.

Anon. "Computer Security: The Menace is Human Error." Office vol 99 no. 3 March 1984 pp. 119-120 This article stresses that managers should understand that data security is a people problem and not a computer problem. People are the ones that either accidentally or intentionally misuse a computer system.

Anon. "Internal Security." PC Week vol 2 no. 18 May 1985 pp. 89-91, 106-107 Experts feel that local computer access is more prone to intrusion than long-distance access. This article discusses how insiders in a company are the ones most likely to abuse a computer system.

Anon. "Reporting Computer Crime." Data Processing & Communications Security vol 8 no. 6 July/August 1984 pp. 20-21 This

article presents a suggested format for a final report to use in documenting actions surrounding a computer crime.

Anon. "Communications and Systems Security." Data Processing & Communications Security vol 9 no. 3 1985 Buyer's Directory pp. 11-13 This article discusses a wide variety of communications and system security protection methods. Includes encryption, fiber optics, key management, optical links, electrical emanations, and dial-up access protection devices.

Anon. "Computer Communications Security Lexicon." Data Processing & Communications Security vol 11 no. 2 Spring 1987 pp. 22-23 This article is an update containing some new added security definitions of terms and phrases.

Anon. "Controlling Access To Your Data." Personal Computing vol 9 no. 9 September 1985 pp. 60-72 Explains measures that can be taken to protect what's in a computer. Focuses not only on vandals, but also on people who accidentally harm the computer.

Anon. "Dial-Up Access Security Products." Data Processing & Communications Security vol 9 no. 2 November/December 1984 pp. 21-24 This article presents some new dial-up access security products and their major features.

Anon. "Enhancements Out For Barrier Security Devices." Computerworld vol 18 no. 35 August 1984 pp. 51 This article discusses the password protection device designed by International Anasazi, Inc. that will limit access on dial-up lines.

Anon. "Firesign Unwraps Security Feature." MIS Week vol 5 no. 23 June 1984 pp. 24 This article discusses Firesign Computer Company's product that provides for network security by its password system.

Anon. "Security Computer Outsmarts Colorado Bandits." Data Management vol 19 no. 7 July 1981 pp. 17-18 This article looks at the effectiveness of a security system that controls access to several high-rise buildings in Colorado.

Anon. "Security Lock Ready for PCs." MIS Week vol 6 no. 26 July 1985 pp. 30 The hard disk security product "Knight Data Security Manager" is discussed. This product allows password protection in a PC.

Anon. "Automated Contingency Planning." Data Processing & Communications Security vol 8 no. 4 March/April 1984 pp. 22 This article presents a special purpose software package CHI/COR that deals with the job of documenting the resources needed to implement a disaster recovery plan.

Anon. "Contingency Planning and the Law." Data Processing & Communications Security vol 8 no. 4 March/April 1984 pp. 17-18 This article reviews the Foreign Corrupt Practices Act and its requirement for record keeping and internal controls. Other potential legal liabilities are also reviewed.

Anon. "Computer Power and Environmental Controls." Data Processing & Communications Security vol 9 no. 3 1985 Buyer's Directory pp. 13 This article discusses common power anomalies and equipment available to overcome them.

Anon. "Computer Back-up Facilities." Data Processing & Communications Security vol 8 no. 4 March/April 1984 pp. 19-22 This article discusses the options of back-up sites including cold sites, hot sites, or empty shell, or fully equipped recovery sites. Also refers to the extent of equipment, space, and services provided by these back-up facilities.

Anon. "Computer Security: Issues and Answers." Datamation vol no. September 15, 1984 pp. 16 Pages This 16-page section sponsored by the Computer Security Institute contains several articles that cover a variety of computer security issues.

Anon. "Computer Security: Issues and Answers." Datamation vol no. September 15 1985 pp. 24 Pages This advertisement section contains eight articles that discuss a variety of computer security issues. The authors include FBI Director William Webster and Department of Defense Computer Security Center Director Robert Brotzman.

Anon. "Making The Case For Computer Security Pure and Simple." Datamation vol no. September 1983 pp. This section of Datamation is sponsored by the Computer Security Institute and covers a broad range of computer security issues in several different articles.

Anon. "Personal Computers vs. Data Security: the Two Need Not Be Incompatible." Data Processing & Communications Security vol 12 no. 1 Winter 1988 pp. 24-26 This article discusses the threat of data loss either intentional or unintentional. It examines the significant risks and the data security policies to lower these risks.

Anon. "Protecting Information and Interest." Computer Management vol no. October 1981 pp. 33-34, 36 Suppliers, consultants, and services related to computer security are listed in this directory.

Anon. "Simple Security Precautions Ensure Information Safety." Computerworld vol 19 no. 17 April 1985 pp. SR-38 This article applies many of the security precautions for mainframes to the microcomputer.

MICROCOMPUTER SECURITY

Anon. "Memo: Disaster Plan For Microcomputer Users." Data Processing & Communications Security vol 8 no. 4 March/April 1984 pp. 27-29 This article is in the form a memo containing a microcomputer disaster recovery checklist. It address issues that should be taken in contingency plans.

Anon. "Media Safes: Countering the Threats of Fire." Data Processing & Communications Security vol 9 no. 6 July/August 1985 pp. 18-20 This article is a review of critical basic information on how to select fire resistant media safes.

Anon. "Protecting The World's Largest Computer User." Data Processing & Communications Security vol 8 no. 4 March/April 1984 pp. 25-26 This article discusses a new high security off-site storage facility opening in Beltsville, Maryland. It also address concern with the lack of proper security storage today.

Anon. "Computer Security Awareness: Organizations and Senior." Management Concerns Data Processing & Communications Security vol 8 no. 5 May/June 1984 pp. 12-13 This article gives the result of a survey of general security and computer security personnel, EDP auditors, and internal auditors to determine the computer security awareness of their company and senior management.

Anon. "Records Storage and Management." Data Processing & Communications Security vol 8 no. 4 March/April 1984 pp. 23-25 This article addresses the questions which records should be stored off-site, and how can an off-site facility be evaluated? It also provides an overview of areas to consider.

Anon. "Computer Security Software." Data Processing & Communications Security vol 9 no. 1 September/October 1984 pp. 19-24 This article provides information for using access control software to protect the terminals, the data and the system itself from unauthorized use.

Anon. "Computer Security Software." Data Processing & Communications Security vol 9 no. 3 1985 Buyer's Directory pp. 17-18 This article addresses a wide variety of computer security software programs and their different uses.

Anon. "Protecting Software With Escrow Services." Data Processing & Communications Security vol 8 no. 5 May/June 1984 pp. 22-24 This article addresses some of the problems and answers for protecting software that concerns major management today.

Ashley, Cliff and Story, Frank Automatic Data Processing Security Program From Kaiser Engineers Hanford, ATTN: Cliff Ashley, SAS Manager February 11, 1987 Training & Awareness Free This manual describes the computer security program used at Kaiser Engineers Hanford.

Associated Press "Jury Selection In 1st "Virus" Trial Begins." Washington Post vol no. 277 September 7, 1988 pp. C1 This article is about a programmer accused of using a computer "virus" to sabotage thousands of records at his former work place.

Atkinson, L.V. "Fraud: Input Data Most Vulnerable." Computerworld UK vol 2 no. 21 September 2, 1981 pp. 10 Article discusses a survey which found that the major danger to computers was the alteration of input data.

Auerbach Data Security Management Bimonthly Journal From Auerbach Publishers Inc. 6560 N. Park Drive Pennsauken, NJ 08109 (609) 662-5599 $265.00 Annually This journal deals with issues related to data security management.

Auerbach Information Management Series Monthly Journal From Auerbach Publishers, Inc. 6560 N. Park Drive Pennsauken, NJ 08109 (609) 662-2070 $750.00 Annually This journal on information security provides insights, approaches, and products related to security.

Avarne, Simon "How to Find Out a Password." Data Processing & Communications Security vol 12 no. 2 Spring 1988 pp. 16-17 This article gives examples of how to discover someones password and discusses weaknesses of traditional passwords.

Baker, R.H. "Lining Up Computer Crooks." Micro Communications vol 2 no. 5 May 1985 pp. 18-22 This article looks at crime patterns of microcomputer users breaking into mainframes. Ways in which these patterns can be learned and then stopped is discussed.

Bailey, Cynthia "Information Security: A Pressing Need" Computer Digest, September, 1989, p. 30, 32.

Bass, Brad "Security Teams Fight Network Invaders" Government Computer News, September 4, 1989, p. 87.

Beitman, L. "A Practical Guide To Small Business Computer Security." Office vol 96 no. 2 August 1982 pp. 86, 90 This article gives advice on how to obtain computer security in a small business environment. A checklist is included that will help to prevent accidental and intentional harm to a system.

ben-Aaron, Diana. "Mailsafe Signs, Seals, and Delivers Files" InformationWeek, September 15, 1986.

Bequai, A. "What to do About Crime in the Electronic Office." Office vol 101 no. 1 January 1985 pp. 101-104 This article discusses the important role that auditing computer systems plays in preventing crimes and abuse.

Bequai, August "Federal Computer Crime Legislation is Needed." Data Management vol no. May 1981 pp. 22-24 The ways criminals use loopholes in our present criminal justice system is discussed along with a history of computer crime legislation.

Berman, A. "Evaluating On-Line Computer Security." Data Communications vol 12 no. 7 July 1983 pp. 145-152 The security problems that have arisen because of on-line processing are discussed in this article. Covered are the two ways to obtain a secure on-line system.

Betts, M. "Government's Computers "Highly Vulnerable" to Abuse." Computerworld vol 18 no. 40 October 1984 pp. 4 Discusses how highly vulnerable the federal government's computers are to abuse, and a congressman who is seeking to change that vulnerability.

Betts, M. "NBS Releases Standards For Managing Password Security." Computerworld vol 19 no. 28 July 1985 pp. 19 This article talks about how the National Bureau of Standards has completed a two- part publication dealing with password systems.

Betts, M. "U.S. Agency Faces Probes, Boosts Security After Audit." Computerworld vol 19 no. 24 June 1985 pp. 8 This article discusses an audit report issued by the inspector general of the U.S. Department of the Interior in March 1985 which revealed inadequate controls over passwords, faulty operating procedures, and lack of audit trails by the Denver Service Center.

Betts, M. "Reagan Systems Security Directive Under Attack." Computerworld vol 19 no. 27 July 1985 pp. 1 This article discusses why members of congress are concerned over how the National Security Decision Directive 145 on computer security could be abused by military and intelligence officials.

Betts, Kellyn S. "Foiling Data Thieves" Modern Office Technology April 1985, pp 112 ff.

Bezdek, J. "Across-the-Board Training Protects Data." Computerworld vol 18 no. 44 October 1984 pp. SR-10 This special report covers the four areas that a training program in computer security needs to

include. These are plant physical security, logical security, administrative security, and the legal and social aspects of security training.

Bigelow, R.P. "Computer Security And Law." Infosystems vol 29 no. 12 December 1982 pp. 84 This article looks at how a memo from the legal department should be structured concerning the protection of assets.

Blakeney, S. "Computer Crime: A Worldwide Concern." Computerworld vol 17, 18 no. 52, 1 December 26, 1983, January 1984 pp. 57-60 This article looks at computer crime as a worldwide problem. The most common types of computer crimes are given along with the estimated losses in various countries throughout the world.

Blakeney, S. "Micro Market Going Full Steam Ahead; IDC Predicts Installed Base of $41.9 Billion by '86" Computerworld March 28, 1983.

Boebert, W. E., Kain, R.Y. A Practical Alternative to Hierarchical Integrity Policies Proceeding of the 8th National Computer Security Conference, Gaithersburg MD, Oct 1985

Boebert, W. E., Ferguson, C.T. A Partial Solution to the Discretionary Trojan Horse Problem Proceeding of the 8th National Computer Security Conference, Gaithersburg MD, Oct 1985

Bologna, Jack "Computer Related Crime: The Who, What, Where, When, Why and How." Data Processing & Communications Security vol 10 no. 1 Winter 1986 pp. 19-23 This article looks at computer related crime from the perspectives of the individual criminal, environmental factors, organization cultures, incidence rate, and security countermeasures.

Bologna, Jack Computer Crime: Wave of the Future Intended to demonstrate that the current state of computer technology exceeds by an order of magnitude our ability to secure our equipment. 102 pp $15. Computer Protection Systems.

Bologna, Jack The Security Manager's Handbook 167 pp. $35 Computer Protection Systems.

Bologna, Jack Strategic Planning for Corporate Directors of Security and Risk Management. 28 pp $10 Computer Protection Systems.

Bologna, Jack "Forensic Accounting." Data Processing & Communications Security vol 8 no. 6 July/August 1984 pp. 16-20 This article identifies the skills and competency of a forensic accountant.

Bologna, Jack "Disaster/Recovery Planning: A Qualitative Approach."

Data Processing & Communications Security vol 8 no. 4 March/April 1984 pp. 11-15 Developing a disaster/recovery plan usually involves a detailed quantitative risk analysis; the author offers a more qualitative approach that is less time consuming and will obtain a higher level of commitment from management, D/P staff, and users.

Bologna, Jack "Industrial Security In a Nutshell: A Risk by any Other." Name Data Processing & Communications Security vol 9 no. 5 May/June 1985 pp. 12-13 This article discusses properly understanding risk and how the opposite side of risk is opportunity for growth and development.

Bologna, Jack "Risk Assessment Guidelines for Fidelity Insurance." Data Processing & Communications Security vol 9 no. 4 March/April, 1985 pp. 18-20 This article is a review of the adequacy of asset protection plans, policies, procedures and controls to enlighten top management.

Bologna, Jack "Security Planning: The "Tapps" Method." Data Processing & Communications Security vol 10 no. 4 Fall 1986 pp. 7-11 This article covers a system approach to assets protection. It discusses an analytical process called Total Assets Protection Planning System (TAPPS) which consist of organization, structure and mandate of the security function.

Bologna, Jack "Selling Computer Security to Top Management." Data Processing & Communications Security vol 8 no. 5 May/June 1984 pp. 13-16 This article discusses positive motivational impact, minimizing risk, and cost feasibility in selling computer security to top managers.

Bologna, Jack "Why the Corporate Security Function is Being Downsized." Data Processing & Communications Security vol 11 no. 2 Spring 1987 pp. 20-21 This article discusses the disbanding and dilution of corporate security functions and how this effects the security of a firm.

Bound, W.A.J. "Security Protecting Information Resources and Media." Information Management vol 18 no. 8 August 1984 pp. 18-19 This article discusses what a manager must consider when designing an office security program to protect against the four vulnerabilities of a system: personnel, physical, administrative, and technical.

Bowmen, Terry "Undercarpet Fiber Optics." Data Processing & Communications Security vol 11 no. 2 Spring 1987 pp. 23-26 This article discusses how fiber optics offer better security than copper cable undercarpet. It also includes how to plan an undercarpet system.

Bramer, W.L. "Computer and Data Security is Battle Cry to the '80s."

Office vol 103 no. 3 March 1986 pp. 78-82 This article discusses the number of organizations that are looking at their security procedures and programs to deter computer abuse. The three main causes of security problems are described.

Branstad, Dennis (editor) Computer Security And The Data Encryption Standard February 1978 NBS SPEC PUB 500-27 Includes papers and summaries of presentations made at a 1978 conference on computer security. Subject areas are physical security, risk assessment, software security, computer network security, applications and implementation of the Data Encryption Standard.

Brenner, Aaron. "LAN Security". LAN Magazine, Aug 1989.

Bunzel, Rick. "Flu Season" Connect, Summer 1988.

Burger, Ralf .Computer Viruses:a High-Tech Disease Abacus Software, 1989. For some reason, this book contains virus source code!

Cabell, D. "Network Backups." Micro Communications vol 2 no. 6 June 1985 pp. 14-18 This article describes how the only way to protect a LAN, micro, mini, or mainframe from a complete system crash is adequate backup.

Call, B. "Buttress Against Computer Crime." PC Week vol 2 no. 18 May 1985 pp. 111, 115 The physical protection of computers is becoming an area of interest for more organizations. The increased number of physical security devices illustrates this point and is discussed in this article.

Carey, Cameron "Data Access Control: Help or Hindrance." Data Processing & Communications Security vol 11 no. 4 Fall 1987 pp. 18-20 This article discusses limiting access to data and how to make access control protection more of a help than a hindrance by developing a set of priorities about various classes of data.

Cipher Irregular Newsletter From Institute of Electrical and Electronic Engineers 9800 Savage Road Fort Meade, MD 20755 (301) 859-4376 This newsletter looks at security and privacy from a technical view.

Ciura, J.M. "Vital Records Protection: Identifying Essential Information." Information Management vol 19 no. 2 February 1985 pp. 11 This article suggest that the best way to resume business activity after an emergency or disaster is to have a vital records protection program.

Clauss, Karl H. "How To Move A Data Center and Avoid a Disaster." Infosystems vol no. December 1981 pp. 46-48, 50 This article describes

how ARCO Oil and Gas Company moved their computer center to a new location and the points a company should consider when moving a data center.

Clyde, Allen R. "Insider Threat on Automated Information Systems." Data Processing & Communications Security vol 11 no. 4 Fall 1987 pp. 11-14 This articles discusses activities to detect sources of abuse that are not widely implemented.

CM Bulletin Bimonthly Bulletin From National Classification Management Society, Inc. 6116 Roseland Drive Rockville, MD 20852 (301) 231-9191 Free to members, non-members $15.00 annually This bulletin contains articles pertaining to information security management.

Cohen, Fred. Computer Viruses, Theory and Experiments. 7th Security Conference, DOD/NBS Sept 1984.

Cohen, Fred. "Computer Viruses: Theory and Experiment." Computers & Security, Vol. 6 (1987), pp. 22-35.

Cohen, Fred. "On the Implications of Computer Viruses and Methods of Defense," Computers & Security, Vol. 7 (1988), pp. 167-184.

Cole, Gerald D. and Frank Heinrich Design Alternatives For Computer Network Security (vol. 1) The Network Security Center: A System Level Approach To Computer Network Security (vol. 2) January 1978 NBS SPEC PUB 500-21 This two-volume study covers network security requirements and design and implementation requirements of a special computer dedicated to network security. The approach utilizes a dedicated minicomputer to check authentication of network users, and, to some extent, to check authorization. The study focuses on use of the Data Encryption Standard to protect network data and recommends procedures for generating, distributing and protecting encryption keys.

Collins, J.A. "Continuous Security Control Clamps Down on Abuse." Data Management vol 23 no. 5 May 1985 pp. 56-59 The need for computer access is discussed in this article that suggest that such access should be a management, security-oriented process. Computer security guidelines are also given.

COM-AND (Computer Audit News and Developments) Bimonthly Newsletter From Management Advisory Services P.O. Box 151 57 Greylock Road Wellesley Hills, MA 02181 (617) 235-2895 $56.00 Annually This newsletter provides auditors with current trends, practices, and developments in their field.

Computer Age: EDP Weekly Weekly Newsletter From EDP News

Services, Inc. 7043 Wimsatt Road Springfield, VA 22151 (703) 354-9400 $225.00 Annually Weekly roundup of computer industry news. Provides analysis of computer events and trends. Articles include coverage of computer security news.

Computer Fraud & Security Bulletin Monthly Newsletter From Elsevier International 52 Vanderbilt Avenue New York, NY 10017 (212) 916-1250 $240.00 Annually This monthly newsletter deals with computer crime and preventive measures that can be taken to avoid misuse.

Computer Law Journal None Specified Journal From Center for Computer Law Box 3549 Manhattan Beach, CA 90266 (213) 372-0198 $72.00 Annually This journal deals with all aspects of computer law from copyright protection of software to penalties for abusing computers.

Computer Law Newsletter Bimonthly Newsletter From Warner & Stackpole 28 State Street Boston, MA 02109 (617) 725-1400 Free Various subjects dealing with computer law including computer crime are covered.

Computer Security Buyers Guide From Computer Security Institute 1988 General Security Members of CSI - Free; Non-members - $75.00 A buyers guide for a wide variety of of computer security products and services.

Computer Security Digest Monthly Digest From Computer Protection Systems, Inc. 150 N. Main Street Plymouth, MI 48170 (313) 459-8787 $110.00 Annually This digest addresses issues of current interest in the area of computer security matters and related crime.

Computer Security Guidelines For Implementing The Privacy Act Of 1974 FIPS PUB 41 May 1975 Provides guidance in the selection of technical and related procedural methods for protecting personal data in automated information systems. Discusses categories of risks and the related safeguards for physical security, information management practices, and system controls to improve system security.

Computer Security Journal Twice A Year Journal From Computer Security Institute 360 Church Street Northborough, MA 01532 (617) 393-2600 $60.00 members, $65.00 non-members annually This journal contains technical papers on a wide variety of computer security related topics including software, contingency planning, and security management.

Computer Security Manual for Unclassified Systems From EG&G Idaho, Inc. Information and Technical Services P.O. Box 1625 Idaho

Falls, ID 83415 April 30, 1987 General Security Call for current cost (TBD) Discusses a variety of unclassified computer security issues. Includes password usage, certification and other categories.

Computer Security Newsletter Bimonthly Newsletter Computer Security Institute 360 Church Street Northborough, MA 01532 (617) 393-2600 $95.00 Annually, for members only. This newsletter covers a broad range of computer security topics.

Computer Viruses - Proceedings of an Invitational Symposium, Oct 10/11, 1988; Deloitte, Haskins, and Sells; 1989

Computers & Security Six Times a Year Journal From Elsevier International 52 Vanderbilt Avenue New York, NY 10017 (212) 916-1250 $89.00 Annually This technically oriented journal covers a variety of topics concerning computer security.

COM-SAC (Computer Security, Audit, and Control) Twice A Year Journal From Management Advisory Services & Publications P.O. Box 151 57 Greylock Road Wellesley Hills, MA 02181 (617) 235-2895 $55.00 Annually Most of this journal contains brief digests of articles on computer security that have appeared in other publications, although it does include some original articles.

Coontz, Constance "Protection through Isolation." Security Management vol 31 no. 11 November 1987 pp. 53-55 This article discusses compartmentalizing valuable data on dedicated PCs or small computer systems to help protect it from hackers and moles.

CPR-R (Contingency Planning & Recovery Report) Quarterly Journal From Management Advisory Services P.O. Box 151 57 Greylock Road Wellesley Hills, MA 02181 (617) 235-2895 $75.00 annually This journal is solely devoted to issues, practices and developments in contingency planning, disaster recovery and business continuity.

Data Encryption Standard FIPS PUB 46 January 1977 Specifies an algorithm to be implemented in electronic hardware devices and used for the cryptographic protection of sensitive, but unclassified, computer data. The algorithm uniquely defines the mathematical steps required to transform computer data into a cryptographic cipher and the steps required to transform the cipher back to its original form.

Datapro Reports on Information Security (2 Volumes) From Datapro Research Corporation (609) 764-0100 1985 General Security $790.00 Annualy Includes management information, market surveys, and product reports.

Data Processing & Communications Security Quarterly Magazine From

Assets Protection Publishing Box 5323 Madison, WI 53704 (608) 274-7751 $48.00 Annually This magazine covers a wide variety of computer and communications security related topics.

Data Processing Digest Monthly Digest From Data Processing Digest, Inc. P.O. Box 1249 Los Angelas, CA 90078 (916) 756-5138 This digest covers more than 130 scientific, business trade, educational, and computer journals. Articles are selected for the specific needs of DP and IS management, computer professionals, and corporate executives.

Davidson, Thomas L. and White, Clinton E. Jr. "How to Improve Network Security." Infosystems vol 30 no. 6 June 1983 pp. 110-112 This article discusses the need to protect network systems using software locks, authorization schemes, logs, and data encryption.

Daview, D.W. & W.L. Price Security for Computer Networks: An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer. John Wiley & Sons. 416 pp 1984. $34.95

Deitz, Larry "Computer Security in the Micro Age" Computers and Electronics, June 1984, pp 68 ff

Denning D. E. Cyptography and Data Security Addison Wesley, 1982

Denning, D. E. An Intrusion-Detection Model IEEE Symposium on Security and Privacy, April 1986.

Denning, Peter J.. "Computer Viruses". American Scientist, Vol 76, May-June, 1988.

Denning, Peter J. "The Internet Worm". American Scientist, Vol 77, March-April, 1989.

DES Modes Of Operation FIPS PUB 81 December 1980 Defines four modes of operation for the Data Encryption Standard which may be used in a wide variety of applications. The modes specify how data will be encrypted (cryptographically occurrence and the damage protected) and decrypted (returned to original form). The modes included in this standard are the Electronic Codebook (ECB) mode, the Cipher Block Chaining (CBC) mode, the Cipher Feedback (CFB) mode, and the Output Feedback (OFB) mode.

Dewdney, A. K. "Computer Recreations - In the game called Core War hostile programs engage in a battle of bits". Scientific American Mar 1984.

Dewdney, A. K. "Computer Recreations - A Core War bestiary of viruses, worms and other threats to computer memories". Scientific

American Mar 1985.

Diamond, F.H. "Computer Network Security: The Need Was Never Greater." Office vol 102 no. 2 August 1985 pp. 94-99 This article discusses the advantages of using the callback approach in computer networks to prevent hackers from getting onto a system.

Dobberstein, M. "To Have and Not to Have a Disaster." Computer Decisions vol 17 no. 18 September 1985 pp. 102-126 This article deals with the importance of actually testing contingency plans to see if they work.

DoD Department of Defense Trusted Computer System Evaluation Criteria, December, 1985. DOD 5200.28-STD. Library No. S225,711. (the "Orange Book")

DoD Computer Security Center Computer Security Requirements: Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments DoD. CSC-STD-003-85. 25 June, 1985, 13pp. *

Dvorak, John "Virus Wars: A Serious Warning". PC Magazine Feb 29, 1988.

EDP Security Bulletin Irregular Bulletin From Royal Canadian Mounted Police Systems Branch 1200 Alta Vista Drive Ottawa, ON KIA OR2 Canada This bulletin provides current information in the field of electronic data processing security.

edpacs: The EDP Audit, Control and Security Newsletter Monthly Newsletter From Auerbach Publishers 210 South Street Boston, MA 02111 (617) 292-8360 $96.00 Annually This newsletter is meant primarily for the auditor, although it will benefit others with computer security responsibility.

EDP Analyzer Monthly Journal From United Communications Group 4550 Montgomery Avenue Ste. 700N Bethesda, MD 20814 (301) 961-8700 Doug O'Boyle $159.00 annually

The EDP Auditor Quarterly Journal From EDP Auditors Association P.O. Box 88180 373 S. Schmale Road Carol Stream, IL 60188-0180 (312) 682-1200 Available as part of annual membership. This journal is intended for the EDP auditor and focuses on education and research.

Edwards, M. "The Sting in a Micro's Tail." Practical Computing vol 6 no. 12 December 1983 pp. 108-109 How criminals exploit information technology is described in this article along with ways to stop them.

Elmer-Dewitt, Phillip "Invasion of the Data Snatchers!." Time Magazine vol 123 no. 13 September 26, 1988 pp. 62-67 Discusses the current threat to computer systems posed by computer viruses. Computer viruses are defined and several examples of viruses are given.

Epner, S.A. "Computer Security: Plenty of Questions but No Easy Answers." Office vol 101 no. 3 March 1985 pp. 74-76 This article covers the physical security of computer equipment including air conditioning and power to pass cards and security guards.

Edwards, J. "Ends in Sight for the Copy-Protection Debate." PC Week vol 3 no. 1 January 1986 pp. 101 & 105 This protection of software from unauthorized use may be coming to an end as Microsoft Corporation has decided to lift the protection from several of its software programs.

Federal Information Processing Standards Publication 83, Guideline on User Authentication Techniques for Computer Network Access Control. National Bureau of Standards, Sept, 1980.

Federal Information Processing Standards Publication 73, Guidelines for Security of Computer Applications; National Bureau of Standards, June, 1980.

Federal Information Processing Standards Publication 112, Password Usage. National Bureau of Standards, May, 1985.

Federal Information Processing Standards Publication 87, Guidelines for ADP Contingency Planning; National Bureau of Standards, March, 1981.

Fiedler, David and Hunter, Bruce M. UNIX System Administration. Hayden Books, 1987

Fisher, M.J. "New Security Device "Fingers" Culprit." MIS Week vol 6 no. 35 September 1985 pp. 12 This article describes a new product that uses a fingerprint device to verify a user's identity and then allow access on the computer system.

Fisher, Sharon "DARPA Sets Up Response Teams to Tackle ARPANET Emergencies" InfoWorld, March 20, 1989, p. 43.

Fitzgerald, Jerry. Business Data Communications: Basic Concepts, Security, and Design. John Wiley and Sons, Inc., 1984

Flach, Joseph P. "Increasing Programming Efficiency While Preventing the "F" Word." Data Processing & Communications Security vol 11 no.

4 Fall 1987 pp. 15-17 This article gives examples of ways to identify fraudulent code in a production program.

Flynn, L. "Data Security: How Much is Too Much?" InfoWorld, March 20, 1989, p. 41-43.

Fong, Elizabeth A Data Base Management Approach To Privacy Act Compliance June 1977 NBS SPEC PUB 500-10 Discusses how commercially available data base management systems can be used to implement Privacy Act requirements for the handling of personal data.

Forensic Accounting Review Monthly Newsletter From Computer Protection Systems, Inc. 150 N. Main Street Plymouth, MI 48170 (313) 459-8787 $110.00 Annually This newsletter takes an in-depth look at the problems of computer fraud and provides possible solutions.

Gait, Jason Maintenance Testing For The Data Encryption Standard August 1980 NBS SPEC PUB 500-61 Describes four tests that can be used by manufacturers and users to check the operation of data encryption devices. These tests are simple, efficient, and independent of the implementation of the Data Encryption Standard (FIPS 46).

Gait, Jason Validating The Correctness Of Hardware Implementations Of The Nbs Data Encryption Standard November 1977 NBS SPEC PUB 500-20 Describes the design and operation of the NBS testbed that is used for the validation of hardware implementations of the Data Encryption Standard (DES). This report provides the full specification of the DES algorithm, a complete listing of the DES test set and a detailed description of the interface to the testbed.

GAO: "Financial Integrity Act: Actions Needed to Correct ADP Internal Control Weaknesses"

GAO: "Computer Security: Compliance with Training Requirements of the Computer Security Act of 1987"

Gasser, Morrie. Building a Secure Computer System. Van Nostrand Reinhold, New York, 1988.

Gaydasch, Alexander "Postimplementation Audits - A Quick, Easy Approach." Data Management vol no. February 1983 pp. 54, 55, 69 This article describes post- implementation audits and how they help to determine whether a computer system has met its original criteria.

Gazarek, Kenneth F. "Cabinets for Electromagnetic Interference/Radio-Frequency Interference and TEMPEST Shielding." Data Processing & Communications Security vol 9 no. 6 July/August 1985 pp. 12-13 This article discusses the electromagnetic interference

and radio-frequency interference control options, designing and building metal cabinets that provide effective shielding.

Gilgor, V.D. On the Design and the Implementation of Secure Xenix Workstation IEEE Symposium on Security and Privacy, April 1987.

Glossary For Computer Systems Security February 1974 FIPS PUB 39 Evaluating security of computer systems. A reference document containing approximately 170 terms and definitions pertaining to privacy and computer security.

Goldstein, Bruce "Information Security: The Information Resource Management." Approach Data Processing & Communications Security vol 8 no. 5 May/June 1984 pp. 18-22 This article addresses information as a asset that must be protected as any other asset. It also discusses information research management providing the framework for a comprehensive information security program.

Grampp, F.T. and Morris, R. H. "UNIX Operating System Security". AT&T Bell Laboratories Technical Journal, Oct 1984.

Guidelines For Adp Contingency Planning FIPS PUB 87 March 1981 Describes what should be considered when developing a contingency plan for an ADP facility. Provides a suggested structure and format which may be used as a starting point from which to design a plan to fit each specific operation.

Guidelines For Adp Physical Security And Risk Management June 1974 FIPS PUB 31 Provides guidance to Federal organizations in developing physical security and risk management programs for their ADP facilities. Covers security analysis, natural disasters, failure of supporting utilities, system reliability, procedural measures and controls, protection of off-site facilities, contingency plans security awareness, and security audit. Can be used as a checklist for planning.

Guidelines For Automatic Data Processing Risk Analysis FIPS PUB 65 August 1979 Presents a technique for conducting a risk analysis of an ADP facility and related assets. Provides guidance on collecting, quantifying, and analyzing data related to the frequency of caused by adverse events. This guideline describes the characteristics and attributes of a computer system that must be known for a risk analysis and gives an example of the risk analysis process.

Guideline For Computer Security Certification And Accreditation FIPS PUB 102 September 1983 Describes how to establish and how to carry out a certification and accreditation program for computer security. Certification consists of a technical evaluation of a sensitive system to see how well it meets its security requirements. Accreditation is the

official management authorization for the operation of the system and is based on the certification process.

Guideline On Electrical Power For Adp Installations FIPS PUB 94 September 1982 Provides information on factors in the electrical environment that affect the operation of ADP systems. Describes the fundamentals of power, grounding, life-safety, static electricity, and lightning protection requirements, and provides a checklist for evaluating ADP sites.

Guidelines On Evaluation Of Techniques For Automated Personal Identification FIPS PUB 48 April 1977 Discusses the performance of personal identification devices, how to evaluate them and considerations for their use within the context of computer system security.

Guidelines For Security Of Computer Applications FIPS PUB 73 June 1980 Describes the different security objectives for a computer application, explains the control measures that can be used, and identifies the decisions that should be made at each stage in the life cycle of a sensitive computer application. For use in planning, developing and operating computer systems which require protection. Fundamental security controls such a data validation, user identity verification, authorization, journalling, variance detection, and encryption are discussed.

Guidelines For Implementing And Using The Nbs Data Encryption Standard FIPS PUB 74 April 1981 Provides guidance for the use of cryptographic techniques when such techniques are required to protect sensitive or valuable computer data. For use in conjunction with FIPS PUB 46 and FIPS PUB 81.

Guidelines On Integrity Assurance And Control In Database Applications FIPS PUB 88 August 1981 Provides explicit advice on achieving database integrity and security control. Identifies integrity and security problems and discusses procedures and methods which have proven effective in addressing these problems. Provides an explicit, step-by-step procedure for examining and verifying the accuracy and completeness of a database.

Guidelines On User Authentication Techniques For Computer Network Access Control FIPS PUB 83 September 1980 Provides guidance in the selection and implementation of techniques for authenticating the users of remote terminals in order to safeguard against unauthorized access to computers and computer networks. Describes use of passwords, identification tokens, verification by means of personal attributes, identification of remote devices, role of encryption in network access control, and computerized authorization techniques.

Hagopian, Greg "Planning and Implementing a Security Package." Data Processing & Communications Security vol 10 no. 4 Fall 1986 pp. 17-20 This article discusses vendor selection and legal issues.

Harris, N.L. "Rigid Administrative Procedures Prevent Computer Security Failure." Data Management vol 22 no. 12 December 1984 pp. 13-14, 16 The best way to keep a security program from failing is the use of strict administrative procedures. This article also discusses why some systems fail.

Harrison, M.A. and Ruzzo, W.L. Protection in Operating Systems Comm of the ACM, Aug 1976.

Helsing, Cherly W. "Disaster Recovery Options." Security vol 24 no. 7 July 1987 pp. 100-103 This article has suggestions on how to find a recovery plan that fits your firm without damaging your profits.

Highland, Harold J. "From the Editor -- Computer Viruses." Computers & Security, Aug 1987.

Holtzman, Henry "Keeping Your Offices Safe and Sound" Modern Office Technology, May 1985 pp 92 ff.

Highland, Harold J. Protecting Your Microcomputer System. John Wiley & Sons, Inc. N.Y.1984

Horgan, J. "Thwarting The Information Thiefs." IEEE Spectrum vol 22 no. 7 July 1985 pp. 30-41 Many organizations are protecting their communication output from electronic interception by trying to detect and foil the surveillance using a variety of methods.

Hutton's Building System and Controls Catalog From Hutton Publishing Co., Inc. 1988 Environmental Security Free This catalog provides a wide variety of environmental computer security related products and services.

Industrial Security Letter Irregular Newsletter From Defense Investigative Service Directorate for Industrial Security 1900 Half Street, SW Washington, D.C. 20324 Free to qualified readers. This newsletter provides operating procedures for the Defense Industrial Security Program (DISP) operations at cleared facilities.

Inglesby, Tom "Fighting Flash 'n' Flicker" Infosystems November, 1984, pp 88 ff.

Internal Auditor Bimonthly Journal From Institute of Internal Auditors 249 Maitland Avenue Altamonte Springs, FL 32701 (305)

830-7600 $24.00 Annually This journal looks at techniques and principles of internal control and auditing.

Israel, Howard "Computer Viruses: Myth or Reality?". Proceeding of the 10th National Computer Security Conference, Gaithersburg MD, Sept 1987.

Isaac, Irene Guide On Selecting Adp Backup Process Alternatives NBS SPEC PUB 500-134 November 1985 Discusses the selection of ADP backup processing support in advance of events that cause the loss of data processing capability. Emphasis is placed on management support at all levels of the organization for planning, funding, and testing of an alternate processing strategy. The alternative processing methods and criteria for selecting the most suitable method are presented, and a checklist for evaluating the suitability of alternatives is provided.

Jackson, Carl B. "Passwords: Comments from the Information Systems Security Association." Security vol 24 no. 7 July 1987 pp. 105 Discusses relevant security issues and how to bring an appropriate degree of LAN information security to your organization.

Johnson, B. "Criminal Minds Keep Pace with Technology. Stop, Thief!." Computerworld vol 15, 16 no. 52, 1 December 28, 1981, January 4, 1982 pp. This article looks at some of the common problems that the DP industry faces today including computer security, asset protection, and computer fraud prevention.

Johnston, R.E. "What You Need To Know." Infosystems vol 32 no. 1 January 1985 pp. 56 Outlined in this article are those things that should be considered when establishing a computer security program or updating an existing program.

Johnston, Stuart J. "Microsoft OS/2 LAN Manager: Network Access Control Issues Remain" InfoWorld, March 20, 1989, p. 42.

Jordan, Halmuth "The Search for Privacy." Security Management vol 31 no. 11 November 1987 pp. 32-36 This article focuses on some of the difficulties the legal profession is having by looking at American and West German law regarding electronic surveillance.

Joseph, Mark K. "Toward the Elimination of the Effects of Malicious Logic: Fault Tolerance Approaches" Proceeding of the 10th National Computer Security Conference, Gaithersburg MD, Sept 1987

Journal of the National Classification Management Society Annually Journal From National Classification Management Society, Inc. 6116 Roseland Drive Rockville, MD 20852 (301) 231-9191 Free to Members Only Identifies communications and information processing systems

their vulnerabilities and a range of methods for improving the security of these systems.

Karser, Paul A. "Limiting the Damage Potential of Discretionary Trojan Horses" Proceedings of the Symposium on Security and Privacy 1987 Oakland CA, Published by the IEEE.

Kluepfel, Henry M. "Computer Security for the Abuser Friendly Environment." Data Processing & Communications Security vol 9 no. 2 November/December 1984 pp. 16-20 This article discusses the underlying lack of adequate controls in computer systems and their relation to computer abuse and crime.

Koelle, Jim "What's in the Cards?." Security vol 23 no. 12 December 1986 pp. 42-44, and 46 This article discusses microchips and how they promise to revolutionize access card technology with fast, calculating, and advanced memories.

Kontur, J.S. and Letham, L. "Locking Up System Security." Electronic Week vol 58 no. 7 February 18, 1985 pp. 68-72 This article describes a system that cannot be broken into by unauthorized users. It uses a random-number generator and encryption logic.

Korzeniowski, P. "Security Dynamics Releases Two-Part Security System." Computerworld vol 19 no. 42 October 1985 pp. 19, 23 This article discusses a product Security Dynamics has designed that is an inexpensive security protection device which keeps hackers out of systems.

Korzeniowski, P. "ADAPSO Making Progress on Software Protection Device." Computerworld vol 19 no. 24 June 1985 pp. 8 This article discusses how the Association of Data Processing Service Organizations (ADAPSO) is getting ready to announce its progress in creating a software authorization mechanism.

Kull, D. "How to Make Even E.F. Hutton Listen." Computer Decisions vol 17 no. 18 September 1985 pp. 42-50 The most effective way for an organization to prevent breaches in a computer system is to plug the holes that have already been used to violate the system and identify the intruders.

Lapid, Ahituv, and Newmann "Approaches to Handling 'Trojan Horse' Threats" Computer & Security Sept 1986.

LaPlante, Alice "Study Finds IS Managers Are More People-Oriented" InfoWorld, March 20, 1989, p.5

Lasden, Martin "Computer Crime." Computer Decisions vol no. June

1981 pp. 104-106, 108 112, 116, 118, 120, 122, 124 This article discusses actual computer crimes that have taken place and the factors that escalate the risk of an organization from these types of crime.

Lemke, Fred H. "Blackouts and Computer Power Protection." Data Processing & Communications Security vol 12 no. 2 Spring 1988 pp. 19-23 This article is a study that was taken to see emerging patterns of blackouts that may be useful in helping evaluate your level of blackout vulnerability and then set up appropriate levels of power protection for your electronic systems.

Lemke, Fred H. "Computer Power Protection." Data Processing & Communications Security vol 8 no. 4 March/April 1984 pp. 31-33 This article gives examples of how to protect your facility against the harmful effects of an electrical power outage.

Leuser, K.G. "Security Programs: Only as Good as We Make Them." Office vol 100 no. 2 August 1984 pp. 91-92 Discusses how an effective security program helps to foil or discourage people with dishonest intentions. Looks at the office administrator's domain to identify areas of potential vulnerability.

Levitt, Karl N., Peter Neumann, and Lawrence Robinson The SRI Hierarchical Development Methodology (HDM) And Its Application To The Development Of Secure Software October 1980 NBS SPEC PUB 500-67 Describes the SRI Hierarchical Development Methodology for designing large software systems such as operating systems and data management systems that must meet stringent security requirements.

Linden, Jack "Automated EDP Risk Analysis and Management." Data Processing & Communications Security vol 9 no. 1 September/October 1984 pp. 16-18 This article gives a cost effective first step in developing a successful computer security program using a cost benefit analysis approach.

Lobel, J. "Third Decade of Concern." Computerworld vol 16 no. 6 February 8, 1982 pp. 1D/31-34 & 36 The author looks at some of the issues associated with distributed data processing including privacy, crime, and security.

Longley, Dennis and Shain, Michael. Data and Computer Security

Lucas, D. "The Invisible Enemy." Business Computing and Communication vol no. February 1985 pp. 18-20 This article describes how home computer users are breaking into some of Britain's mainframe computers. Various procedures that can protect against intrusion are also discussed by the author.

Lundell, Allan. A video based on his book VIRUS! called VIRUS! The Video. Write him at 175 Flintrock Lane, Ben Lomond, CA 95005.

McCarthy, Charles J. "Passwords." Data Processing & Communications Security vol 10 no. 4 Fall 1986 pp. 13-14 This article discusses the two primary password configurations passwords defined by user, and passwords assigned to a user. It shows the differences between these two from a security view.

McGowan, Kevin J. "Computer Power Protection." Data Processing & Communications Security vol 9 no. 5 May/June 1985 pp. 21-25 This article looks at understanding AC power conditions in data processing site preparation and its criticality for preventing future computer downtime and disruptions.

McKibbin, W.L. "Who Gets The Blame For Computer Crime." Infosystems vol 30 no. 7 July 1983 pp. 34-36 MIS managers are ultimately responsible for the security of their computers. Since they are responsible they should make sure upper management is aware of the vulnerabilities of their computers.

McLellan, Vin "Computer Systems Under Siege" The New York Times, January 31, 1988.

Meason, Robert "System Security at the Terminal." Data Processing & Communications Security vol 10 no. 4 Fall 1986 pp. 16-17 This article discusses considerations of MIS management protection of the processor from access by unauthorized users.

Menkus, Belden "Agencies Fail to Appreciate Threat to Data Security" Government Computer News, April 29, 1988, p. 36.

Miskiewicz, J. "DP Security: A Delicate Balance." Computer Decisions vol 17 no. 8 April 1985 pp. 104-106 This article discusses the delicate balance between protecting vital resources in a data processing facility and enhancing productivity.

Minoli, D. "Backup Needs Merit Special Attention." Computerworld vol 19 no. 15 April 1985 pp. 91, 96 This article focuses on the merits of backing up a data center to prevent a major disaster from critically affecting a company.

Moore, Gwendolyn B., John L. Kuhns, Jeffrey L. Treffzs and Christine A. Montgomery Accessing Individual Records From Personal Data Files Using Nonunique Identifiers NBS SPEC PUB 500-2 February 1977 Analyzes methodologies for retrieving personal information using nonunique identifiers such as name, address, etc. This study presents statistical data for judging the accuracy and efficiency of various

methods.

Moulton, R. "Prevention: Better Than Prosecution." Government Data Systems vol 10 no. 6 November/December 1981 pp. 20 & 22-23 The focus of this paper is on deterrence of computer abuse, whether it is unintentional or intentional.

Munro, N. & Danca, R.A. "Federal Officials Puzzled by Computer Virus Attacks", Government Computer News, April 29, 1988.

Murray, W.H. "Security Considerations for Personal Computers," IBM System Journal, Vol. 23, No. 3 (1984), pp. 297-304.

Murray, W.H. "Security Risk Assessment in Electronic Data Processing Systems," IBM Publication Number G320-9256-0 (1984).

Murray, W.H. "Good Security Practices for Information Systems Networks," IBM Publication Number G360-2715-0 (1987).

Murray, W.H. "An Executive Guide to Data Security," IBM Publication Number G320-5647-0 (1975).

Murray, W.H. "Security, Auditability, System Control Publications Bibliography," IBM Publication Number G320-9279-2 (1987).

Muzerall, Joseph V. and Carty, Thomas J. "COMSEC and Its Need for Key Management." Data Processing & Communications Security vol 11 no. 2 Spring 1987 pp. 11-14 This article explains the establishment of a standard set of protection mechanisms for both the classified and private user communities.

Mylott, T.R. "Computer Security and the Threats from Within." Office vol 101 no. 3 March 1985 pp. 45-46, 190 This article explains that the greatest computer-related danger to a company may be from internal threats by employees.

National Computer Security Center, Personal Computer Security Considerations December, 1985. NCSC-WA-002-85.

National Institute of Justice NIJ Reports Bimonthly Journal From National Criminal Justice Reference Service Box 6000 Rockville, MD 20850 (301) 251-5500 Free to registered users of the NIJ. This journal provides summaries of research reports to help keep you up to date with advances in the field of criminal justice.

NBS Special Publication 500-120. Security of Personal Computer Systems: A Management Guide. National Bureau of Standards, Jan 1985.

Neugent, William, John Gilligan, Lance Hoffman, and Zella G. Ruthberg Technology Assessment; Methods For Measuring The Level Of Computer Security October 1985 NBS SPEC PUB 500-133 The document covers methods for measuring the level of computer security, i.e. technical tools or processes which can be used to help establish positive indications of security adequacy in computer applications, systems, and installations. The report addresses individual techniques and approaches, as well as broader methodologies which permit the formulation of a composite measure of security that uses the results of these individual techniques and approaches.

Nicolai, Carl "Encryption Decyphered" Computers and Electronics, June 1984, pp 64 ff.

NIST Special Publication 500-166. Computer Viruses and Related Threats: A Management Guide. National Institute of Standards and Technology, Aug 1989. Available from Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402. Order by stock no. 003-003-02955-6 for $2.50 prepaid. Editors and reporters can get a copy from the NIST Public Information Division, 301/975-2762. The guide is intended to help managers prevent and deter virus attacks, detect when they occur, and contain and recover from an attack. It provides general guidance for management and users, plus more specific guidance for multi-user computer environments and for personal computer environments. It also contains a list of suggested readings.

Orceyre, Michel J. and Robert H. Cortney, Jr. Edited by Gloria R. Bolotsky Considerations In The Selection Of Security Measures Of Automatic Data Processing Systems Details methods and techniques for protecting data NBS SPEC PUB 500-33 processed by computer and transmitted via telecommunications lines. This report identifies the controls that can be instituted to protect ADP systems when risks and potential losses have been identified.

Parker, D.B. "The Many Faces of Data Vulnerability." IEEE Spectrum vol 21 no. 5 May 1984 pp. 46-49 Discussed in this paper are both the need for new computer security methods and the attainable limits that can be reached by computer security.

Parker, T. "Public domain software review: Trojans revisited, CROBOTS, and ATC." Computer Language. April 1987.

Patrick, Robert L. Performance Assurance And Data Integrity Practices January 1978 NBS SPEC PUB 500-24 Details practices and methods that have been successful in preventing or reducing computer system failures caused by programming and data errors. The methods

described cover large data processing applications, scientific computing applications, programming techniques and systems design.

Personal Identification News Monthly Newsletter From Personal Identification News P.O. Box 11018 Washington, DC 20008 (202) 364-8586 $265.00 Annually This newsletter discusses advanced access control technologies including plastic cards and authentication to biometrics.

Pieper, Oscar R. "Voice Authentication Wages A War on Data Base Fraud." Data Processing & Communications Security vol 8 no. 6 July/August 1984 pp. 12-13 This article reviews the present state of voice authentication technology and how it applies to secure data bases from bogus intruders.

Police & Security Bulletin Monthly Newsletter From Lomond Publications P.O. Box 88 Mt.Airy, MD 21771 (301) 829-1496 $72.00 Annually This newsletter is designed for specialist in law enforcement, criminal justice and security.

Power, Kevin "Over Half of Agencies Meet Security Training Deadline" Government Computer News, May 15, 1989, p. 85.

Pozzo, M.M., Gray, T.E. "An approach to containing computer viruses" Computer & Security, Aug 1987.

Pozza, M.M., Gray, T.E. "Managing Exposure to Potentially Malicious Rograms" Proceeding of the 9th National Computer Security Conference, Gaithersburg MD, Sept 1986.

Privacy Journal Monthly Journal From Privacy Journal P.O. Box 15300 Washington, DC 20003 (202) 547-2865 $89.00 Annually This journal looks at privacy issues and how they relate to all levels of government and private sectors.

Pujals, J.M. "What is a Contingency Plan?." Data Processing & Communications Security vol 12 no. 1 Winter 1988 pp. 19-23 This article tells how to construct a contingency plan and goes over the major mandatory steps that have to be taken to end up with a workable product.

Raimondi, D. "E.F. Hutton Underscores Practicality in Backup Plan." Computerworld vol 19 no. 15 April 1985 pp. 19 Describes how E.F. Hutton has built a new computer room as part of its disaster recovery plan.

Rames, David "Recovering From Disasters." Computer Decisions vol no. September 1981 pp. 108-110, 112, 114, 120, 122, 124, 126-131, 188-189

Described in this article are criteria for developing an emergency backup plan and examples of emergency backup alternatives.

Reber, Jan "The Essence of Industrial Espionage." Data Processing & Communications Security vol 10 no. 1 Winter 1986 pp. 24-25 This article discusses understanding espionage by a characteristic all spies have in common "access to the target".

Reeds, J. A. and Weinberger, P. J. "File Security and the UNIX Systems Crypt Command" AT&T Bell Laboratories Journal, Oct 1984

Reid, T. R. "Fending Off a 'Computer Virus' Means Taking Only a Few Precautions" Washington Post, Feb 15, 1988.

Rhodes, B. "Micro Security That Makes Sense." Computer Decisions vol 17 no. 9 May 1985 pp. 72, 74-76 This article describes security procedures that can be used by employees to solve microcomputer security problems.

Risk Management Manual (3 Volumes) From The Merrit Company 1985 (Bimonthly Supplements) Risk Management $283.00 This manual provides easy-to-understand fundamentals and specifics for initiating and maintaining a risk management program.

Roberts, J.E. "Filing Software Copyrights." Computerworld vol 19 no. 36 September 1985 pp. 116 This article describes how copyrighting software is accomplished and what copyrighted software means.

Roberts, Ralph. Computer Viruses COMPUTE! Publications Inc., 1989.

Rosch, W. "Three Products Help Cork Computer Leaks, Feature Blocked Access, Disk-File Encryption." PC Week vol 2 no. 18 May 1985 pp. 122-124 This article discusses a trio of products to help prevent unauthorized access to a computer system.

Rosch, Winn L. "Internal Security" PC Week May 7, 1985 pp 89 ff.

Rosen, Richard D. and Dvorsky, James "Portable Data Carrier Technology." Data Processing & Communications Security vol 12 no. 1 Winter 1988 pp. 9-19 This article presents an overview of the general field of portable data carrier technology. Included are not only smart cards but other devices and systems that are beginning to emerge in the marketplace.

Rosenthal, Lynne S. Guideline on Planning and Implementing Computer Systems Reliability NBS Spec PUB 500-121 January 1985 This report presents guidance to managers and planners on the basic concepts of computer system reliability and on the implementation of a

management program to improve system reliability. Topics covered include techniques for quantifying and evaluating data to measure system reliability, designing systems for reliability, and recovery of a computer system after it has failed or produced erroneous output. An appendix contains references and a list of selected readings.

Ruder, Brian and J. D. Madden An Analysis Of Computer Security Safeguards For Detecting And Preventing Intentional Computer Misuse January 1978 NBS SPEC PUB 500-25 Analyzes 88 computer safeguard techniques that could be applied to recorded actual computer misuse cases. Presents a model for use in classifying and evaluating safeguards as mechanisms for detecting and preventing misuse.

Ruthberg, Zella G. Audit And Evaluation Of Computer Security Ii: System Vulnerabilities And Controls April 1980 NBS SPEC PUB 500-57 Proceedings of the second NBS/GAO workshop to develop improved computer security audit procedures. Covers eight sessions: three sessions on managerial and organizational vulnerabilities and controls and five technical sessions on terminals and remote peripherals, communication components, operating systems, applications and non-integrated data files, and data base management systems.

Ruthberg, Zella and Bonnie Fisher Work Priority Scheme For Edp Audit And Computer Security Review August 1986 NBSIR 86-338 This publication describes a methodology for prioritizing the work performed EDP auditors and computer security reviewers. Developed at an invitational workshop attended by government and private sector experts, the work plan enables users to evaluate computer systems for both EDP audit and security review functions and to develop a measurement of the risk of the systems. Based on this measure of risk, the auditor can then determine where to spend review time.

Ruthberg, Zella and Robert McKenzie (editors) Audit And Evaluation Of Computer Security October 1977 NBS SPEC PUB 500-19 Reports on the recommendations of audit and computer experts to improve computer security audit procedures. Subjects covered include audit standards, administrative and physical controls, program and data integrity, and audit tools and techniques.

Ruthberg, Zella G. and William Neugent Overview Of Computer Security Certification And Accreditation April 1984 NBS SPEC PUB 500-109 This publication is a summary of and a guide to FIPS PUB 102, Guideline to Computer Security Certification and Accreditation. It is oriented toward the needs of ADP policy managers, information resource managers, ADP technical managers, and ADP staff in understanding the certification and accreditation process.

Rutz, Frank "DOD Fights Off Computer Virus" Government Computer News Feb 5, 1988.

Samuel, J. "Defense Net Broken Into - Again", Communications Week, December 5, 1988, p.1

Schabeck, Timothy A. Computer Crime Investigation Manual From Assets Protection 1980 Abuse/Misuse/Crime $39.95 Clear and precise overview of computer hardware, software, operations, and job functions.

Schiller, Michael "Security at the Touch of a Finger." Data Processing & Communications Security vol 9 no. 6 July/August 1985 pp. 15-17 This article discusses using biometric security systems for high-tech solutions to access control problems.

Schmonsees, Robert J. "Identification and Authentication: The Security Challenge of the 80's." Data Processing & Communications Security vol 9 no. 4 March/April, 1985 pp. 22-23 This article discusses the computer security issues of identification and authentication showing the common problems and offering some suggestions for improving by random passcode.

Schnaidt, Patricia. "Fasten Your Safety Belt". LAN Magazine, Oct 1987.

Schriever, Joe F. "Structuring for Security." Data Processing & Communications Security vol 9 no. 1 September/October 1984 pp. 14-16 This article is a set of guidelines that will remove ambiguities as to what will be done by whom to provide system security.

Schweig, Barry B. "Decision Matrix: A Risk Handling Decision Aid." Data Processing & Communications Security vol 8 no. 4 March/April 1984 pp. 16-18 This article discusses conceptualizing a decision-matrix as an integral component of a risk management process.

Scoma, Louis "How Secure Is Your Computer Operation From A Disaster." Office vol no. August 1981 pp. 96, 98 The failures of companies to protect their computer centers is discussed along with the need for recovery systems to serve as backup security.

Security Monthly Magazine From Cahners Publishing Company 275 Washington Street Newton, MA 02158 (617) 964-3030 Free to qualified readers. This magazine is written for the industrial and commercial loss-prevention specialist.

Security Awareness Bulletin Irregular Bulletin From Department of Defense Security Institute (DoDSI) C/O Defense General Supply

Richmond, VA 23297-5091 Free Discusses security awareness and compliance with security procedures through dissemination of information to security trainers.

Security Dealer Monthly Magazine From PTN Publishing Co. 210 Crossways Park Drive Woodbury, NJ 11797 (517) 496-8000 $10.00 Annually This magazine contains articles relating to security products and general security procedures.

Security Distributing & Marketing Monthly Magazine From Cahners Publishing Company 275 Washington Street Newton, MA 02158 (617) 964-3030 Free to qualified readers. This magazine is written for dealers, distributors, and installers of loss prevention equipment, including crime and fire prevention and detection products and services.

Security Letter Biweekly Newsletter From Security Letter, Inc. 166 East 96th Street New York, NY 10128 (212) 348-1553 $147.00 Annually This newsletter looks at industrial and commercial security, and emphasizes not only corporate security planning but also physical security systems and personnel security.

Security Management Monthly Magazine From American Society for Industrial Security 1655 N. Ft. Meyer Drive Suite 1200 Arlington, VA 22209-3198 (703) 522-5800 $65.00 Annually This magazine was written for managers in charge of both security and loss prevention.

Security Systems Monthly Magazine From PTN Publishing Company 210 Crossways Park Drive Woodbury, NJ 11797 (516) 496-8000 Free to qualified readers. This magazine covers topics of interest to the professional security director- industrial, governmental, institutional, or retail.

Security Systems Digest Biweekly Digest From Washington Crime News Service 7043 Wimsatt Road Springfield, VA 22151-4070 (703) 941-6600 $95.00 Annually This digest provides news on the latest developments in security systems.

Shaw, James K. and Stuart W. Katzke Executive Guide To Adp Contingency Planning July 1981 NBS SPEC PUB 500-85 This document provides, in the form of questions and answers, the background, and basic essential information required to understand the developmental process for automatic data processing (ADP) contingency plans. The primary intended audience consists of executives and managers who depend on ADP resources and services, yet may not be directly responsible for the daily management or supervision of data processing activities or facilities.

Shoch, J.F and Hupp, J.A. "The 'Worm' Programs: Early Experience with a Distributed Computation". Communications of the ACM, Mar 1982.

Shabeck Computer Crime Investigation A comprehensive manual for investigating computer crimes. 380 pp $39.95 Computer Protection Systems.

Shabeck Emergency Planning Guide for Data Processing Centers Provides information necessary for preparing an effective emergency/disaster plan for your organization. 92 pp $10. Computer Protection Systems.

Shabeck Managing Microcomputer Security Addresses security in a wide variety of micro settings. 180 pp $25. Computer Protection Systems.

Shannon, Terry C., Technical Editor Computer Security Handbook: The Practitioner's "Bible" From Computer Security Institute 1985 General Security $95.00 Contains a number of articles and technical papers dealing with computer security issues such as training and security safeguards.

Sharp, Brown "Computer Viruses Invade a Low-Immunity Congress. Government Computer News, September 4, 1989, p. 11.

Shoch, J. F. and Hupp, J. A. "The Worm Programs: Early Experience with a Distributed Computation" Communications of the ACM, Mar 1982.

Shoop, Tom & David J. Stang "Beating Back a Virus Attack" Government Executive, April, 1990, p. 40 ff.

Smid, Miles E. A Key Notarization System For Computer Networks October 1979 NBS SPEC PUB 500-54 Describes a system for key notarization, which can be used with an encryption device, to improve data security in computer networks. The key notarization system can be used to communicate securely between two users, communicate via encrypted mail, protect personal files, and provide a digital signature capability.

Software Protection Monthly Journal From Law and Technology Press P.O. Box 3280 Manhattan Beach, CA 90266 (213) 470-9976 $187.00 This journal provides current developments oriented around software protection methods, products, and services.

Spafford, Eugene H. "The Internet Worm Program: An Analysis". Purdue Technical Report CSD-TR-823, Nov 28, 1988.

Srinivasan, C.A. and Dascher, P.E. "Computer Security and Integrity: Problems and Prospects." Infosystems vol 28 no. 5 May 1981 pp. 5 Pages Various aspects of computer security are discussed including data security, data privacy, data integrity, etc.

Standard On Computer Data Authentication FIPS PUB 113 May 1985 This standard specifies a Data Authentication Algorithm (DAA) which, when applied to computer data, automatically and accurately detects unauthorized modifications, both intentional and accidental. Based on the Data Encryption Standard (DES), this standard is compatible with requirements adopted by the Department of Treasury and the banking community to protect electronic fund transfer transactions.

Standard On Password Usage FIPS PUB 112 May 1985 This standard defines ten factors to be considered in the design, implementation and use of access control systems that are based on passwords. It specifies minimum security criteria for such systems and provides guidance for selecting additional security criteria for password systems which must meet higher security requirements.

Stang, David J. Computer Security National Computer Security Association, Washington, D.C. 1990. Revised every three months or more often.

Stang, David J. Computer Viruses National Computer Security Association, Washington, D.C. 1990. Revised every three months or more often.

Stang, David J. Defend Your Data! A Guide to Data Recovery National Computer Security Association, Washington, D.C. 1990. Revised every three months or more often.

Stang, David J. "How to Sell Data Integrity" Reseller Management, March 1990, p. 131ff.

Stang, David J. "PC Viruses: The Desktop Epidemic" The Washington Post, January 14, 1990, p. B3.

Steinauer, Dennis D. Security Of Personal Computer Systems - A Management Guide NBS SPEC PUB 500-120 This publication provides practical advice on the following issues: physical and environmental protection system and data access control; integrity of software and data; backup and contingency planning; auditability; communications protection. References to additional information, a self-audit checklist, and a guide to security products for personal computers are included in the appendices.

Stieglitz, M. "Security For Shared Resources." Micro Communications vol 2 no. 6 June 1985 pp. 19-26 This article discusses data security products and procedures for network use. Includes description of encryption techniques that are now popular.

Sugawara, S. "Report Says Computers Are at Risk. Government Told to Tighten Security" The Washington Post, November 22, 1988, p. C1, C2.

Taft, Darryl K. "Computer Security Center Sees Opportunity in UNIX" Government Computer News, September 4, 1989, p. 68.

Thompson, Ken. "Reflections on Trusting Trust (Deliberate Software Bugs)" Communications of the ACM, Vol 27, Aug 1984.

Tinto, Mario. "Computer Viruses: Prevention, Detection, and Treatment." National Computer Security Center C1 Tech. Rpt. C1-001-89, June 1989.

Troy, Eugene F. Security For Dial-up Lines May 1986 NBS SPEC PUB 500-137 Ways to protect computers from intruders via dial- up telephone lines are discussed in this guide. Highlighted are hardware devices which can be fitted to computers or used with their dial-up terminals to provide communications protection for non-classified computer systems. Six different types of hardware devices and the ways that they can be used to protect dial-up computer communications are described. Also discussed are techniques that can be added to computer operating systems or incorporated into system management or administrative procedures.

U.S. Government Telecommunications: General Security Requirements for Equipment Using the Data Encryption Standard Federals Standard 1027.

Vernick, Paul R. "Providing Data Processing Recovery Backup." Data Processing & Communications Security vol 9 no. 4 March/April, 1985 pp. 14-16 This article covers some of the major emergency and recovery planning options available that need to be considered prior to the occurrence of any serious emergency.

Walsh, Timothy J. and Healy, Richard J. Protection of Assets (4 Volumes) From The Merrit Company 1974 (Updated Monthly) General Security $285.00 This manual helps you design and maintain an effective, cost saving, on-going program for total assets protection.

Weber, A. "Effective Security Programs Start with Awareness." Data Management vol 23 no. 11 November 1985 pp. 34-35 Educating end users is the key to helping prevent crime and computer abuse in an

organization.

Weixel, S. "Most accidents happen when companies neglect the basics." ComputerWorld, March 13, 1989, p.83.

Weller, Reginald H. "Off-Site Data Storage: A Changing Industry." Data Processing & Communications Security vol 9 no. 5 May/June 1985 pp. 18-20 This article discusses selecting a backup site while meeting the criteria of integrity, reliability, access, reasonable cost, appropriate location, good security, and comprehensive insurance coverage.

Westin, Alan F. ERS, Personnel Administration, And Citizen Rights NBS SPEC PUB 500-50 July 1979 Reports on the impact of computers on citizen computer rights in the field of personnel record keeping. This study traces the changing patterns of employment and personnel administration and examines the trends in computer use in personnel administration. It recommends policy actions to guide the management of personnel systems that respect citizen rights.

White, Steve, David Chess, & Jimmy Kuo "Coping with Computer Viruses and Related Problems" IBM, Thomas J. Watson Research Center, Distribution Services F-11 Stormytown, Post Office Box 218, Yorktown Heights, New York 10598. 1989.

White, L. "Data Security - You Can't Work Without It." Computerworld vol 19 no. 11A March 1985 pp. 27-30 The problem of the disgruntled employee or ex-employee who sabotages a computer system is seen as more of a threat than an outside hacker.

Withrow, J.B. Security Handbook for Small Computer Users From National Technical Information Service April 1985 Microcomputer Security $13.95 This manual discusses various security issues dealing with small computers and the responsibilities users of small computers have towards security.

Witten, I. H. "Computer (In)security: infiltrating open systems." Abacus (USA) Summer 1987.

Wolbrecht, J.E. "Can Your Records Storage Center Stand a Disaster." Office vol 102 no. 3 September 1985 pp. 112-113 A manager's responsibility to protect a records storage center by recognizing vulnerable areas and making them more secure is discussed.

Wood, Helen The Use Of Passwords For Controlled Access To Computer Resources May 1977 NBS SPEC PUB 500-9 Describes the need for and uses of passwords. Password schemes are categorized according to selection technique, lifetime, physical characteristics and information content. Password protection and cost considerations are discussed. A

glossary and annotated bibliography are included.

Wood, Charles Cresson "A New Approach to Computer User Authentication." Data Processing & Communications Security vol 10 no. 4 Fall 1986 pp. 21-26 This article gives a new approach to authentication called dial-guard. It addresses the two problems of password/users IDs not providing sufficient security and identifying the location of dial-up users.

Wood, Charles Cresson "Information Security with One-Way Functions." Data Processing & Communications Security vol 9 no. 5 May/June 1985 pp. 14-16 This article explains how one-way functions can be used to safeguard information that is too sensitive to be protected via encryption.

Wright, J.R. Jr. "User Responsibility for Security." Government Data Systems vol 15 no. 1 December 1985 through January 1986 pp. 52-55 This article looks at the circular "Management of Federal Information Resources" printed by the Office of Management and Budget. This circular provides guidance to Federal Managers concerning computer security and the associated responsibilities.

Young, Catherine L. "Taxonomy of Computer Virus Defense Mechanisms" Proceeding of the 10th National Computer Security Conference, Gaithersburg MD, Sept 1987.

Zalud, Bill "Security and DP Cooperate to Attack Computer Crime." Security vol 24 no. 10 October 1987 pp. 52-56, & 58 This article stresses teamwork as computer crime becomes a company fact of life by effectively cuts across a number of functional areas.

Zimmerman, J.S. "P.C. Security: So What's New." Datamation vol 31 no. 21 November 1985 pp. 89-92 This article looks at the problems data security officers are going to encounter even as they implement safeguards for micros.

Zimmerman, J.S. "Is Your Computer Insecure?" Datamation vol 31 no. 10 May 1985 pp. 119-120 This article challenges widely accepted notions concerning computer security. It suggest that people's views should be changed so that the challenge will be making a security system work instead of beating it.

How to order ICST publications

These publications are available through the Government Printing Office (GPO) and the National Technical Information Service (NTIS). The source and price for each publication are indicated. Orders for publications should include title of publication, NBS publication

number (Spec. Pub. 000, Tech. Note 000, etc.) and NTIS or GPO number. Your may order at the price listed; however, prices are subject to change without notice. Submit payment in the form of postal money order, express money order or check made out to the Superintendent of Documents for GPO-stocked documents or to the National Technical Information Service for NTIS-stocked documents.

Mailing addresses are:

Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402

National Technical Information Service, 5285 Port Royal Road, Springfield, VA 22161

Telephone numbers for information are: GPO Order Desk: (202) 783-3238; NTIS Orders: (703) 487-4780; NTIS Information: (703) 487-4600

About FIPS (Federal Information Processing Standards) Publications

FIPS PUBS are sold by the National Technical Information Service (NTIS), U.S. Department of Commerce. A list of current FIPS covering all ICST program areas is available from: Standards Processing Coordinator (ADP), Institute for Computer Sciences and Technology Technology Building, B-64, National Bureau of Standards, Gaithersburg, MD 20899 (30l) 975-2817