PREVAILING VIEW OF LAN SECURITY: LOTS OF TALK

Security is often pushed aside as a priority, but here is how a few micro managers handle it

By Johanna Ambrosio

Computer security is a lot like the weather. People talk about it, but no one does much about it.

Nowhere is this more true than in personal computer local area networks.

Although microcomputer managers consistently identify security as an issue, many rely on whatever level of security comes with the network operating system. Few, if any, additional measures are taken.

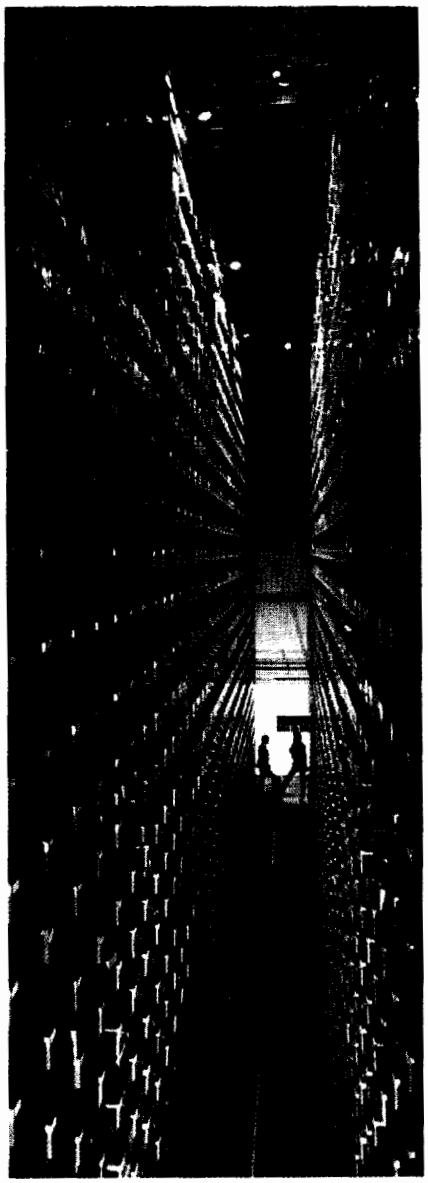
Experts say this could come back to haunt microcomputer managers as their LANs grow and become interconnected with other networks.

At most companies, the level of security provided depends a great deal on:

- what the LAN is used for;
- how many people are on the network and in the company;
- the culture of the organization;
- whether the LAN has hooks to and from the outside world; and
- the extent of central data processing organization control on the LAN.

The experiences of users in a hospital management group, a California college, a bank and a Big Eight accounting firm provide a realistic picture of how PC LAN security is being managed today.

LAN security encompasses not only software but the physical security of the computers and components; the confidentiality of data that is passed around the LAN; and the data integrity of the files that reside on the LAN's file servers.



Few would argue against the importance of any of these aspects of security, but day-to-day demands tend to win the most attention on priority lists in most companies.

"Network administrators say that security and backup are most crucial when it comes to LANs," said Matthew T. Camden, director of data processing for the University Hospital Consortium (UHC), Oakbrook Terrace, Ill. "Yet they are also the most boring parts of a network administrator's job, so they are also often the most lax."

IMMATURE LAN SECURITY PRODUCTS

Those MIS managers who have tuned into what PC LAN security products are available, often find essential features missing.

Owen Perillo, a telecommunications consultant with the Chicago office of Arthur Andersen & Co. in Chicago, said that while many network operating systems provide at least two levels of security, that is often not sufficient.

"PC LANs aren't as mature as other technologies like mainframes," Perillo said. "So the level of security built in isn't as sophisticated."

At the network operating system level there is generally a log-on and password required to get on the LAN. And at the file server level, depending on the user's security


PERILLO

clearance, he or she may have access to one or more pieces of the server.

But "a clever hacker can get around that, and you need security at the file level," Perillo said. However, even though there are over 30 third-party security packages, few organizations take security quite this far.

At the UHC, for example, Camden said, "Ours is a relatively small company with a user community that doesn't spend its time trying to break my security."

Nevertheless, he maintains several levels of security. "We have a half-billion dollars' worth of purchasing information on our network. If that were to fall into our competitors' hands, or be destroyed in any way, the damage to our company would be immense."

The UHC provides management services for hospitals affiliated with universities. The UHC can help negotiate volume purchasing agreements and arrange for the sharing of research and development resources.

Some 50 employees at UHC share a Novell LAN with two file servers. One server is dedicated to database applications. Administrative applications such as spreadsheet, word processing and graphics reside in the other. When users log onto the LAN, they are automatically hooked into both servers.

FUNDAMENTAL LEVELS

Camden concentrates on three fundamental security levels: internal on the LAN itself; to and from any outside sources; and viruses. He handles the last by insisting that no one beside himself put any software on the network. If anyone wants to install software brought from home, or from a bulletin board, Camden first inspects it and then installs it himself.

As for internal security, every user has a home directory that only he or she can access. This amounts to a safe haven for their own information, a place on the network for individual files. These directories are dynamically set up by the Novell Netware software when a user logs in and types in a specific password.

The shared files on the server are protected by Netware's feature that flags the user with allowed or disallowed actions when requesting a file. "The user is given a list of things he can and can't do, such as read but not alter," Camden said. He also has the option to change those parameters.

Additionally, UHC has a few communications PCs that are set up to allow people to dial in. With a package called Carbon Copy Plus from Meridian Technology, Atlanta, that resides on the PC, users are

asked for a password whenever a user dials into the PC. After getting through this level, a user then logs onto the LAN in the usual way.

Security can also be accursed by data processing people who, after all, are trying to provide services to their constituents. "You want to provide information and easy access. But there is an increasing need for adequate security, so you have to balance the two," Camden said.

Security controls are not stringent at Rancho Santiago College in Santa Ana, Calif., because the purpose of the LAN is to help educate the students, said John H. Luxenberg, coordinator of computer-assisted instruction.

Luxenberg runs a general-purpose microcomputer laboratory, where 18 workstations are hooked up with a Novell network. Students access software off the LAN to learn programming, and can also access outside databases.

However, because security is important for a network that handles traffic for administrative data and inventory control, that network is maintained separately. Luxenberg said, "You have to look carefully at who gets access to what. The easiest way is to only give write access where absolutely necessary."

Likewise, at Deloitte Haskins & Sells in New York, the Reports Department uses a 20-workstation LAN to produce reports with text and graphics. "At this point security hasn't been a major issue," said R. Bruce Johnson, manager of the Personal Computer Resource Center. "We use LANs to share devices and software, not to do transaction processing," he said. "Security isn't as much of a problem as file backup is."

NETWORK OPERATING SYSTEM TRUST

Other large organizations also rely wholly on the network operating system.

New Orleans-based Hibernia National Bank, with $5.5 billion in assets, is Louisiana's largest bank. The bank has eight Novell LANs; soon to be increased to 10. By year-end, 100 people will be hooked into the various LANs.

CARENDER

Tom Carender, information center manager, said, "Novell security is adequate. There are flaws with every system, but you can control the security."

Users who try to run single-user packages on the network are a problem for Charles W. Koman, vice president of communications systems at Drexel Burnham Lambert, Inc., New York City. He described his major gripe as "losing stuff as opposed to people stealing stuff."

Koman said, "A single-user package tries to write to a particular portion of the disk." "But by the

Turf Wars in Land of LANs

Some users find advantages in ceding territory to MIS

In many companies where local area networks were pushed and managed by the end user community, the central MIS department has begun to assert control.

MIS control can range from decision-making power over who gets LANs and which LAN they get, to consulting with end-user departments that want to install LANs.

Many observers feel this new MIS aggressiveness is long overdue. "Loss of control is the number one issue relating to LANs," said Mark Ricca, vice president of The Eastern Management Group, a consulting firm in Parsippany, N.J.

"It's a turf battle," he added. "Many user departments feel they're abdicating control when they go to the central DP department, but that [central] group looks beyond parochial interests to serve the company as a whole."

Tapping into MIS offers the advantages of bringing the departmental LAN into synch with the company's overall communications strategy, which encompasses security and portability issues, and the economies of scale through central purchasing. The disadvantages include added complexity and the need to give up some turf to MIS. "These issues can be ignored if the DP organization is circumvented," Ricca said.

PURCHASE METHOD IMPLICATIONS

The way a LAN is purchased usually determines its status in the organization. Most LANs are installed on a department-by-department level; the user groups either install the LAN themselves, go to a retail store or to the LAN manufacturer. One person in the end-user department then takes on the unofficial management of the LAN part-time.

"But as requirements grow, users want to connect to other LANs—and that's when the corporate MIS or telecom group usually gets involved," said Owen Perillo, telecommunications consultant with Arthur Andersen & Co. in Chicago.

"At that point it's discovered that each department has bought a different kind of LAN and that there are major incompatibilities to overcome."

MANAGE YOUR OWN

The central MIS group does not usually argue for control over the LANs because it does not have the resources to deal with them. So MIS relies on the user groups to manage their own LANs.

The solution of a Fortune 100 company in New York, one of Perillo's clients, was for MIS to select and install the LANs. But an administrator in each user department distributed passwords and managed hard disk backup concerns.

MIS control can range from decision-making power over who gets LANs and which LAN they get, to consulting with end-user departments that want to install LANs.

However, this approach does not always work. Hibernia National Bank in New Orleans at first relied on administrators in user groups, but now the central MIS group is doing all those tasks. "The people in user groups aren't really technical, so things can get really messed up," said Tom Carender, information center manager at the bank.

"Some people may get access to data they shouldn't have, and even if they don't know about it that's not a situation we want to occur," Carender added. "Or sometimes the administrators issue duplicate passwords."

Now Carender and an assistant see to the corporate networks.

HANDS-OFF APPROACH

Still, many MIS groups are comfortable with a more hands-off attitude toward LANs. At Drexel Burnham Lambert in New York, the end user groups have as much control as they wish. "The local department runs it. We don't have an involvement in the LANs, other than to help them get it up and running," said Charles Koman, communications systems vice president.

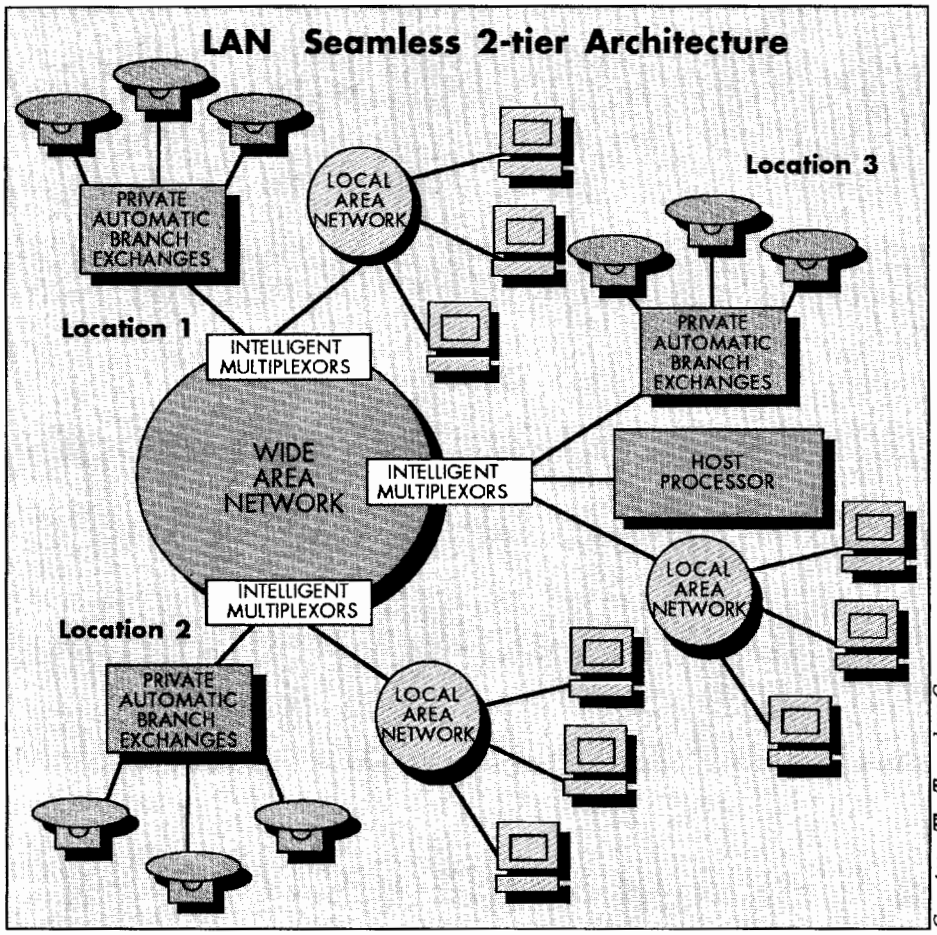
Typically, users who have no idea what products they want come to Koman's organization for help early on; other user groups want only a second opinion.

On the other hand, some companies take the middle ground between little involvement and total control. One midwestern Fortune 100 company in the health-care field recently published a handbook for user departments considering a LAN. "We give them a methodology for determining whether they really need a LAN, to share information for example, or whether all they really need is another printer," said Julian Horwich, who is involved with LAN strategy at the company.

Some 50 to 60 user departments have requested the handbook, which also includes tips on LAN selection and installation, Horwich added.

The question of who controls the network will no doubt be debated for years, especially as more LANs are installed in corporate America.

"I don't know that DP has to take complete responsibility," said Ricca of Eastern Management. "But user departments may want to consult that group for advice the same way the company consults a lawyer. They would tap into the experience base to make sure no major mistakes are made."□



Courtesy: The Travelers Corp.

time you try to store something, someone else may have taken that bit of space. The two collide, and data may get lost."

Several LANs exist at various Drexel subsidiaries—from a Network Systems Corp. Hyberbus at the headquarters office to Ethernets in London and on the West Coast.

In Chicago, a Novell network is used to maintain pricing records for the company's expense information and other very sensitive data.

Those organizations which are extremely security-conscious are often reluctant to make public their security measures. "Talking about what we've done really defeats the purpose of having done it," noted Julian Horwich, who is involved with LAN strategy at a Fortune 100 company in the health care field.

His organization has several hundred LANs for transaction processing and office automation applications. The networks are mostly IBM Token-Rings, Novells and Ethernets.

The really secure LANs are those that are for transaction processing; encryption and passwords are used. "What is considered adequate security depends on the application, and whether the LAN is really local or whether it allows dial-in," Horwich said. "But in general, depending on the LAN, the built-in security is adequate."

In his role as executive director of the Chicago Association for Microcomputer Professionals (Camp), Horwich said, "LANs are less of a problem than minis or mainframes because most of them are really local. If the LAN does not communicate outside the workgroup, the issues are much less serious." He agreed that as LANs become more interconnected, security needs to be beefed up.

Many LANs are installed and managed by individual user departments and not corporate MIS. Until MIS steps in, the LANs often do not include what some experts consider to be truly adequate security measures.

By that time, however, the MIS concern is generally the physical and logical connection of the LANs that have proliferated around the company. So security gets short shrift.

SPECULATING ABOUT OS/2

Another issue is how well IBM's OS/2 LAN Manager will support additional security features.

Hibernia's Carender is not optimistic. "If it's as good as some other IBM products, it's going to be far behind the current Novell capability," he said.

"LANs under OS/2 is one of the major topics of discussion at Camp," Horwich said. "This will be the year many of us will try to understand the various strategies, and '89 and '90 will be when we implement."

Arthur Andersen's Perillo said, "Customers are talking about it, but they're not turning around tomorrow and installing it. Maybe a year from now they'll install it on one of their LAN servers and see how the software evolves." He said that in the long run, OS/2 and LAN Manager will have "a significant impact."

Bart Stuck, vice president of Probe Research Inc. in Cedar Knolls, N.J., said that over the years "network security will grow in importance." And the conundrum of providing easy access *vs.* security will ease somewhat with the new generation of OS/2 software that provide graphical user interfaces and improved directories.

"Directories are the fundamental issue," Stuck said. "Things must be completely transparent to the user, who shouldn't have to know where something resides. It could be three gateways away from the user and, if you have the appropriate access clearance, you can still get it."

He added that the industry's direction "is toward a host of directory services."

Stuck said, "In five years the PC LAN business will be the single largest segment of the data communications industry." Then, as now, security will be one of the most important issues in the minds of micro managers. ■