Computer Security Management

Donn B. Parker

COMPUTER SECURITY MANAGEMENT

DONN B. PARKER

Reston Publishing Company, Inc.
A Prentice-Hall Company
Reston, Virginia

Library of Congress Cataloging in Publication Data

Parker, Donn B.
Computer security management.

Includes index.
1. Computers—Access control. 2. Electronic data processing departments—Security measures. I. Title.
QA76.9.A25P38 658.4'78 81-823
ISBN 0-8359-0905-0 AACR2

Editorial/production supervision and interior design
by Barbara J. Gardetto

10 9 8 7 6 5 4 3 2 1

Printed in the United States of America

COMPUTER SECURITY MANAGEMENT

To Lorna
Diane
David
My mother, Miriam
The memory of my father, Don
and Aunt Louise

Preface

Ideas for this book started well before I received the assignment to write a security handbook for John O'Mara and his Computer Security Institute. The writing rapidly became a professional book manuscript as the concept of a how-to-do-it handbook faded from view amid the pages of more basic text on problems, concepts, theory, and, finally, practice. The history started 11 years ago with computer abuse research with which I am more generally associated. However, the primary purpose of the research has been to advance computer security by study of the problems that security is supposed to solve. This book is a logical outgrowth.

In addition to the research on computer abuse, a computer security program was developed at SRI International to apply what we were learning to assist organizations in using their computers more safely. As a result, this book expresses the ideas and methodologies coming from study of actual loss and experience in conducting many security reviews to develop computer security for clients.

If any single conclusion is to be drawn from the 11 years of research and consulting, it is that computer security is not primarily a technological subject. It is a subject of psychological and sociological behavior of people. As I have said repeatedly in my worldwide lecturing, computers do not commit errors, omissions, or crimes; only people can do these things that may subsequently be manifested in computers. Solutions to these problems also must come from people, their actions and their attitudes. These concepts are strongly emphasized in this book.

Only a few people assisted me. First, members of my family tolerated my long evenings and weekends of isolation. Secondly, SRI management agreed to do without some of the energy and attention I might have otherwise given to my SRI work. Finally, I thank specific people for special assistance: my wife, Lorna, for her many hours of typing; John O'Mara for guidance; Robert Courtney and Gerald Weinberg for tearing apart early drafts; Susan Nycum for her insights on the law; and copy editor Vickey Macintyre and production editor Barbara Gardetto.

Donn B. Parker

Contents

Introduction

In a more perfect world, computer security might readily be achieved by applying a finite list of do's and don'ts found collectively in books and manuals on the subject. Unfortunately, the task is not that straightforward. Computer security strives toward both protecting assets and limiting their loss from three basic threats: natural disasters (for example, extreme weather conditions), human errors and omissions (for example, incorrect tape labeling), and intentional acts such as fraud or sabotage. The first two threats are empirically predictable. We know from experience how to prevent them or control their severity, and thus how to limit the resulting losses. The cookbook approach of checklist do's and don'ts, cautiously adapted and applied to specific environments through much common sense and trial and error, works quite well except for securing the computer system itself, but more about that later.

The threat from intentional acts is not amenable to effective treatment by the cookbook approach in current use. The sad history of the war against crime is proof that traditional efforts of control have minimal effect. The "Maginot Line" syndrome of setting up massive protective efforts to correct obvious weaknesses but ignoring others invites perpetrators to "end run" such a line and to attack computer assets through remaining weak areas. The perpetrators know the cookbook safeguards, too, and merely subvert or circumvent them.

A different methodology must be employed to control intentionally caused losses. The checklist approach alone won't suffice. Robert Courtney, IBM corporate strategist for Data Security, has collected over 800 checklist safeguards, is still accumulating new ones, and is finding fault with already documented ones at such a high rate that their publication even in a looseleaf binder would be impractical. A ten-year study of computer abuse at SRI International reveals that new variations of intentional acts are continually being generated (Parker 1979). They are the same old crimes of fraud, embezzlement, theft, larceny, sabotage, espionage, and extortion. However, when computers are involved, these old crimes take on new characteristics that make them into totally new crimes. Automation of asset storage and processing has resulted in new occupations of perpetrators, new modi operandi, new crime environments, and new targets. In other words crime has become automated now that data processing has penetrated the environments in which crime has traditionally occurred.

This automation of crime has confounded the traditional security specialists and law enforcement and prosecution agencies (Parker and Nycum 1980). At the same time, the automation of the environments and processes subject to crime opens an exciting new opportunity to automate the safeguarding against crime. Can automation survive the onslaught of crime? Will the automation of security for the first time in history, bring financial and information crime under control? If such control is to be achieved, surely new security methodologies consistent with automation methodologies of systems and operations analysis must be employed.

The SRI study of the new phenomenon of computer abuse and automated crime has resulted in a new method of attacking the problem of all types of losses associated with computers. The traditional method of selecting safeguards from checklists found in many books on computer security can be effective against errors and omissions. However, a checklist method against the intelligent enemies' intentional attacks is ineffective, because the enemy uses a different checklist. In other words, computer crime perpetrators find vulnerabilities that were not anticipated in published checklists. Therefore, the computer security specialist must think like the enemy and be as innovative as he is. An effective method must anticipate that a game is being played, and the rules of the game are made by the enemy, not the security specialist. This calls for a method that includes development and use of threat scenarios based on experience and playing the role of the enemy.

Such an approach has many advantages. It avoids the unimaginative and ineffective cookbook method since it offers great flexibility in several dimensions. Its methodology can be applied to any size or type of computer system (defined here in the broadest sense to include staff, facilities, hardware, and software). Most discussions of computer security recommend safeguards that are suitable for the largest systems but that are difficult or impossible to scale down for the smaller system, for example, one separating responsibilities in positions of great trust. Other methods assume almost unlimited resources for security planning and for imposing recommended safeguards, whereas the method proposed here can be scaled to fit any budget. It can be used for planning and implementation even where little safeguarding previously existed; it can be used for compliance auditing; and it can be used for incremental increases in protection.

Some shortcomings and some difficulties need to be recognized, however.

First, the proposed method has not been widely tested. It has evolved over two years through three applications. Although it has never been fully implemented in the ideal form presented here, its results have been encouraging. Furthermore, it has been tested by the SRI computer security staff, who have had great experience in security planning and in conducting security reviews. Most important, this method is based on in-depth knowledge of and experience with victims, perpetrators, and others associated with actual losses. This information is a great aid in predicting the development of realistic and practical threat situations. There may be some concern that computer security specialists without this experience may have difficulty in developing scenarios. In fact, the success of this method does depend on some security experience and practice. Some critics may complain because the number of scenarios to sufficiently provide for all potential threats may be too large. It will be seen, however, that scenarios can be generalized to reduce the number needed, and that this method will still be able to treat threats more comprehensively than the cookbook method. The threat scenario method is not very different from methods used by experienced electronic data processing (EDP) auditors who implicitly play out scenarios when they evaluate controls and safeguards. The method presented here merely formalizes this process, and thus makes the scenario approach an explicit one.

Some readers may think that more emphasis than is appropriate is being placed on intentional acts, versus accidental acts. After all, losses from accidental acts are said to be significantly higher than losses from intentional acts. It might also be argued that since the author's principal area of study is computer-related crime, this discussion might direct readers toward a presumably less serious problem. Of course, a universal problem with books on computer security is that the subject is so broad that no two authors are likely to be expert enough in all aspects of security to do them justice. One book may treat data base management security very well, while another may do a thorough job on physical security. Certain topics are bound to be left in the background, regardless of the comprehensive treatment claimed by any given author.

With this concern in mind, I warn the reader that this book mentions only superficially such important subjects as natural disasters, insurance, operating system security, and some others. On the other hand, it emphasizes and covers extensively some new concepts of computer security, it treats accidental and intentional acts as separate problems (a controversial idea), and it closely examines methods of analyzing threat and risk and methods of organizing the computer security function. It also examines methods of conducting a security review, selective rather than comprehensive application of quantitative risk assessment, and principles of safeguard selection.

This book focuses on security against intentional acts rather than against errors and omissions. The reasons are thoroughly explained in the text. No one knows whether either of these problems predominates, but surely it is more challenging to deal with the schemes responsible for intentionally caused losses. In addition, I believe that protection from intentional perpetrators, while only marginally increasing the cost over protection from accidents, provides protection from both types of loss, whereas protection against accidents does not include effective protection from intentionally causes losses. This relationship works in one direction but not the other.

To get through this book the reader must live with my prejudices and limitations. He may not agree with my concepts, conclusion, and emphasis, but I guarantee challenging and stimulating reading.

SECTION I

COMPUTER SECURITY AND THE ORGANIZATION