Commonsense Computer Security

Your practical guide to preventing accidental and deliberate electronic data loss

Commonsense Computer Security

Your practical guide to preventing accidental and deliberate electronic data loss

Martin R. Smith

McGRAW-HILL BOOK COMPANY

London · New York · St Louis · San Francisco · Auckland · Bogotá
Caracas · Hamburg · Lisbon · Madrid · Mexico · Milan · Montreal
New Delhi · Panama · Paris · San Juan · São Paulo · Singapore · Sydney
Tokyo · Toronto

Published by
McGRAW-HILL Book Company (UK) Limited
SHOPPENHANGERS ROAD · MAIDENHEAD · BERKSHIRE · ENGLAND
TEL: 0628 23432; FAX 0628 770224

British Library Cataloguing in Publication Data

Smith, Martin R.
Commonsense computer security: your practical guide
to preventing accidental and deliberate electronic data loss.
1. Computer systems. Security measures
I. Title
005.8

ISBN 0-07-707162-X

Library of Congress Cataloging-in-Publication Data

Smith, Martin R.
Commonsense computer security: your practical guide to
preventing accidental and deliberate electronic data loss/Martin R. Smith
p. cm.
Bibliography: p.
Includes index.
ISBN 0-07-707162-X
1. Computers—Access control. 2. Data protection. I. Title.
QA76.9.A25S64 1989
055.8—dc20 89-32197

234 WL921

Filmset by Eta Services (Typesetters) Ltd, Beccles, Suffolk
and printed and bound in Great Britain by
Whitstable Litho Printers Ltd., Whitstable, Kent

Foreword

Computer security is not a new subject but until recent years was either largely ignored or inadequate attention was paid to it by corporate management. Recognition of its critical importance has grown as organizations have become increasingly dependent upon computers and thereby vulnerable to business loss or damage in the event of computer system failures, whether accidental or deliberate.

The historical approach to computer security has generally been oriented towards the protection of computer resources as seen from the viewpoint of data processing professionals. This book, however, brings a new perspective to the subject in that its author is a security specialist whose emphasis is on the practical application of traditional security methodology tailored to the electronic data processing environment. Security as a management issue is clearly described, with particular concentration on people rather than technology as the key factor. Also well demonstrated is the important consideration that computer security does not have to be a complicated or unduly expensive affair.

Awareness is the prime objective of this book—by line management as well as by computer professionals. It is a comprehensive work with a style that is both technical and readable: it will provide a framework for developing and implementing an effective corporate computer security policy.

I welcome its publication.

David Lindsay FBCS BA(Com)
Honorary President, BCS Computer Security Specialist Group
Member, BCS Security Committee
UK Representative and Secretary, IFIP TC11(Security)

Preface

Information is the key resource of industry and business today; it is the new currency. Growth and success follow from good information; failure follows from its loss, corruption or unavailability. Possession of information has become a goal in itself, and the methods the opposition use to acquire it vary from the ingenious through the improper to the downright dishonest. Like capital and people, information is an essential corporate asset. Yet this vital resource now resides in vast quantities unnoticed and unprotected within the new technology that today has become part of our everyday lives—the computer—and the perils associated with the loss, corruption or non-availability of such electronic data await the unwary, unwise or careless.

Computer security has become the subject of much discussion and a whole industry of books, seminars, conferences and courses has emerged. But still precious little has been done about introducing it practically. Most believe they have no need for it, or insist that disasters and security breaches only happen to others; some learn the hard way that this is not so. We can no longer claim, as most do, that computer security is in its infancy: this is not true and is just an excuse. It need not be, as many claim it is, either complicated or expensive, nor is it an impossible task. The solutions are straightforward, and need not be highly technical. Low-tech insider crimes and operator errors are the greatest threats, not highly sophisticated attacks; the countermeasures need to be similarly uncomplicated. Computer security is a people problem, not a machine one, and should be dealt with accordingly.

Yet computer security continues to be dismissed from the business equation. Management is only interested in results with the minimum overheads, and has no time for the new-fangled machines provided they do their job; computer personnel nurse their charges with all the fervour of young mothers, with total faith in them and complete blindness to their faults and weaknesses; and security staffs display ignorance, and a suspicion and distrust of this new technology verging on the phobic. All this and a frenetic rate of development—half the products on the market today had not even been thought about a few years ago.

Positive efforts by all concerned are needed if progress is to be made towards improving the safety and security of computers, their operations and their data. The importance of this increases as we are driven towards greater networking, more distributed resources pushed downwards to the desk of the lowliest worker, and with open systems interconnection (OSI) a more open and therefore inherently more insecure computing environment. However, the beginning of this process is an understanding of the dangers and available defences, in terms comprehensible to all parties involved. This book aims to provide just that. In simple language, free from the misconceptions, prejudices and suspicions of managers, ADP experts and security staffs alike, the threats to computers are described and their vulnerabilities defined. Countermeasures are listed to allow a cost-effective security policy to be developed. No simple answers are offered, but armed with a basis of common knowledge the corporate team may then consider the options available, if not to eliminate the threat, then at least to reduce it to an acceptable level. Further, armed with such knowledge, management will once more be in charge to dictate its security requirements to the computer suppliers and not, as is the case now, the reverse.

My background is not in computing but within the diverse world of security, and I bring with me into the world of information technology the lessons I have learned in traditional security methodology. Defence in depth is offered as the most effective counter to the many weaknesses inherent in computer systems, and I discuss each element of security in detail but in non-technical terms—I know no other way. It is hoped my small contribution to the 'great debate' will reach all staff, whatever their role, training and background, and enable everyone to meet on the common ground of understanding. The views expressed in the book are obviously my own and not to be taken as representative of the Royal Air Force or any other organization.

One final word of encouragement: I believe the vast majority of those involved in any way with the computing world, like their colleagues in almost every other walk of life, to be honest and conscientious. If they are failing in their duties it is probably due to over-enthusiasm or ignorance rather than from malice aforethought. During the time I have worked within the field of computer security I have encountered a most positive reception from computer, security and executive staff alike. They are uneasy in their minds anyway, without really knowing why, but once the dangers have been explained to them there is an almost frantic willingness to learn about and improve computer security standards. It seems the only barrier to a massive step forward is the current lack of awareness. In 1960, following his study of security in government departments, Lord Radcliffe stated that then the biggest single risk to security was probably a general lack of conviction that any substantial threat exists. Nearly 30 years on, this has become so true today of computer security, but as noted in the Radcliffe Commission report this attitude of mind can be overcome by a 'sustained and skilfully directed educational effort in the right quarters'. This, then, must be the way forward.

Martin R. Smith
1989

Acknowledgements

I would like to thank my mother and father for their support and example, and my good friends and colleagues Gordon Burge and Rob Murray for their assistance and encouragement throughout the writing of this book. The work of officers and airmen of the Royal Air Force Police, and especially the early and painstaking research by Bill Pepper, have been the source of much inspiration. I am very grateful also to the following for their advice: John Sherwood, for network security; David Davies, for insurance; Alex McIntosh, for the security of personal computers; Duncan Whitley, for physical security; David Lindsay, for personnel security; and Alan Reed, whose excellent book *Computer Risk Manager* was the basis for my chapter on disaster planning.

Finally, I would like to pay my respects to John M. Carroll. His book, *Computer Security*, the first edition of which was published as long ago as 1977, has in my opinion yet to be surpassed, and I recommend it without reservation as the next step for those of my readers who wish to delve yet deeper into the fascinating topic of computer security.

Part One

The nature of the problem

Contents

Foreword xi

Preface xiii

Acknowledgements xvii

Part One The nature of the problem

Chapter 1 **The nature of computer security** **1**
What is a computer? 1
What is security? 3
What is computer security? 4

Chapter 2 **Threats and vulnerabilities** **7**
Qualities of information 7
Vulnerabilities of computers 7
Threats to computers 9
Risk to computers 12
Methods of exploitation 13

Chapter 3 **Countering the dangers** **15**
The nature of the security features 15
Defence in depth 16

Chapter 4 **Valuing data** **21**
Types of data 21
Classification 22

Part Two Responsibilities for computer security

Chapter 5 **Computer versus security staffs?** **27**
The interdisciplinary approach 28
Mutual problems 28
The problems with being a computer person 29
The problems with being a security person 30
The role of the auditor 33

Chapter 6 Allocation of computer security duties **35**
Naming names 35
Who's in charge? 35
Chain of command 36
The allocation of computer security duties 36
Installation security committees 43

Chapter 7 Registration of computers **45**
Why register computers? 45
Responsibility for registration 46
Uses for the register of computers 47
Updating the register 48
Serial numbering of computers 48
Contents of computer registration documents 48

Part Three The solution

Chapter 8 Physical security **53**
Defence in depth—the fortress concept 53
Aims of physical security 54
The physical protection of computers 55
The physical protection of computer installation services and utilities 59
Fire protection 61

Chapter 9 Document security **65**
What is a computer document? 65
Handling computer documents 66
Marking computer documents 67
Accounting for magnetic media 69
Accounting for associated documents 70
Purging magnetic media 71
Backing up magnetic media 73
Destruction of computer documents 74
Checks and musters of computer documents 75

Chapter 10 Personnel security **76**
The elements of personnel security 76
Fundamental principles of personnel security 77
The threats from staff members 79
The motivation for crime 81
Personnel security measures within a computer installation 82

Chapter 11 Hardware security **92**
Securing hardware from tampering 93
Hardware identification devices 93
Hardware integrity checks 94
Maintenance procedures 95
Fault tolerance 98
Contracts 99

Chapter 12 Software security **101**
The aims of software security 101
The limitations of software security 102
Software security—general measures 104
Software security—access control 106
Software security—separation 112
Software security—audit 116
Software security—programming 118
Covert channels 119
The 'Orange Book'—the US Department of Defense trusted computer system evaluation criteria 120
Bugs and viruses 127
Some final thoughts 128

Chapter 13 Compromising emanations (TEMPEST) **130**
The nature of the problem 130
The dangers from TEMPEST 131
Simple precautions against TEMPEST 132
TEMPEST-proofed equipment 133

Chapter 14 Communications and network security **135**
Methods of data transmission 136
Transmission characteristics 137
Networks 139
Aims of communications and network security 140
Threats to communications and networks 143
Methods of protection—cryptology 144
Methods of protection—physical and procedural security 150
Hacking 154

Chapter 15 Disaster planning **157**
The need for a disaster recovery plan 157
Developing a disaster recovery plan 158
Stand-by facilities 166
Contents of the plan 168
Invoking the disaster recovery plan 169

Chapter 16 Computer insurance **170**
Problems with insurance 170
Risks that can be covered 172
Types of cover 173
Claims that can be made 173
Where to buy your policy 174
Do's and don'ts of computer insurance 174

Chapter 17 Security of personal computers **176**
History of the personal computer 176
Uses of the personal computer 177
Weaknesses and vulnerabilities of personal computers 179
Countermeasures to protect the personal computer 181

Part Four Plan of action

Chapter 18 Developing a computer security policy **193**
Defining the computer security policy 194
Risk analysis 194
Format of the computer security policy 197
Contents of the computer security policy 199
Uses for the computer security policy 202
Security operating procedures 203

Chapter 19 Training and awareness **206**
The need for training and awareness 206
Training for computer security 207
Awareness of computer security 211
Some final thoughts 213

Bibliography **215**

Index **217**

1

The nature of computer security

What is a computer?

> *Computer—automatic electronic apparatus for making calculations that are expressible in numerical or logical terms; reckoner, calculator. . . .*
>
> (Concise Oxford Dictionary of Current English)

> *It's a sort of electric brain, daddy.*
>
> (Madeleine Rose Smith, age 7)

We all know what a computer is, at least until we have to define one precisely. Certainly, computer technology has entered our everyday lives to an extent most of us have yet to fully realize, and as such computer applications become increasingly diverse and widespread, our dependence on them grows accordingly. Indeed, we are already at a stage where the loss of computer facilities in a host of areas would endanger our lives, our well-being and our businesses. There are few functions in our modern society that are not becoming computer dependent.

But what is a computer? It is nothing more than a machine for the manipulation of information in electronic form. It is no more important in itself than any other tool, except that its fuel is the modern currency of information, and its speed, accuracy and memory provide considerable attractions to all areas of commerce, industry and the Government. And because it is such an efficient and helpful tool, it makes itself indispensable in a very short time. Its principles of operation are unseen; its functioning is silent and mysterious. Many people are ignorant and fearful of this still modern invention, and this prejudice is self-perpetuating. Understandably, computer personnel do little to dispel their unsought status and strength as masters of these awesome machines; their specialist language further isolates them from others. Many of us 'outsiders' do nothing to come to terms with the inevitable march of progress towards a computerized society. Instead of education, there is polarization, especially between the young and the old; and as computer technology becomes more advanced and its applications more specialized, this gap between computer people and non-computer people can only widen. Yet the fact remains that computers are only tools for the manipulation of data, and are basically extremely simple and remarkably stupid machines. They are nothing to be frightened of.

It is the information within the computer which is the essential resource. Possession of accurate, up-to-date and comprehensive information is now the key to growth and success, when once it was perhaps the ability to manufacture, or harvest crops, or trade overseas. The City of London, for example, is nothing more than a giant information factory. The capacity to manipulate data, to model forecasts of events, to store, channel and transmit information as required--these are the modern measures of success or failure. The computer myth has masked information as the real hero of the modern age, and our attentions must not be diverted from the need to protect and preserve that vital data by an obsession with its container, the computer. It is the data which we must keep confidential, free from corruption, safe from the elements, the thief, and the saboteur, and available when needed, literally at the touch of a button.

A computer, then, is a data processor which permits arithmetic and logical operations without the intervention of a human operator and working to a set of stored instructions (the program). Computers are unintelligent, although they appear to be more clever than they actually are because their programs can be written to take account of previous data and results.

The main characteristics of a computer are:

1. *Speed* The speed with which computers, in particular the latest models, can process and manipulate data is almost beyond comprehension, with millions of calculations taking place each second.
2. *Accuracy* Computers will perform a given task exactly as instructed, as many times as required, with an error rate a fraction of that of humans. The operators, the programmers and the users are responsible for the greatest part of any computer's failings.
3. *Memory* Computers can store data in vast amounts, compacted into minute areas within microchips, or on magnetic tapes or fixed and floppy magnetic disks.

Processes may thus be complex to a degree previously beyond the normal realms of human ability. Not only can tasks now be performed with ease and speed, which before would have required an inordinate effort or simply have been beyond sensible or manageable human resources, but also human effort can be eliminated entirely in many areas. Such savings can be used to release staff from drudgery and improve efficiency; often though, they have simply resulted in staff reductions which in turn have contributed to the fear of, and resentment towards, computers.

The refinement of computers has raced ahead since the invention of the earliest device. Several generations of computers have come and gone, and the progress continues with ever-increasing pace. As this evolution has continued, the computer has moved away from the enormous, environmentally controlled frame rooms, in centralized locations and with specialist staffs tending to their every whim, to the personal computer taking massive processing power to the office desk, typing pool and factory floor and placing it in the hands of the ordinary worker. It is as if the mainframe has burst like a ripe fruit, scattering its seeds throughout all parts of the organization to germinate as personal computers (PCs), which in turn have spread their network connections like the threads of a spider's web.

Whatever its form, though, the computer remains essentially a simple device, and while its internal workings will be necessarily complex, the actual operation remains straightforward. While the modern road vehicle can be a highly sophisticated piece of machinery, most of us can, with only a little training and some practice, drive one. There is no real need to understand how a car works, merely how to work it, and once mastered it is then a relatively straightforward progression to the juggernaut. It is thus with computers. (Nevertheless, a basic understanding of the principles of any machine must improve one's performance on it.)

What is security?

> *Keeping me safe, and keeping people out.*
>
> (Peter Henry Smith, age 5)

We live in an unsafe world, in which every day we encounter threats against our safety and security. There are, too, our own weaknesses and vulnerabilities, those of our families, and those in the physical defences we have built around us to defend our lifestyles. These threats and vulnerabilities to our well-being are often inevitable: sometimes they can be reduced or avoided, or they can be transferred to an insurer, or we can accept and ignore them. Our lifestyles are a balance between the risks, the threats and vulnerabilities and the countermeasures, or else we would all either be dead or nervous wrecks. We can never hope to protect ourselves entirely, risk taking is an essential ingredient of our make-up, and a level of stress is necessary for us to achieve a balanced state. Too little stress can be as harmful for us as too much—the racing car driver or mountaineer will testify to the benefits and pleasures of controlled stress.

We build up our homes over a considerable period. Our endeavours over many years can be most clearly seen in our possessions, our homes, cars, gardens. These valuable and sentimental assets, and our loved ones, are subjected to the threats of fire, flood, theft, damage, and a host of nightmarish dangers which we cannot entirely eliminate but which we can accept within reasonable limits. We develop, often subconsciously, our personal risk assessments to produce unique security policies within which we live our lives. We spend a certain amount on insurance; we spend so much money on locks and anti-burglar devices; we drive at certain speeds and in a way which makes us feel safe; we empty ashtrays in the lounge last thing at night; we don't allow our daughters to walk home from the dance on their own at night. Most of us discover an acceptable position in the centre ground which, in the main, avoids the unfortunate experiences, or at least softens the results, while allowing us to continue normal lives and avoid the traps of obsession or paranoia.

Good security, then, both at home and at work, consists of the identification of all the threats and vulnerabilities, an assessment of the likelihood of a particular misfortune afflicting us, and a reasonable and personally acceptable combination of countermeasures to protect our families, ourselves and our possessions accordingly. The effort applied will, of course, depend on the value of the asset concerned; we will take more care of our personal safety than we will of our possessions, or at least a reasonable person will, but of those possessions we are likely to take more care of our expensive jewellery, or the deeds to our houses, than we are less valuable or important objects. But, human nature being what it is, stable doors will be bolted too late, our efforts being redoubled after a threat materializes; homes, once burgled, will sprout alarms, and driving will be far more cautious after an accident—for a while!

What is computer security?

Within the specific environment of the computer, security entails:

1. Identification and valuation of the assets to be protected, so that none is overlooked and the more valuable can be looked after better.
2. Recognition of the peculiar vulnerabilities and weaknesses of computers in general, and the system in question in particular.
3. Identification of all the threats against computers in general, and the system in question in particular.