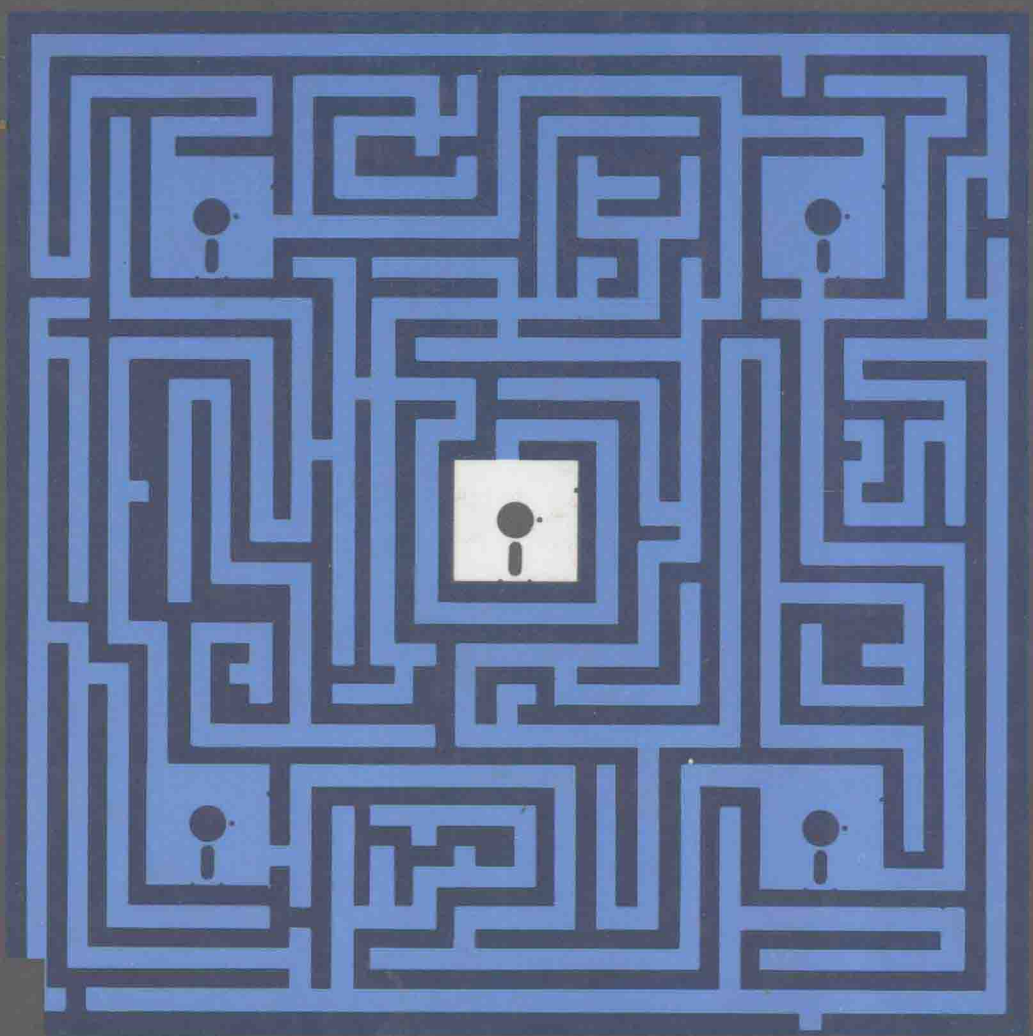
Protecting Information on Local Area Networks

James A. Schweitzer



Butterworths

PROTECTING INFORMATION ON LOCAL AREA NETWORKS

James A. Schweitzer

Butterworths
Boston London Durban Singapore Sydney Toronto Wellington

All references in this book to personnel of male gender are used for convenience only and shall be regarded as including both males and females.

Library of Congress Cataloging-in-Publication Data

Schweitzer, James A., 1929–
Protecting information on local area networks /
James A. Schweitzer.
p. cm.
Bibliography: p.
Includes index.
1. Local area networks (Computer networks)—Security measures.
I. Title.
TK5105.7.S39 1988
004.6′8—dc19 87–17219
ISBN 0–409–90138–5

British Library Cataloguing in Publication Data

Schweitzer, James A.
Protecting information on local area networks.
1. Local area networks (Computer networks)
2. Data protection
I. Title
658.4′78 TK5105.7
ISBN 0–409—90138–5

Butterworth Publishers
80 Montvale Avenue
Stoneham, MA 02180

10 9 8 7 6 5 4 3 2 1

Printed in the United States of America

PROTECTING INFORMATION ON LOCAL AREA NETWORKS

To Art Axelrod, Carl Grovanz, Myra Johnson,
Paul Kittredge, and all others who have contributed
to the development and implementation
of electronic information security at
Xerox Corporation, 1977–1987.

And to Brian Hollstein and Dick Randazzo,
who have provided us with consistent
management support.

Introduction

Information has become a valuable resource. Not only is information costly to produce and maintain in a usable form at the right time and place, but it is also crucial to maintaining market share and competitive position in a technological world. Many experts (see, for example, Diebold 1979 and Naisbitt 1982) conclude that information is among the most valuable business resources.

Although networks allow us to make better use of information, the large number of network-connected devices poses a serious threat to information quality. Thousands of people are now connected to business networks, with potential access to information bases. There is a churning of information as these system users change data or move information around. A critical problem is how to manage the valuable information flowing across many networks to hundreds or thousands of employees (and outsiders).

Some idea of this challenge can be gained from considering that one large company has more than fifty individual networks with thousands of connected employees. Similarly, a leading computer manufacturer has networks connecting fifteen hundred mainframe computers with two hundred thousand workstation or terminal users.

We can infer two things from such networks. First, almost everyone who owns a microcomputer with a communications connection is physically connected to everyone else, by virtue of the worldwide telecommunications grid. All those computer users may not be logically connected, but that separation is likely the result of a lack of standards rather than a control effort by management. Second, protecting the information passed through this grid requires careful planning and an immense educational and motivational effort by business managers.

USING NETWORKS IN BUSINESS

Before we consider appropriate management actions to ensure some control over the use of networks and the business information resource, we should look at the various types of networks and why they are being expanded at such a rapid pace.

Today's microcomputers and highly efficient communications systems constitute an economic driver that encourages management to invest in more business networks. The economic driver results from these factors:

1. Administrative work is essentially a process of communication of information. Analysis of almost any office job will show that it consists of developing, collecting, modifying, and distributing information. All "knowledge workers"—

that is, those persons whose contribution to the business consists of nonphysical products—work at information tasks. These people tend to be the most highly paid and most important employees in a business. A study by Booz Allen & Hamilton concluded that skilled professionals in the United States were paid $400 billion in 1979; clerical workers received only $125 billion. Hence, a 15 percent improvement in productivity from managers and professionals would save a lot more money than would an equivalent improvement for secretaries (Yourdon 1986). New applications of computing and communications will tend to spread throughout those employee groups that have not traditionally had office equipment. These are the decision makers, analysts, and professionals who have been wedded to the pencil and calculator. No more!

2. Administrative costs are the fastest rising portion of business overhead. The most promising opportunity to reduce administrative costs is through the use of automation systems for knowledge workers. The payoff level, where system costs are justified by a reduction in administrative costs, is being driven lower and lower by the continually improving cost-performance ratio of microcomputing and communications systems (Strassmann 1985).

3. Highly competitive worldwide marketplaces, especially for high-technology industries, make current information a critical need. Business leaders see automation as a means of delivering strategic decision-base information at the time and place needed. Networks are the key to this service.

4. Communications costs are declining rapidly in many cases; for instance, the cost of a four-minute call from New York to Los Angeles during business hours fell 26 percent from 1983 to 1986. The fact that telecommunications price reductions are not consistent across all applications is more than offset by computing functionality delivered by local area networks (LANs).

Basic data processing is no longer the answer to management needs for control and information. Rather, traditional information systems are now being integrated with communications technology to create vast networks of computers. In addition, most critical, time-sensitive business information now spends a good portion of its life cycle in electronic form.

THE NETWORKS

This book is not a tutorial on network technology, but every business manager should be aware of the various network options available for both intersite and intrasite communications and the security risks involved in each application.

Intersite Data Communications

Because of the huge investments required to establish a viable communications system, most intersite business network traffic travels over circuits (land lines and

radio links) provided by the communications utilities (in the United States, these include AT&T and GTE; in Europe, the PTTs and British Telephone). These public carriers provide various classes of service, including conditioned data lines and packet-switched services. Selection from among the alternatives is usually based on volume of traffic and quality of service required.

Value-added providers resell the communications utilities' capacity after adding special features such as packaging and delivery services. Private carriers also offer network services. One example is a railroad that has used its right-of-way to lay fiber-optic cable connecting the larger cities. Some of the capacity of the optical net is used for railway signals and other traffic, while the excess capacity is sold to businesses.

Sometimes a network, when leased by a business, will be referred to as a private network, although this might not be strictly true. A company usually pays for a logical circuit, not a physical wire, radio relay, or satellite. The seller can then switch traffic among various network alternatives, making sure the capacity remains constant. In some cases, the user does lease specific circuits and can identify the circuit numbers for purposes of traffic analysis. This does not always mean, however, that the physical identity of the circuit is constant.

Computer manufacturers have provided special network architectures (essentially, collections of communications protocols) to improve the efficiency of sets of computers and devices connected via communications lines. IBM's Systems Network Architecture, or SNA, sets specification standards for the devices and services of a data network. Similarly, Digital Equipment Corporation's DECNET establishes interconnection protocols and requirements. A critical problem today is the inability to connect networks and equipment from various suppliers.

In 1981 the International Standards Organization (ISO) adopted the Open Systems Interconnection Reference Model. This model provides for eight layers of architecture to be used in defining the functions required for all communications systems. Eventually, when widely implemented, the ISO model should ease the problem of interconnection of various communications facilities and equipment.

Intrasite Data Communications

While it has long been possible to connect computers and terminal devices located in one building or in a collection of nearby buildings using telephone circuits, really efficient communications within a site were first delivered by the local area networks, or LANs. These networks allow high-speed, high-volume concurrent interconnections among large numbers of workstations (microcomputers), central processors, and communications gateways. The latter allow further communications with outside public networks and, via those facilities, with other LANs and computers.

The number of LANs is growing rapidly. In 1985 and 1986, the number of LAN connections in the United States increased by more than 200 percent. The

installed LAN-connected unit base (mostly microcomputers) grew from 735,000 units to 2,383,000 units during that same time. The use of digital private branch exchanges (PBXs), an alternative to LANs in some situations, also increased markedly in that same period. The LAN is generally considered superior, however, in terms of potential for business data handling applications (Ellison and Pritchard 1986).

A brief consideration of two LANs offered by widely known suppliers might help explain what a LAN is and how it works.

Xerox Network System and Ethernet

Xerox Network System (XNS) presents an architecture that distributes microcomputers throughout a network-serviced organization. There is no need for a central processor or host. Fast (10 megabits per second or 1,000,000 bytes per second) data communications are provided among microcomputer workstations (used by people) and servers (systems service machines) connected to the local network using carrier sense multiple access/collision detection methods. The carrier is a baseband cable implementing the Ethernet protocols (also used by Digital Equipment Corporation, or DEC). Communication with external networks, computers, and other devices is provided through one of the connected servers, which acts as a controller. In many applications, all the stations (or servers) on the network are replications of one equipment scheme programmed to provide different services. All appropriate standards are implemented to allow connection with equipment and networks of other design.

AT&T Starlan and ISN

ISN is a high-capacity, packet-switched backbone for integrating dispersed and varying devices. Starlan is a one-megabit-per-second baseband LAN for personal computers, file servers, and peripherals. Multiple Starlan networks can be connected via an ISN node. ISN also can provide communications services to outside networks of varying architectures.

DISTRIBUTED PROCESSING

While not strictly a type of network, distributed data processing (DDP) is a relevant concept that uses both centralized and decentralized information systems. Local intelligent terminals or microcomputers are connected to a central mainframe system via a communications network. Part of the information processing load is carried by the remote computers, thus performing the work closer to the originator and also providing for redundancy in case one unit fails. Data are usually forwarded periodically to a central computer, where the company's data base is maintained. Summary reports, invoices, and so forth are then returned from the central site to the distributed processors. The local computers, of course, are also used for various specialized applications unique to each site. To-

day, 50 percent of large companies have some kind of DDP. This reflects a trend toward decentralized management, found in more than 80 percent of large businesses (Blank 1986). The spectacular growth in personal computing, driven by cheap hardware and obvious benefits, is the driving force behind the application of DDP.

CONCLUSION

The use of LANs with flexible architectures such as those described for XNS and Starlan means that business managers can design, almost without limits, networks configured to meet all business requirements. They can choose from a wide variety of communications services provided by others for connection over long distances by land lines, radio (including satellite communications), or a combination of these. Services can be tailored to volume or quality requirements, and a variety of such services is offered by public utilities and value-added marketers. Further, business managers can also invest in substantial communications facilities within a building or set of buildings. Most often, these facilities are LANs, special high-speed integrated systems of terminal devices and cables.

Current networks involve the integration of office systems with personal and departmental computing. The rapid development of network-supporting technologies and applications reflects an apparently insatiable demand for connectivity. The host of new technologies and innovative network systems applications, along with the changing work structure and relationships, are altering the ways in which business operates (Kirkley 1986).

The selection and installation of a network is only one part of the management task. In this book, we will consider how management can gain control of the valuable network-serviced information resources now generally available. We will see that the information resource is sometimes wasted or exposed through poorly planned, widespread employee use of computing and communications, and through broadly authorized access to business information bases. Within a short period of time, almost all employees (and perhaps others less welcome) will have access to at least a portion of a business's information base, usually network-connected in electronic form. Our ability to manage and control this valuable yet widely accessed resource is the subject of this book.

Contents

PART I

Background

ONE

Understanding Today's Computer Networks

Digital Equipment Corporation founder Ken Olsen, quoted in the *New York Times,* September 4, 1986: "You start with the network, then you hang the computers on later."

"We need to adopt the realities of today's technology: that computing power is cheaper and more expendable than people power; that the network is of ultimate importance in determining overall systems performance." (Manganelli 1986)

Since the delivery of the first commercial computer in the mid-1950s, computing technology has developed at a startling pace. As computers have become more cost-effective (that is, each year a computer of a given size can perform x additional millions of instructions per second), they have also become cheaper and smaller. H.R. Grosch, a well-known authority on computing, says that computer economies relate directly to computer speeds; that is, to achieve a tenfold improvement in price performance, the computer must work one hundred times as fast (Kang et al. 1986). The microcomputer (the ubiquitous personal computer) has proven that general theory to be true, delivering astonishing computing power to the individual at work, at home, and even on airplanes. The technological breakthrough of being able to place an entire processor on a single mass-produced silicon chip (called very large system integration, or VLSI) has made the microcomputer possible (Blank 1986).

Computing applications have evolved to fit almost every requirement, from basic replacement of routine manual clerical work (such as payroll) to sophisticated process control (oil refining). Recently, imaginative applications have given rise to new businesses and have provided existing businesses the opportunity to

---

This chapter introduces our subject. If you are familiar with computing and networks, you may wish to skip to Chapter Two.

expand their activities. Computers have become such an integral part of daily life that our present era is often referred to as the Computer or Information Age.

Today we see a wide variety of powerful computer hardware, from the number-crunching supercomputer to the tiny lap-top portable, with an endless array of applications software, from the word-processing package to the complex programs running an automated steel mill. And the cost per million instructions processed per second (the "MIPS" discussed in computer articles) continues to go down.

Imagine all those computers, large and small, working away at applications. If they each worked individually, the benefits would be far less than optimal. The one factor that makes all these uses of the computer possible, and so attractive, is intercomputer communications.

COMMUNICATIONS BRINGS ADDED VALUE TO COMPUTING

Mainframe computers are being connected to other mainframes and to distant minicomputers, microcomputers, and workstations in a rapidly growing network of high-speed communications lines. In his book *Computer Networks,* Andrew Tanenbaum identifies some good reasons for this (Tanenbaum 1981):

- Business computers that were initially placed to serve the processing requirements of one site are being connected so that executives can quickly call up summaries of data for companywide management purposes.
- Business recognizes that, with the decreasing costs of communications, companies can reap important benefits by making data base information available to anyone, anywhere, when he or she needs it. The individual user, however, should not have to go to the trouble of preparing applications programs or getting expert technical help. The real promise of a business data base is that of sharing current, reliable information. Effective networks, smart workstations, and powerful data base software make this promise a reality (Curtice 1986).
- The reliability of a company's information processing infrastructure can be enhanced by backing up facilities via communications lines.
- The impressive cost performance of microcomputers (also known as personal computers, or PCs) means that data can be processed at the site where it is generated, resulting in more accuracy, and then forwarded to company headquarters on a network, perhaps using otherwise idle time at night.
- A network of intelligent workstations, connected through local and wide area networks, can provide a powerful information exchange medium for all the company's managers. Message (or electronic mail) systems can allow persons thousands of miles apart to coauthor documents, sign off or modify engineering specifications, and exchange messages in a few seconds.
- Microprocessors have a vastly superior price-performance ratio than main-

frames. Although big computers are ten times faster, they may cost a thousand times as much per unit of computing as personal computers.

A *computer network* is an interconnected collection of autonomous computers or a set of computers using common protocols. Some are enormous and complex; the Digital Equipment Corporation operates a network with 60,000 users in 250 locations spread across 29 countries. Certain computer networks might be called *distributed computing systems;* these are networks of computers that share a common operating system. (Xerox Corporation's Internet is an example of such a system, which is comprised of a set of LANs interconnected by a wide area network.) Other networks of computers are called *distributed processing systems;* these share common applications and software but may have different operating systems.

Finally, Tanenbaum (1981) points out that increased reliability can be gained by connecting computers; if one fails, another can pick up the load. Also, the relative price of communications services versus computer hardware is an important consideration. Communications has become inexpensive over the past fifteen years, the same time frame in which the cost of microcomputers has fallen sharply. Thus, the cost of a network is most attractive when measured against the potential business benefits.

TYPES OF COMPUTERS

If we consider current computer use in a simplified way, we see that there are three general types or sizes of computers, although the groups do overlap. Further, we see that most of these computers are now connected by some kind of network.

The general types of computers are mainframes, minicomputers, and microcomputers. Mainframes are large, high-volume, high-speed data processors, which are almost always found in data centers with specialized operating staffs. The work processed on mainframe computers usually consists of data base and high-volume records processing. Mainframe computers are typically connected to wide area networks, for subsequent connection with LANs or other mainframes. In some applications, such as time-sharing uses, the mainframe services various dumb terminals. Mainframes are usually separated from the communications network by a front-end processor, which controls communications and also can provide access security.

Minicomputers are smaller, often specialized high-speed computers used in research, engineering, and other single-purpose environments. Usually most of the minicomputer load is for pure (mathematical) computing. In many applications, minicomputers work in networks with intelligent workstations and terminals.

Microcomputers are very small desktop or portable computers used at work, at home, and while traveling for financial analysis, word processing, and as pro-

fessional workstations. Most units connected in a LAN are actually microcomputers that act as "servers" with specialized tasks or as general purpose workstations. The personal computer is one type of microcomputer.

A fourth device, the terminal, is not really a computer, although when connected to a computer network, it takes on many of the same attributes, being able to retrieve information and to make use of the processing power of a central mainframe or minicomputer. The terminal, however, cannot do processing, so its uses are limited in potential information activities.

BENEFITS FROM NETWORKING COMPUTERS

While all computers offer important potential benefits to businesses, the real efficiency occurs when they are tied together in networks (Strassmann 1985). Interconnection of computers has the following implications:

1. Microcomputer-using individuals can retrieve data from large data bases on mainframe computers or minicomputers, can make use of the tremendous power of those larger machines, and can process retrieved information locally using programs written and run on the microcomputer.
2. Terminal users can access the central processor directly to retrieve or add data from or to central disk files. They also can use the power of the larger central computer to perform complex calculations that would otherwise be extremely time-consuming.
3. Microcomputer users can exchange data files, messages, and documents with any other microcomputer or terminal owner connected to an appropriate network.
4. Mainframe computers, minicomputers, microcomputers, and terminals can exchange data, messages, and documents.

One example of the advantages of intercomputer communications is an engineering department where various professionals are working on the design of a new product. Without leaving his or her workstation (a network-connected microprocessor), an engineer can perform various calculations, change schedules and drawings, coordinate and obtain approval of those changes with others working on the product, send drawings or messages to colleagues around the world, and print out paper copies of documents. Computer-aided engineering (CAE), manufacturing (CAM), and design (CAD) are illustrations of powerful systems using networked microprocessors and minicomputers.

Similarly, accountants, financial analysts, scientists, manufacturing supervisors, managers, executives, and secretaries can process data, create documents, send messages, file information, retrieve information from central data bases, process data, and do many other business tasks at electronic speeds. On a LAN these applications may involve filing, data retrieval, message, and computing services.