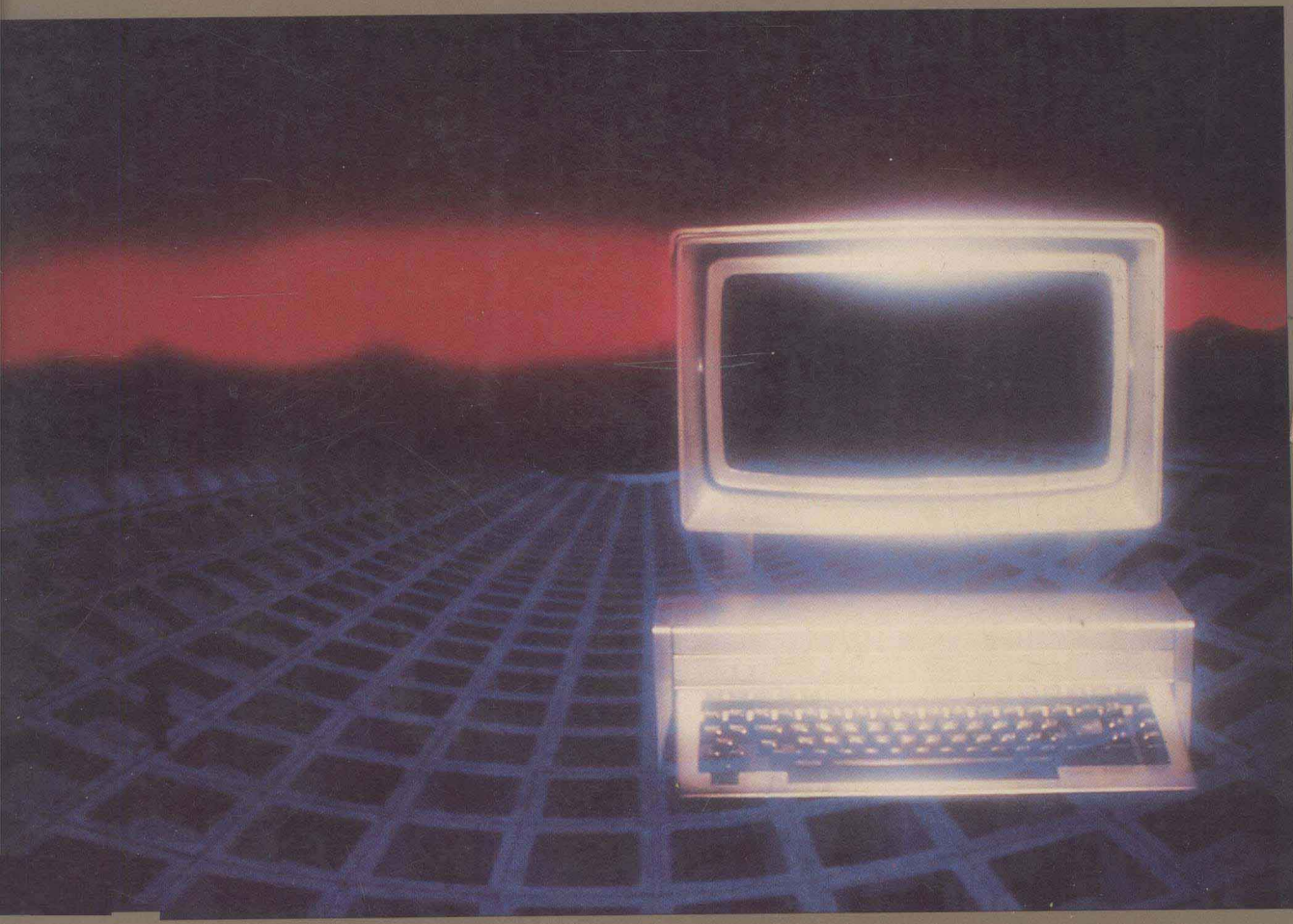
Brady

Microcomputer Data Security

Issues and Strategies for Business



Daniel J. Cronin

MICROCOMPUTER DATA SECURITY

Issues and Strategies

Daniel J. Cronin

A Brady Book
Published by Prentice Hall Press
New York, NY 10023

A Brady Book
Published by Prentice Hall Press
A Division of Simon & Schuster, Inc.
Gulf + Western Building
One Gulf + Western Plaza
New York, New York 10023

PRENTICE HALL PRESS is a trademark of Simon & Schuster, Inc.

Designed by Geraldine Ivins
Manufactured in the United States of America

1 2 3 4 5 6 7 8 9 10

Library of Congress Cataloging-in-Publication Data

Cronin, Daniel J., 1955—
Microcomputer Data Security

"A Brady book."
Bibliography: p. 261
Includes index.
1. Microcomputers—Access control. 2. Electronic data processing departments—Security measures.
I. Title.
QA76.9.A25C76 1986 005.8 86-91491
ISBN 0-89303-672-2

LIMITS OF LIABILITY AND DISCLAIMER OF WARRANTY

The author and publisher of this book have used their best efforts in preparing this book and the programs contained in it. These efforts include the development, research, and testing of the theories and programs to determine their effectiveness. The author and publisher make no warranty of any kind, expressed or implied, with regard to these programs or the documentation contained in this book. The author and publisher shall not be liable in any event for incidental or consequential damages in connection with, or arising out of, the furnishing, performance, or use of these programs.

REGISTERED TRADEMARKS

ACF2 is a registered trademark of SKK, Inc.

CyLock is a trademark of Cytrol, Inc.

Datakey memory device and Datakey are registered trademarks of Datakey, Inc.

Data Lock & Key is a trademark of MicroFrame, Inc.

DiskToolKit is a trademark of Morgan Computing Company, Inc.

DualTec is a trademark of C & K Security Systems, Inc.

Etherlink is a trademark of 3Com Corporation.

IBM Personal Computer, XT, AT, and PC-DOS are trademarks of International Business Machines Corporation.

NetlOne is a trademark of Ungermann-Bass, Inc.

MS-DOS is a trademark of MicroSoft Corporation.

RACF is a trademark of International Business Machines Corporation.

Rolltop 100 is a registered trademark of MicroComputer Accessories, Inc.

Smarthome is a registered trademark of CyberLYNX, Inc.

Smokeeter is a registered trademark of United Air Specialists, Inc.

TOP SECRET is a trademark of CGA Software Products Group, Inc.

Water Alert is a registered trademark of Dorlen Products/Division of Electro-Consultants, Inc.

PREFACE

Myth and reality, security and insecurity, right and wrong—contradictions surround the diverse issues of microcomputer security. The global microcomputer community has been ambushed by these contradictions, and as a result, misconceptions abound concerning the depth of the microcomputer community's exposure to security breaches.

Late last summer, I was disinterestedly watching the evening news, when a report came on that provoked my attention. Authorities in Florida had raided the suburban headquarters of yet another teenage hacker band allegedly tapping into Government installations. My immediate reaction was one of consternation—not another hacker siege! But as I listened further, my reaction quickly turned to a mixture of irritation and disbelief. Authorities were reported as saying the wizard hackers had been responsible for moving NASA satellites electronically, thousands of miles off course in outer space.

This book represents my commitment to challenging the many myths about computer security; my singleminded purpose is to dispel these myths and supplant them with facts.

ACKNOWLEDGMENTS

Many people have helped shape this book in one form or another, and I am indebted to them all. My gratitude extends to the legion of data processing and security professionals who sacrificed their time to endure intensive interviews. I would like to give special thanks to a handful of individuals: my data processing mentor, Philip Leftwich, president of Synergistic Cybernetics, for judiciously critiquing the chapter on power technology and making several recommendations; Wade Clark, president of Consolidated Security Supply, for his mini-lectures on current intrusion alarm technology and burglar alarm systems; my friends, Paul Kwan, systems programmer with Phaser Systems, and Tim Sammonds, national expert on PC networks, for their technical advice on the networking security chapter; Bill McDonald, of the Computer Doctor, for putting many of the microcomputer hardware problems into proper perspective; and Jay BloomBecker, director of the National Center for Computer Crime Data, Los Angeles, for his sobering profiles of the computer criminal.

I owe a special round of thanks to my editor, Burton Gabriel, for his support and confidence. For her perseverance and patience through the final stages of publication, Geraldine Ivins of Brady Books deserves an encore of thanks.

CONTENTS

1

Overview

FACT. Microcomputers have exploded on the scene unchecked, and their vulnerability has come to haunt us after the fact.

FACT. By 1986, the total number of PCs shipped to the major metropolitan areas is expected to climb to 6.5 million.

FACT. At the end of 1985, close to a million and a half PCs were linked to local area networks in corporate America.

FACT. Over three million PCs are merrily beeping and tweaking away in homes throughout the country.

FACT. In 1983, shipments of security products totalled $2.6 billion. By 1988, shipments are predicted to soar above $4.4 billion.

FACT. Computer crime is the nation's fastest growing industry. The average "take" for each reported crime has exceeded $100,000.00.

Sensational cases of microcomputer-related crime have sizzled across the mass media over the last couple of years. One of the more notable cases involved the Milwaukee 414 Hackers club, an elite of maniacal teenagers who bragged about cracking over 60 business and Government computers. In late 1984, the TRW Credit Bureau break-in topped the scandal charts for an inordinate period of time. Media efforts intensified on the heels of the Hollywood fantasy movie (emphasis on fantasy) "WarGames," where a peach-fuzzed youth wreaked global havoc as a result of clever meddling and blind audacious luck. In every instance, media coverage was predictably overplayed, distorted, and inconsistent from one report to the next. Yet something valuable came out of this excess—a growing awareness of computer security. Or is it computer insecurity?

WHAT IS COMPUTER SECURITY?

Managers of firms large and small are waking up to some bitter facts. Firms are growing increasingly more dependent on their IBM PCs to

track inventory levels, monitor sales reports, chart growth strategies, design products, store patented secrets, run payroll, and manage accounts payables/receivables. And now, all of a sudden, this strange question pops up out of nowhere: HOW SECURE IS MY SYSTEM?

No two security experts will ever quite agree on a precise definition of computer security. It isn't that computer security is such an elusive discipline, but that so many factors are involved: physical security, maintenance of the computer, protection of the hardware from theft, data integrity controls, classification of data as to sensitivity, data access controls, and the authentication of users, to name a few. In the popular mind, computer security is often confused with computer crime. Nothing could be further from the truth.

The definition of computer security that follows is all-encompassing; it will serve as a springboard and guideline for the direction taken in this book:

> Security assumes the safe and continuous operation of your computer system performed by trained, authorized personnel. The computer system itself must be protected, as well, the integrity of all programs and data. Finally, security means that any entered data can be retrieved at any future time, without alteration by accident or deliberate intent.

SECURITY AS A MANAGEMENT ISSUE

Micro security is a managerial blind spot. Though awareness of security threats is growing, managers on the whole still pay inadequate attention to the problem. Awareness must reach all levels of management in the corporate tree, from supervisors on up to top executives.

Part of the problem is that computer misdeeds, a fraudulent attack from an employee or a "bug" buried in the computer software causing processing errors, are usually hidden, and slow in coming to the surface. It's difficult to make management realize potential dangers, since there isn't any "smoking gun" to warn them. In many cases, breaches in security are discovered by accident--the thief blows his own cover. The following account of Zwana's round down fraud is a perfect example:

Zwana's Account

Several renditions of this classic salami scam (rounding down figures in order to steal a little off the top) have circulated in the press. It's anyone's guess how many cases have actually been perpetrated, but quietly kept on ice out of embarrassment. The salami technique is old and corporate auditors can recount some outlandish versions. Thirteenth century Venetian merchants began the practice of carrying two ledger books to protect themselves against this same abuse.

Zwana's story goes something like this: A programmer in a southern California bank made a profitable discovery one day. He realized that the bank system calculated a customer's interest rates into the thousandanths of a percent, but rounded to the nearest hundredth. The computer dropped any interest beyond this rounded figure. The programmer didn't want to see this money going to waste, so he wrote a patch (clandestine instructions added to a computer program) that would cause the extra interest for every customer in the bank to roll into a phony account under the name of Zwana. He happily collected pennies that turned into hundreds, then thousands of dollars over a three-year period. Until the scam was detected by fluke. The marketing department of the bank was demonstrating the wonders of the system and pulled the last name in the file, Zwana. Much to their embarrassment, Zwana did not exist.

Superstition can be an unfortunate characteristic among management. Security is often given a low priority status because managers would rather believe that it's the guy across the street who will get hit, not them. They haven't been hit yet, so why throw money away?

All it takes is one. Do you go out and buy car insurance *after* you've totaled your car in a collision? The lucky charm approach to security has a short life.

Not long ago, I interviewed a top-level manager who had a particularly enlightened attitude toward security. He hired a security consultant knowing the consultant would bring a wealth of experience to the firm. The manager felt that it was about time to make some original mistakes, and not repeat the mistakes everyone else had made.

In today's information-mad society, computers have us by the jugular. Millions of computers link people to offices, bureaus, divisions, and homes across continents. The growth of PCs in corporate America rises exponentially with each passing year. Coupled with this growth is the

staggering problem of control, a decentralized nightmare. Who is performing what on which machine and when and where and . . . WHY?

SECURITY AS RISK MANAGEMENT

The effective manager is a master juggler—he knows the meaning of balance. Security is the province of the risk manager; any manager who is forced to decide on security issues is by definition, a risk manager. The risk manager is the gambler who holds the cards, and whose job it is to know exactly what is at stake. The level of security a risk manager chooses must be based on his company's dependence on the computer system. In other words, how crippled would the firm be in a worst case scenario?

The risk manager must evaluate the company's dependence on its system, be suspicious by nature and trust little on face value. He must plan fall-back strategies, and hope he hasn't overlooked anything.

What exactly are the risks to which the microcomputer system is vulnerable? Here are but a few:

- Destruction of the computer hardware, software, or vital data by disgruntled employees.
- Damage to computer hardware, programs, or data due to power failures.
- Loss of unpatented trade secrets, designs of products in development that find their way into the hands of competition.
- The disclosure of private, potentially discriminatory personnel records (such as alcohol rehabilitation or psychiatric records).
- Leakage of personnel salaries.
- Alteration or erasure of months, perhaps years of vital company data stored on magnetic media—financial records, accounts receivables, sales orders.
- Willful data entry errors for the purposes of embezzlement or fraud.

The risk manager's task is not an easy nor an enviable one. While the corporate information resources may ride on his shoulders, the risk manager cannot fall prey to the Chicken Little Syndrome. At the first instance of a breach or threat, managers often react in a crisis vein, overly paranoid. Risk managers are ineffective when formulating