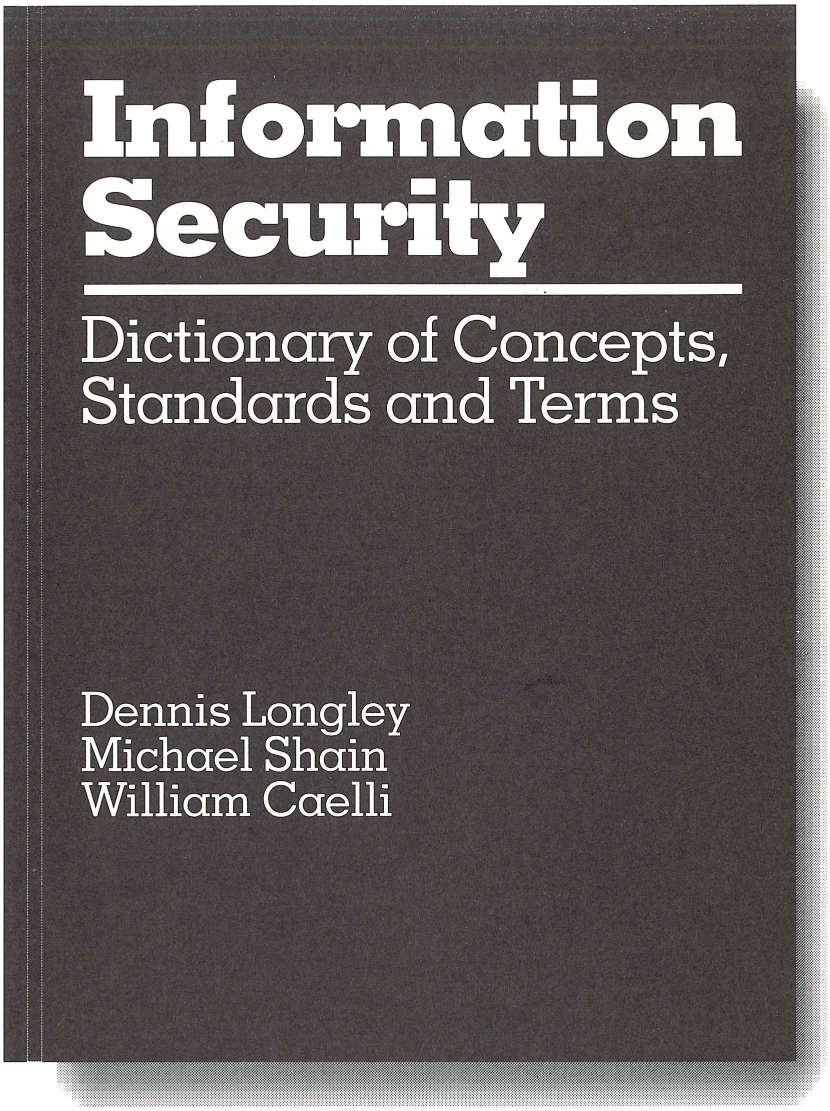
"Everyone involved with computer security ... should have this volume as a reference."

- Security Audit & Control Reviews

*From a review of the previous edition titled: **Data and Computer Security***

MACMILLAN

Previous Edition Titled
Data and Computer Security



Information Security

Dictionary of Concepts, Standards and Terms

Dennis Longley
Michael Shain
William Caelli

December 1992, 632 pages, hardcover
ISBN 0 333 54698 9, $169

- The most complete collection of information security terms ever assembled
- Updated throughout including 30% new material
- Numerous extended essays on vital subjects
- Easy-to-use format for rapid access to information

INFORMATION SECURITY

Dictionary of Concepts, Standards and Terms

New!

Dennis Longley, Michael Shain, & William Caelli

This comprehensive dictionary (formerly titled **Data and Computer Security**) of more than 3,500 entries offers you a one-stop reference on all aspects of information security. This new edition — the first in five years — has been thoroughly updated to reflect the many significant changes that have occurred in the field, and contains 30% additional information.

As before, the dictionary is designed to help the non-expert assess his or her security concerns, and then to initiate appropriate action. It provides clear explanations of technical terms and concepts, and offers further detail in a broad range of in-depth extended essays, including essays on such topics as:

- Risk analysis
- Standards
- Database security
- Network security
- Personal computers
- Key management
- Viruses
- Trusted systems
- Authentication
- Access controls

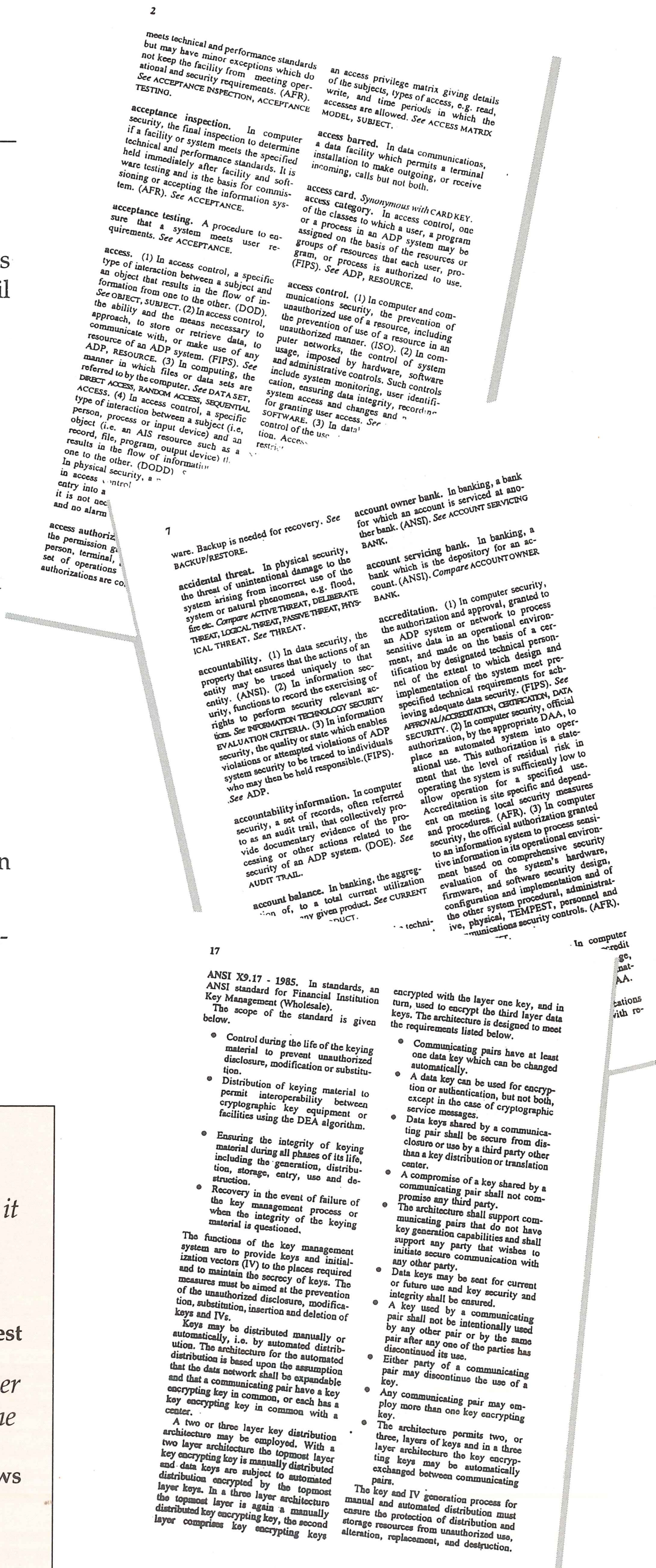
For the specialist reader, the dictionary also covers the relevant theory and mathematics of modern data security and relates it to current developments in information security.

In addition, the dictionary's extended cross-referencing helps you to build a complete picture of a particular interest by enabling you to penetrate a subject as deeply as you need.

Dennis Longley is Dean of the Faculty of Information Technology, Queensland University of Technology, Australia.

Michael Shain is Director of Information Technology at World ORT Union in London.

William Caelli is Founder and Technical Director of ERACOM, an Australian data security company, and is also the Director of the Information Security Research Centre at the Queensland University of Technology, Brisbane, Australia.



2

meets technical and performance standards but may have minor exceptions which do not keep the facility from meeting operational and security requirements. (AFR). *See* ACCEPTANCE INSPECTION, ACCEPTANCE TESTING.

acceptance inspection. In computer security, the final inspection to determine if a facility or system meets the specified technical and performance standards. It is held immediately after facility and software testing and is the basis for commissioning or accepting the information system. (AFR). *See* ACCEPTANCE.

acceptance testing. A procedure to ensure that a system meets user requirements. *See* ACCEPTANCE.

access. (1) In access control, a specific type of interaction between a subject and an object that results in the flow of information from one to the other. (DOD). *See* OBJECT, SUBJECT. (2) In access control, the ability and the means necessary to approach, to store or retrieve data, to communicate with, or make use of any resource of an ADP system. (FIPS). *See* ADP, RESOURCE. (3) In computing, the manner in which files or data sets are referred to by the computer. *See* DATA SET, DIRECT ACCESS, RANDOM ACCESS, SEQUENTIAL ACCESS. (4) In access control, a specific type of interaction between a subject (i.e, person, process or input device) and an object (i.e. an AIS resource such as a record, file, program, output device) th... results in the flow of informatio... one to the other. (DODD) ... In physical security, a ... in access control ... entry into a ... it is not nec... and no alarm

access authoriz... the permission g... person, terminal, ... set of operations ... authorizations are co...

an access privilege matrix giving details of the subjects, types of access, e.g. read, write, and time periods in which the accesses are allowed. *See* ACCESS MATRIX MODEL, SUBJECT.

access barred. In data communications, a data facility which permits a terminal installation to make outgoing, or receive incoming, calls but not both.

access card. *Synonymous with* CARD KEY.

access category. In access control, one of the classes to which a user, a program or a process in an ADP system may be assigned on the basis of the resources or groups of resources that each user, program, or process is authorized to use. (FIPS). *See* ADP, RESOURCE.

access control. (1) In computer and communications security, the prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner. (ISO). (2) In computer networks, the control of system usage, imposed by hardware, software and administrative controls. Such controls include system monitoring, user identification, ensuring data integrity, recording system access and changes and ... for granting user access. *See* ... SOFTWARE. (3) In data... control of the use... tion. Access... restri...

7

ware. Backup is needed for recovery. *See* BACKUP/RESTORE.

accidental threat. In physical security, the threat of unintentional damage to the system arising from incorrect use of the system or natural phenomena, e.g. flood, fire etc. *Compare* ACTIVE THREAT, DELIBERATE THREAT, LOGICAL THREAT, PASSIVE THREAT, PHYSICAL THREAT. *See* THREAT.

accountability. (1) In data security, the property that ensures that the actions of an entity may be traced uniquely to that entity. (ANSI). (2) In information security, functions to record the exercising of rights to perform security relevant actions. *See* INFORMATION TECHNOLOGY SECURITY EVALUATION CRITERIA. (3) In information security, the quality or state which enables violations or attempted violations of ADP system security to be traced to individuals who may then be held responsible.(FIPS). *See* ADP.

accountability information. In computer security, a set of records, often referred to as an audit trail, that collectively provide documentary evidence of the processing or other actions related to the security of an ADP system. (DOE). *See* AUDIT TRAIL.

account balance. In banking, the aggregation of, to a total current utilization ...ny given product. *See* CURRENT ...DUCT.

... techni-

account owner bank. In banking, a bank for which an account is serviced at another bank. (ANSI). *See* ACCOUNT SERVICING BANK.

account servicing bank. In banking, a bank which is the depository for an account. (ANSI). *Compare* ACCOUNT OWNER BANK.

accreditation. (1) In computer security, the authorization and approval, granted to an ADP system or network to process sensitive data in an operational environment, and made on the basis of a certification by designated technical personnel of the extent to which design and implementation of the system meet prespecified technical requirements for achieving adequate data security. (FIPS). *See* APPROVAL/ACCREDITATION, CERTIFICATION, DATA SECURITY. (2) In computer security, official authorization, by the appropriate DAA, to place an automated system into operational use. This authorization is a statement that the level of residual risk in operating the system is sufficiently low to allow operation for a specified use. Accreditation is site specific and dependent on meeting local security measures and procedures. (AFR). (3) In computer security, the official authorization granted to an information system to process sensitive information in its operational environment based on comprehensive security evaluation of the system's hardware, firmware, and software security design, configuration and implementation and of the other system procedural, administrative, physical, TEMPEST, personnel and ...munications security controls. (AFR).

. In computer ...credit ...ge, ...nat- ...AA.

...tations ...with re-

17

ANSI X9.17 - 1985. In standards, an ANSI standard for Financial Institution Key Management (Wholesale).

The scope of the standard is given below.

- Control during the life of the keying material to prevent unauthorized disclosure, modification or substitution.
- Distribution of keying material to permit interoperability between cryptographic key equipment or facilities using the DEA algorithm.
- Ensuring the integrity of keying material during all phases of its life, including the generation, distribution, storage, entry, use and destruction.
- Recovery in the event of failure of the key management process or when the integrity of the keying material is questioned.

The functions of the key management system are to provide keys and initialization vectors (IV) to the places required and to maintain the secrecy of keys. The measures must be aimed at the prevention of the unauthorized disclosure, modification, substitution, insertion and deletion of keys and IVs.

Keys may be distributed manually or automatically, i.e. by automated distribution. The architecture for the automated distribution is based upon the assumption that the data network shall be expandable and that a communicating pair have a key encrypting key in common, or each has a key encrypting key in common with a center.

A two or three layer key distribution architecture may be employed. With a two layer architecture the topmost layer key encrypting key is manually distributed and data keys are subject to automated distribution encrypted by the topmost layer keys. In a three layer architecture the topmost layer is again a manually distributed key encrypting key, the second layer comprises key encrypting keys encrypted with the layer one key, and in turn, used to encrypt the third layer data keys. The architecture is designed to meet the requirements listed below.

- Communicating pairs have at least one data key which can be changed automatically.
- A data key can be used for encryption or authentication, but not both, except in the case of cryptographic service messages.
- Data keys shared by a communicating pair shall be secure from disclosure or use by a third party other than a key distribution or translation center.
- A compromise of a key shared by a communicating pair shall not compromise any third party.
- The architecture shall support communicating pairs that do not have key generation capabilities and shall support any party that wishes to initiate secure communication with any other party.
- Data keys may be sent for current or future use and key security and integrity shall be ensured.
- A key used by a communicating pair shall not be intentionally used by any other pair or by the same pair after any one of the parties has discontinued its use.
- Either party of a communicating pair may discontinue the use of a key.
- Any communicating pair may employ more than one key encrypting key.
- The architecture permits two, or three, layers of keys and in a three layer architecture the key encrypting keys may be automatically exchanged between communicating pairs.

The key and IV generation process for manual and automated distribution must ensure the protection of distribution and storage resources from unauthorized use, alteration, replacement, and destruction.

From the reviews of the previous edition formerly titled - DATA AND COMPUTER SECURITY

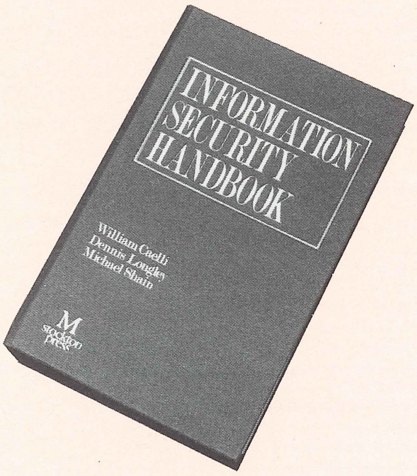
> *"Anyone involved with computer security in any way should have a copy of **Data & Computer Security** as a reference. It contains one of the most complete, detailed listings of security-related terms I have ever seen. There may be someone somewhere who knows all the material in this well-prepared book, but I have yet to meet this person. I highly recommend this book for everyone's personal library."*
>
> **—Security Management**

> *"Not only is it a first in the field, it is comprehensive, well organized and easy to use and to understand."*
>
> **—Computer Security Digest**

> *"Everyone involved with computer security…should have this volume as a reference."*
>
> **—Security Audit & Control Reviews**

> *"Essential for research libraries, and highly recommended for college and university libraries."*
>
> **—Choice**

An Ideal Companion to *Information Security: Dictionary of Concepts, Standards and Terms*



INFORMATION SECURITY HANDBOOK

William Caelli, Dennis Longley & Michael Shain

Focusing on both the managerial and technical aspects of information security, the **Handbook** is a virtual blueprint for setting up a secure computer infrastructure.

The first part of the **Handbook** deals with the non-technical areas of policy formulation, risk management, contingency planning, and the law. The second half, which builds upon the foundation of the earlier chapters, covers the technical areas of cryptography, access control, database security, communications security and security modelling.

> *"...if you have anything at all to do with information security, this book should be on your desk....over 800 pages of answers to virtually every security question you are likely to have....If you are a network manager, security officer or system programmer, get a copy of the **Information Security Handbook** right now. When it arrives don't put it on the bookshelf. Read it and then pick it up whenever you have an information security question."*
>
> **—Computer Security Alert**

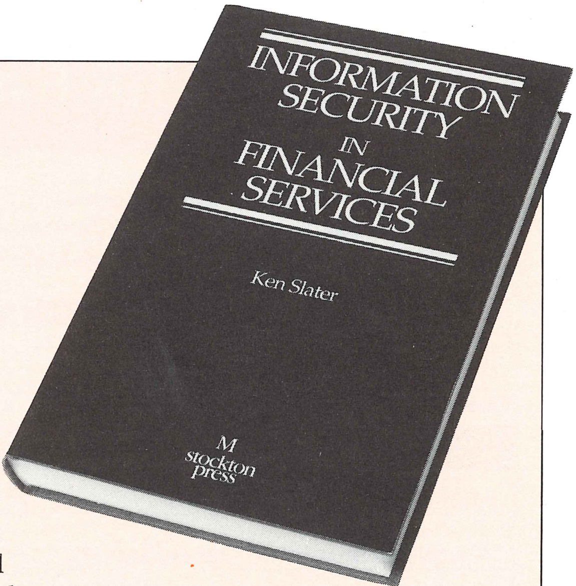
Table of Contents (Summary):

An Overview of Security • Security Management and Policy • Risk Management • Contingency Planning & Damage Avoidance • Information Security and the Law • Monitoring and Auditing Control • Applications and Theory of Cryptography • Access Control • Security of Stored Data and Programs • Communications Security • Formal Models of Secure Systems • Index.

October 1991, 830 pages, ISBN 0 333 51172 7, $175

INFORMATION SECURITY IN FINANCIAL SERVICES

Ken Slater



This unique book offers a wealth of practical advice on all aspects of information security in financial organizations, particularly banks, insurance companies and investment firms.

Among the book's key features are:

- An in-depth discussion of the organization and development of the security function within a financial institution
- Numerous examples of actual fraud...and specific suggestions on how to avoid similar disasters, including using knowledge-based systems to detect bank fraud
- Helpful self-test "checklists" that can be used to identify potential trouble spots
- Extensive appendices that provide detailed and valuable guidance on security procedures and requirements in specific areas, e.g. SWIFT, BACS, and CHAPS
- An outline of the security aspects of financial legislation and of security-related laws

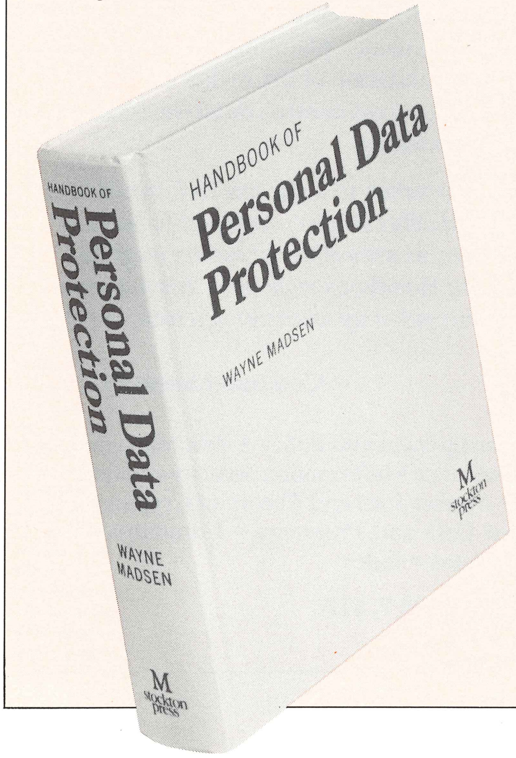
January 1992
275 pages
ISBN 0 333 54702 0, $159

Table of Contents (Summary):

Introduction • Risk and Vulnerability • The Security Policy • Personnel Security • Physical Security • Security of Computer Operations • Communications Security • Controlling the System • Secure System Development and Maintenance • Logical Access Security • Securing the Customer's Cash • If the Worst Happens: Disaster Recovery and Insurance • Micro-computer Security • Analysis Packages • Managing Security • The Auditor • Security Aspects of Compliance Reviews • Appendices • Glossary.

HANDBOOK OF PERSONAL DATA PROTECTION

Wayne Madsen



From medical history records to annual salary information to shopping habits, personal data is easily obtained by a variety of users. Increasingly, the American people are voicing their concerns regarding personal data uses and abuses, an issue that's being addressed worldwide.

The **Handbook of Personal Data Protection** is the first book to address data privacy from an international perspective.

It summarizes the highlights of the European data protection movement, including the OECD guidelines, the Schengen Agreement on police files, the Council of Europe and the EC directive. It focuses also on personal data abuses in the developing nations of Latin America, Asia, and Africa.

Closer to home, a chapter titled "The USA: First in Technology and Last in Data Protection" discusses the Government's history of political surveillance — from blacklists to databases. It concludes with the author's view that the U.S. Privacy Act is weak, outdated and badly in need of repair.

The book's 800 pages of appendices include the texts of most national data protection laws, as well as the addresses and telephone numbers of data protection offices around the world.

Wayne Madsen is a computer scientist in the integrated systems division of Computer Sciences Corporation. He is a well-known speaker on computer security and data privacy issues, and has written numerous articles on data security and privacy, computer viruses, network security and trans-border data flow security.

April 1992, 1200 pages, 0 333 56920 2, $198

Introductory Offer for 30 Day Trial

Mail, fax or phone to:
Ms. Dainaz Aaron, Macmillan Education Australia,
REPLY PAID 18, 107 Moray Street, South Melbourne VIC. 3205,

📠 (03) 690 6938 or ☎ (03) 699 8922.

Please send me the following books:

Title	Price $	Qty	Total
Information Security Handbook	175		
Information Security in Financial Services	159		
Handbook of Personal Data Protection	198		
Information Security: Dictionary of Concepts Standards and Terms	169		
Plus postage and insurance at $5.50 each in Australia and $12 each outside Australia.			
		Total	

MONEY BACK GUARANTEE

If for any reason your publications prove unsatisfactory, simply return them in their original condition within 30 days of receipt for a full refund.

METHOD OF PAYMENT

□ I enclose a cheque for $__________ payable to Macmillan Education Australia.

□ Please invoice me (Companies, Institutions and Govt. Bodies only) Order No.________

□ Please charge my credit card $__________

□ MasterCard □ Visa □ Bankcard □ Diners Club □ American Express

Card No. ____________________

I.D. No for Amex only ____________________

Cardholder's Name ____________________

Signature ____________________

Expiry Date ____________________

DELIVERY ADDRESS

Name: Mr Mrs Miss ____________________

Company ____________________

Street Address ____________________

____

Post Code ________ Telephone (   ) ____________________

(Street address is required for delivery - do not state P.O. Box)