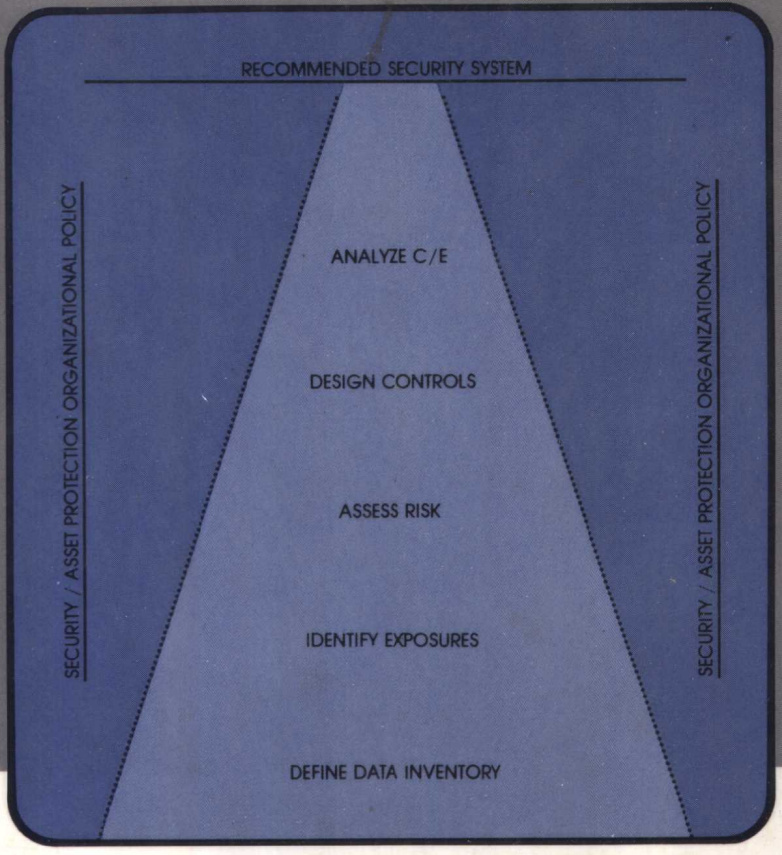
INFORMATION SYSTEMS SECURITY

Royal P. Fisher



INFORMATION SYSTEMS SECURITY

ROYAL P. FISHER
IBM Corporation

PRENTICE-HALL, INC.
Englewood Cliffs, New Jersey 07632

Library of Congress Cataloging in Publication Data

Fisher, Royal P. (date)
Information systems security.

Includes index
1. Electronic data processing departments—Security measures. 2. Computers—Access control. I. Title.
HF5548.2.F474 1984 658.4'78 83-19138
ISBN 0-13-464727-0

Editorial/production supervision: Nancy Milnamow
Jacket design: Photo Plus Art (Celine Brandes)
Cover design: Edsal Enterprises
Manufacturing buyer: Gordon Osbourne

Printed in the United States of America

10 9 8 7 6 5 4 3 2

ISBN 0-13-464727-0

Prentice-Hall International, Inc., *London*
Prentice-Hall of Austrialia Pty. Limited, *Sydney*
Editora Prentice-Hall do Brasil, Ltda., *Rio de Janeiro*
Prentice-Hall Canada Inc., *Toronto*
Prentice-Hall of India Private Limited, *New Delhi*
Prentice-Hall of Japan, Inc., *Tokyo*
Prentice-Hall of Southeast Asia Pte. Ltd., *Singapore*
Whitehall Books Limited, *Wellington, New Zealand*

INFORMATION

SYSTEMS SECURITY

Dedicated to
GINGER

PREFACE

ABOUT THE BOOK

This book is probably a "first" in the industry. It was written to present a simple, effective, complete, structured approach for the design of data security in computerized systems. Equally or perhaps even more important, it provides guidance as to where attention should be focused before resources are committed to such an endeavor. That is, what cost effective actions may be taken immediately to secure information systems to an acceptable level of risk?

WHAT THE BOOK IS NOT

This book is *not* intended as an in-depth technical presentation on data security. Nor is it a treatise on specific designs for each issue within the data security framework (such as data libraries, passwords, or functional organization). Rather it has been written to present a suggested structure or methodology wherein the main issues of data security may be effectively considered. It sets forth several approaches for recognizing and handling the data security issues existing in automated information systems. And it provides a useful overview of the factors to be considered before embarking on a data security program.

WHERE TO BEGIN

What are the critical areas of control concern and what are the fundamental principles, properties, and functions of secure systems applicable in those areas? Furthermore, what is management's role and function in planning, implementing, and administering the data security function? Chapters 1 through 4 address these questions, which in the author's opinion need to be addressed *first* before resources are committed to implementing a systems methodology. Chapters 1 through 4 thereby provide a general review of good security practice in information systems.

Chapter 1: A Top Management Priority

Is data security really a matter of significance to an organization? If so, why? Is there evidence that adequate controls may be missing in today's information systems? What really needs to be done? How do I determine if a need exists in my organization for improving the level of data security? Chapter 1 points out why many existing computerized information systems lack adequate control. It offers a simple self-assessment checklist to let you rate your organization's need for management attention to prevailing data security issues and concerns.

Chapter 2: Critical Control Areas

What were the key elements to adequate control in formerly designed information systems? Where should management, audit, designers, and others interested in data security focus their attention and concentrate their resources? Chapter 2 serves as a pointer, providing direction as to where one should first look. Although the treatment is superficial (a book could be written on each area), the chapter does define the nature of each critical element and provides an understanding of the problems to be addressed.

Chapter 3: Basic Principles, Properties, and Functions

What basic principles, properties, and functions of secure systems may be used as an aid for those interested in data security? What constitutes good security practice? Chapter 3 presents a *snapshot* of the many

ideas, concepts, and techniques IBM and others have found useful for developing adequate security in an information system. It quickly reviews some of the published basics of good security design. And, for those unfamiliar with data security, it provides an awareness of what is suggested practice.

Chapter 4: Management Contributions

Part 1: Management Policy, Plans and Programs. What is management's role with regard to data security? Part 1 stresses the need for management to set appropriate policy, plans, and programs for data security. Illustrations of form, content, and use are described with the referenced examples from the Appendices. Part 1 also serves to point out that data security must extend outside the information system, per se, to management in order to be effective.

Part 2: Role of the Security Administrator. Whose responsibility *is* data security? What characteristics and capabilities should a security administrator have? A function of this nature must be established in order to manage the security of the data resource. A functional matrix is suggested to aid in the affixing of the accountability. Small organizations and systems must recognize this need though they may not assign a person full-time to such a function.

THE METHODOLOGY

Many excellent articles have been published on security. To date, however, much of the information they offer remains to be synthesized into a structured and straightforward methodology. The practitioner has always needed detailed guidelines or "how to" manuals in order to perform the data security design and control function. And the auditor has searched for a simple, effective tool to assist in the adequate assessment of business controls. The methodology presented in Chapters 5 through 11 helps meet both of these basic needs. These chapters represent the main purpose of the book. They suggest the viewing of all data security concerns across eleven definable, understandable, manageable, exposure control points representing a complete data life cycle. The chapters use a methodical approach to achieve the goal of presenting to management a cost-effective recommendation for system security and control.

Chapter 5: Identifying Exposures

Chapter 5 begins by defining what is meant by exposure and data security. The definitions provide a simple way of viewing the results or consequences of violations (threats) to data. Exposures may be grouped into six basic effects resulting from adverse actions: accidental/intentional disclosure, modification, and destruction. Basic causal agents are then defined to narrow the scope of the identification process, and finally a data exposure life cycle is suggested, offering a structured thought process for identifying exposures in information systems.

Chapter 6: Exposure Control Points

Chapter 6 provides the framework within which to apply the process for identifying exposures—a data exposure life cycle comprised of eleven discrete control points.

Chapter 7: Applying the Methodology

This chapter illustrates how the structured thought process for identifying exposures can be directly applied to an information system (payroll) using the eleven-basic-exposure-control-point life cycle.

Chapter 8: Limiting Risk

How can risk be minimized? What initial steps can be taken to reduce risk? Chapter 8 offers the designer insight on how risk may be reduced, in general, in all information systems. It suggests some basic control guidelines. Such guidelines help information systems to score well (minimum exposure) when they undergo a risk analysis.

Chapter 9: Risk Analysis

Chapter 9 offers the practitioner a method for quantifying the risk associated with each defined exposure. This study may become rigorous. However, *caution* must be exercised that the process of quantification is not more costly than the expected risk. Common sense is a good guide!

Chapter 10: Basic Controls

This chapter suggests a unique way of viewing controls in order to simplify the selection process. The applicability of package software controls can be seen by viewing them across the data life cycle. Once a control is selected, its cost and its associated probability of success are assigned and recorded. Suggested worksheets are presented.

Chapter 11: Cost-Effectiveness Selection Process

Chapter 11 carries the process forward by applying the concept of return on investment (ROI) to the derived quantified values of risk and cost. Some non-cost-effective controls may be mandated by outside authority. The final adequacy of controls selected is based on a predetermined acceptable level of risk.

THE "QUIK" APPROACH

Chapter 12: "Quik" Approach

Chapter 12 offers a shortcut to the methodical approach presented in Chapters 5 through 11. The "Quik" approach uses the same methodology but reduces the rigors of quantification. It provides a *general* indication of security status rather than a detailed picture. A general assessment of controls can now be made with less effort. System weaknesses are easily identified at a higher level for control consideration. The "Quik" approach offers an excellent tool when only a fast, first-blush overview of system security is required.

SUGGESTION ON READING THIS TEXT

It is suggested by the author that this text first be read straight through for an understanding of its structure. Specific chapters or sections may then be focused on to meet individual interests and needs. Hopefully, the content will act as a catalyst for the reader to create and implement a better way, if one is to be found. The present text is just one effort among many to develop more effective approaches to data security in today's information systems.

ACKNOWLEDGEMENTS

I wish to make special acknowledgement to William H. Murray, Program Manager of Data Security, IBM Corporation, for his contribution in several chapters of this book. Many of his published basic ideas are presented as part of the overall data security framework.

In addition, I would like to express my personal gratitude to the IBM Corporation for permission to include several excerpts of IBM publications on data security. These reports, as well as several papers by other data security specialists, are included in the appendices.

I wish also to thank the following people:

- Dr. Claude W. Burill and Leon W. Ellsworth for their continued encouragement to write this book.
- Mel Quinn, manager of the Chicago Information Systems Management Institute, IBM Corporation, for his interest and encouragement in this endeavor.
- My family and other personal friends who supported me throughout the months of preparation and writing.

ROYAL P. FISHER

INFORMATION SYSTEMS SECURITY

CONTENTS

1

A TOP MANAGEMENT PRIORITY

LEVEL OF PRIORITY

Top management is entrusted with the development, growth, and prosperity of the business under its command. Its key activity has always been the planning and utilization of the organization's resources, traditionally classified as the big "M's": Men, Money, Material, and Machines-and-facilities.

With the advent of the electronic computer, a new resource has emerged for top management's concern—not the computer itself, but the elements making up the information processed by the computer. . . DATA!

Management has been slow to recognize data as a major resource. Viewed in its fragmented state, data appears to be meaningless and quite harmless. Viewed in total as an established database, however, it may constitute one of the most critical assets of the business. What gives such value to data? The answer lies in its worth to those who have it or want it. They recognize that information is power—power to manage, power to manipulate, power to control. Often the value of data is directly proportional to how much it alters or influences action or behavior.

The computer and its associated storage media enable management to have the information it wants and needs. However, management does not always assign a high priority to its responsibility in managing and protecting the *process* through which it now obtains that information.

Electronic data collection and dissemination systems are now pervasive in most organizations. Many of these systems were developed and implemented with little or no management participation and direction. Controls are not only poor but generally nonexistent. Some systems today are developed in the same manner.

Perhaps control is lacking because the data processing, audit, or other management support function has not stressed or sold the need for it. Another reason may be that computer vendors and salesmen have emphasized simplicity more than involvement. Perhaps, too, management should share some blame for its lag in really stepping up its new responsibilities in dealing with computerized information.

THE IMPETUS

Two major events have put information systems security in the foreground of management's concern. First came Equity Funding. Although publicized as a computer crime, it involved the computer only remotely in the generation of bogus policies. However, the headlines of a $27.25 million loss drew the attention of management to their responsibility for data security (i.e., the protection of information from unauthorized disclosure, modification, and/or disclosure, whether accidental or intentional). Unfortunately, lack of reinforcement and continued support of this concern made the period of recognition very brief.

The second major management awakening on data security came packaged as the Foreign Corrupt Practices Act of 1977, now known as the Business Practices and Records Act. Its provisions affect any publicly held domestic corporation. Although originally enacted by Congress to deter American companies from making improper payments to foreign officials (bribes for business), it was later enforced by rulings of the Securities and Exchange Commission (SEC) to require management to state in their financial reports that controls were adequate and functioning as intended.

The Act, with provisions amending the Securities Exchange Act of 1934, made it mandatory that a company implement a system of internal accounting controls to meet four objectives:[1]

1. Transactions are executed in accordance with management's general or specific authorization.

[1]The American Institute of Certified Public Accountants (AICPA) Statement on Auditing Standards.

2. Transactions are recorded as necessary to
   (a) permit the preparation of financial statements in conformity with generally accepted accounting principles and
   (b) maintain accountability for assets.
3. Access to assets is permitted only in accordance with management's general or specific authorization.
4. The recorded accountability for assets is compared with the existing assets at reasonable intervals and appropriate action is taken with respect to any differences.

In addition, each corporation was mandated to demonstrate upon request that it has:

1. Assessed the current status of its control system.
2. Improved any deficiencies.
3. Continued to monitor the actual effectiveness of the system.

Violation could result in a five-year prison term, a $10,000 fine, or both for the responsible executives. Once again, this made the issue of computerized information system security and control one of management's major concerns. Direct benefits from this concern were the establishment of an EDP audit function, the appointment of asset protection administrators, and the preliminary formulation of specific information system security policies, plans, and programs.

In June of 1980, however, the SEC[2] withdrew a proposal to implement the accounting provisions of the Foreign Corrupt Practices Act by requiring managers of publicly held companies to report on the adequacy of their internal controls. In withdrawing the proposal, the SEC said it would rely on voluntary management reporting . . . the fangs of the Act were pulled!

Although management has started to respond to its responsibility in managing and protecting the process through which it obtains computerized information, much still needs to be done. Chapter 4 highlights many of these activities.

Computer crime is the latest development pushing the security of information systems into headlines for management's attention. Security Pacific, the Dalton Gang, and Wells Fargo, to name a few, were well publicized. However, what is misleading here is that computer crime ap-

[2]"Taxation and Accounting," The Bureau of National Affairs Inc., Washington, D.C. 20037, page G-6, #19, 1/28/82.