LANs pose risks and should be audited, but few auditors are technically equipped to do so.

Local Area Networks:

A Realistic Audit Approach

Dan Kinne

Managerial Auditing Journal, Vol. 9 No. 5, 1994, pp. 8-15

Introduction

Information system (IS) auditors today are facing an ever increasing array of areas requiting audit attention. Most of these involve new technologies in which the auditor is not an expert. At the same time, the resources necessary to provide adequate audit coverage (mostly human resources) are not forthcoming. Therefore, it is realistic to say that we must audit more with less and, at the same time, do it better than we ever have because of the increasing reliance our organizations are placing on these technologies.

I am an IS auditor in exactly this situation, since I am a one-man function and likely to remain as such but still have to broaden my scope of audit activities to cope with technological advances. One of the most interesting of these is the spectrum of the local area network (LAN). Like many others in our profession, I have no communications background, which further complicates matters.

I thought it might be useful to share some ideas in LAN control weaknesses and priorities and to discuss how we might realistically approach LAN audits given the constraints which exist.

Background and Environment

The purpose of this section is to present a minimum of LAN terminology and concepts which will help the auditor understand his or her specific environment.

Baseband versus Broadband

These terms relate to data transmission methods. With *baseband* a digital signal is applied directly to the transmission medium, while with *broadband* an analog signal is transmitted. This means that, with broadband, the data are *modulated* or changed from digital form to a radio frequency signal and back to digital at the receiving location. It is important to remember that, due to wider band width, broadband may be used for video as well as voice and data transmission. We also note that *network interface units* (NIUs) are significantly more expensive on broadband LANs because of the modulation which is necessary. Another important distinction is that a broadband cable may support simultaneous transmission on several channels, each operating at a different frequency. However, along with this increased flexibility comes the need for more sophisticated LAN management (i.e. more administrative overhead).

Topologies

The term *topology* really refers to a specific LAN concept or shape supported by a unique hardware/communication protocol. There are three major topologies which we will discuss briefly and a number of others which are less common and will not be discussed here. The three topologies to be discussed are Bus, Star and Ring.

Bus

This consists of a single backbone cable utilizing repeaters at consistent intervals to keep up the signal quality. Ethernet is the most common LAN implementation using this. Its advantages include ease of adding and removing users, high reliability (coaxial cable is usually the medium), and its ability to handle high transmission activity and contention. There are some disadvantages in that the cost of cabling can be high and that high transaction volumes may noticeably degrade performance. It is important to note that, with a Bus, each network device has access to all network traffic, which may pose a security risk.

Star

The Star is typified by each user being connected to, and all transmissions passing through, a central node. The most common application of this is the PBX (private branch exchange). It is similar to a telephone system. In fact one of its advantages is that cabling costs may be low since, in some cases, existing telephone cabling may be used. Other advantages include centralized control (ease of trouble shooting) and support of voice and data. It has the disadvantages of long cabling lengths (each user is cabled to the central node) and the fact that the failure of the central node disables the entire network.

Ring

The Ring is aptly named, since the main cabling forms a complete circle. There are a number of different im-

plementations of the Ring of which the IBM Token Ring is probably the best known. However, this is somewhat of a hybrid which we will touch briefly upon a little further on. This typology has the advantage of allowing high data transmission rates which are predictable, regardless of network trafffic. Also, unlike the Star, control is distributed. Troubleshooting may be difficult as there is no master terminal.

As already mentioned, the IBM Token Ring is a hybrid comprising a Ring topology but using a cabling technique similar to a Star. This provides fewer control points which simplifies identifying and correcting problems.

Cabling

There are three types of cable (sometimes referred to as media or transmission media) commonly used in LANs. They are twisted pair, coaxial cable, and fibre optics.

Twisted Pair

This is the most inexpensive medium, consisting physically of two tightly twisted wires as its name implies. It is most commonly used in PBX or telephone systems and can support voice and data transmission. It can also maintain a consistent signal quality over a relatively long distance without a *repeater* or amplification. However, this medium has a relatively low bandwidth or data transmission rate. Also transmission *noise* or interference may be somewhat greater than the other media creating the possibility of lower reliability. We should note as well that signal *emanations* or leakage may be slightly higher than other media which means that there is more of a possibility that a signal could be intercepted outside the medium itself. Cable shielding is very important here. Twisted pair is best suited for point-to-point networks such as a Ring rather than as a shared medium such as a Bus.

Coaxial Cable

Physically, this consists of a solid inner copper conductor surrounded by layers of shielding and an outer jacket. It is large, being about one centimeter in diameter. There are two basic types of cable — broadband and baseband. Broadband coax is standard CATV cable. Both types are very reliable and support much higher data rates than twisted pair. Repeaters are required at more frequent intervals than with the other media. It must be noted here that this medium is relatively easy to tap, making the location and security of the cable important. An additional disadvantage is that cable cost and installation can be considerably higher than the other media. As one might guess from the discussion of topologies, coax is used in Bus networks.

It should be mentioned here that there is a new cabling medium for baseband called *thinwire* which is, as its name implies, a thin version of coax. It has most of the advantages of traditional coax but is less expensive and easier to intall although physical connections may cause some LAN disruption.

Fibre Optics

This medium was more recently developed than the others and consists of hairlike glass strands with twine and paper cladding and an outer sheath. Laser technology is used to transmit digitized data by a system of varying light beams. It has many advantages over the other media induding extremely high data rates and reliability, the need for significantly fewer repeaters than the other media over a given distance, and ease of cabling due to the ability to carry enormous amounts of data on a very thin flexible cable. The major disadvantage of this medium for LANs is that, although the cable cost is relatively low, connection to network devices is difficult and costly. It is important to note here, however, without going into any detail, that the emerging FDDI standard (Fibre Distributed Data Interface) may not only solve this problem but will provide a LAN with vastly increased performance.

Software

Informatics or telematics hardware is little more than a hunk of metal (or plastic) without software to drive it and make it serve our functional requirements. This, then, is an area which becomes of special interest to us as auditors. Particularly so since LAN software lags behind the hardware capabilities. There is real power, but potential risk, in the new generation of OS/2 or Unix 386-based multitasking LANs. These can, at a relatively reasonable cost, provide the power of a minicomputer operation but may not have the software sophistication to control it as well as we might wish.

Depending on the particular LAN environment, there are generally three major aspects to the software. These are network management, the LAN operating system, and drivers. The PC-operating system is not considered as LAN software for purposes of this article although its use certainly comes into play.

Network Management Software

This is for use by the LAN administrator to configure, manage, and troubleshoot the network.

LAN Operating System

This, like any operating system, allows us to use and tailor the capabilities and resources of the LAN for our specific needs. It includes such things as defining file servers and print servers and is key in overall control and security. It must be noted that all, or parts of it, are generally resident on each individual PC or server in the network and may require, to a greater or lesser degree, each user to be responsible for access control and security. Increasingly, parts of this software are stored

on the LAN card, reducing the memory required on each PC node.

Drivers
This is low-level software (often vendor specific) which provides protocol conversion for LAN components using different communication protocols allowing transparent communication among these components.

File and Printer Servers

Alluded to earlier, these are PCs which provide file/data sharing or interface with one or more printers which can be shared by a number of users. PCs used as a server are generally dedicated to that purpose and not used concurrently for stand-alone processing, although the latter is possible with some operating systems. In any event, servers may be left unattended. Because of the concept of concentration of data in one place, sharing of a single resource and, consequently, more reliance being placed on one device, we, as auditors, must pay special attention to assessing the adequacy of controls over these.

LAN Control Priorities

This section aims to provide the auditor with an understanding of the major risk areas which an audit must cover. This assumes that a LAN has already been selected and installed and does not address audit involvement in the selection process. However, audit involvement in this phase is just as important as with any other system resource. The auditor should be involved in LAN acquisition and should ensure that management is actively involved and has sufficient comprehensible information to make their decision. This is too important in terms of investment and organizational impact to be left solely to technicians. It is important to have requirements stated functionally, not just at that particular point in time, but for the near-term future as well.

Management/Organization

As with most other areas these controls are fundamental to achieving and maintaining a successful LAN operation. The objective is to determine and assess the organizational structure of network management and control as well as the policy base supporting network use. This last aspect is particularly important as decentralized and powerful LAN resources may be in the hands of relatively unsophisticated users. Such policies are vital to the effective, controlled, and consistent use of the LAN and its resources. Again, this takes on even more importance with the emergence of the new multitasking LANs as their increased power and sophistication requires more management and administration. The auditor should look specifically at the following areas.

Information Policy (Existence and Content)
Information is an organizational asset of immeasurable value. There should be policies as to what information exists, what form it is in, and how it may be used.

Security Policy
This is an important subset of information policy. This specifies who is responsible for securing LAN data. It may also detail data ownership, classificafion of data for security purposes, and means of enforcement. One might look for such a policy to be broken down into data access security and transmission security.

Use and Planned Use of the LAN and Senior Management Involvement
A LAN should never be acquired just as a piece of interesting technology, but should support functional requirements from which a management plan has been formulated. Without such a plan, it is unlikely that effective (or cost effective) use of the LAN will ever be realized.

Network Management Organization
This includes separation of duties between LAN administration and applications developers. To the extent possible, the effectiveness of network management in supporting user needs, complying with management policies and maintaining a well-configured, reliable network should be determined.

Physical Security

Even though technology has advanced, many of the same basic physical control principles which auditors have been assessing for years still apply and, in fact, provide some of the most effective means of data security.

Access to Servers
As already stated, these devices pose more of a risk than stand-alone components because of the increased reliance an operation must place on them since they serve a number of users. Although LAN security software may limit access to data, there is often no such restriction for someone using the console of the server itself. Also, given access to a printer server, it is sometimes possible to monitor what is being printed or about to be printed by scanning the print buffer. Therefore, by simply restricting access to the server, these risks may be eliminated. This also minimizes the risk of theft or physical damage. If it is not possible to restrict access, it may be wise to remove and secure the keyboard as it is not necessary for the functioning of the server.

Backup and Recovery
This indudes procedures for servers as well as stand-alone PCs on the network. Ideally one should be able to use the resources of the LAN to facilitate this process through the use of a mass storage device connected to the network. In this way, data can be easily backed up at a

remote site. Otherwise, we should expect to find the types of backup procedures which are used in any good computing environment along with a written policy.

Cable Shielding
This may be important for highly secure environments since emanations of transmissions may occur and allow unauthorized reception and scanning of those transmissions.

Emergency Contingency Planning
In the event of the failure of the network, it is important to have a well-conceived strategy for continuance of operation as would be expected in any other area of information processing. We should note here that the type of LAN in use should be a factor in the type of contingency procedures and the emphasis they are given. For example, since the failure of a Star network can disable the entire network, more emphasis should be given to this area in this type of network environment.

Cable Access
We should also keep in mind the possibility of unauthorized tapping into the network. Of particular concern are coaxial cable and telephone or wiring closets. Controls should be in place or mechanisms used to prevent free access to these.

Data Access
The objective of data access controls is, of course, to limit an individual's access to only those LAN resources necessary for that person's function. This can be particularly difficult since LAN access controls tend to be rather decentralized although some of the new LAN operating systems do allow some centralized access control. Along with the capability to limit access effectively is the need to be able to ensure that security policies/procedures are being adhered to. In other words, LAN security should be auditable and verifiable, a weakness in some LAN operating systems. Again, servers deserve priority. Following are some areas of concern to auditors in assessing the effectiveness of access controls:

Limitation of Access to the LAN Itself
There should be some mechanism, such as password control, limiting access to the LAN only to authorized persons or devices. Ideally, this should be centralized and monitored and maintained by a data security officer.

Limitation of Access to Specific LAN Resources
Again, it is preferable to have central control of this. Unfortunately, some LAN operating systems rely completely on each user to establish access controls. This leaves implementation of access control to many, some of whom may not be aware of potential risks. It also makes it virtually impossible to audit if there are more than just a few users on the network. Another important consideration is the security defaults of the system, as several LAN operating systems have, as their default, no security. In these cases overt action by the user is required to establish access control.

Access Logging
There is little capability in older LAN operating systems for monitoring access violations, as this information simply is not available. In some newer operating systems this capability does exist. In this case there should be a regular review by the data security officer.

User Access Profile
Where some sort of centralized access control is in effect there should be an authorization procedure for establishing and modifying these profiles outside the total control of technical personnel.

Password Control
As usual, passwords should be changed on a regular basis and should be in encrypted form on file media. It should be possible for users to change their own passwords.

Dial-in-Capabilities
Unless absolutely required this capability should not exist. If it does exist there should be some sort of authorization control such as a callback control. Naturally, password/user code control should be in place.

Uploading Data to Other Host Computers
This should require filtering by the host computer application's own validating/update routines.

Access to File Servers
Ideally, it should be possible to control this access to the file level. If the data on the server are critical, consider putting it on a stand-alone unit or configuring a separate restricted network. In some installations the locations and network addresses of servers, as well as all other network components, are public information. This should be prohibited as it can increase the probability of unauthorized access.

Access to Printer Servers
These should be password or otherwise protected since, mentioned earlier, print buffers can sometimes be read.

Designation of a PC as a Server
It should be determined if this is under user control or centrally controlled. In either case, keep in mind that, depending on the LAN operating system used, it may be possible to save a particular LAN configuration – meaning that when the PC is booted it can automatically come up as a server. This capability should be used with caution as sometimes users forget that others can access their data.

File Encryption
Consideration should be given to scrambling or encrypting sensitive data while it is stored on file media. Sometimes system designers go to great lengths to encrypt data during transmission but leave it decrypted in its stored form making it vulnerable to unauthorized access.

LANs Connected via Gateways
It is increasingly common to see LAN configurations consisting of a number of smaller networks (e.g. Token Ring) linked together by what is termed a gateway. In designing LAN security it is as important to have a mechanism for controlling access to other networks through these gateways as it is to control access to the resources of one LAN.

LAN Components Active when Not in Use
There should be time-out controls for active PCs or workstations, just as one would expect in a stand-alone computing environment. However, with a LAN, the result of not having such a control is potentially more damaging due to the increased number of components and access points in a network.

Viruses
No discussion of access controls would be complete without at least some mention of virus protection. The LAN has geometrically increased the adverse effect of a virus being introduced into a system. Within minutes the virus can run rampant throughout the network. It can take weeks to determine and correct the damage. There should be an organizational policy addressing the issues and software tools available to all users to detect and eliminate known viruses. However, the most effective control is user awareness and caution.

Transmission Security

This type of data security is important in highly secure environments. The most common application of it is, of course, data encryption at the source of the transmission and decryption at the receiving location. We will not go into any detail here in discussing various techniques and procedures. However, consideration should be given to the following points:

Encryption Algorithm
If the data transmitted through the network are sensitive enough to justify encryption, it is worth using a secure algorithm such as DES rather than something which may be easily broken.

File Encryption
It is reiterated here that security may be diminished if we go to the trouble of encrypting data during transmission but leave it stored in decrypted form.

Key Management
Of course, secure data encryption implies good key management techniques as this is really the basis of it. An organization must be prepared to put forth the human and administrative resources necessary to accomplish this. It is not difficult to see that data encryption requires a good deal of administrative overhead as well as expense. It might be more cost effective, as mentioned earlier, to use stand-alone systems or configure a small restricted access network to handle sensitive data.

LAN Administration and Support

This function is of great importance but entails significant access authority such as a systems programmer. The LAN administrator is responsible for establishing and maintaining the network configuration(s), managing network activities on a day-to-day basis, troubleshooting problems, and generally supporting user needs. The need for such a powerful function is indisputable, but specific duties and responsibilities should be assigned with internal control in mind.

Nature of LAN Administration
The auditor should understand fully how this function is structured in the specific environment under review. The type of LAN and the LAN software in use will have a lot to do with how the function is structured and what degree of access to system resources may be obtained. That is also the determining factor in how effective the administrator can be in managing the network. Generally, a dedicated function is preferable from a separation of duties point of view. There may be a number of people involved at different organizational levels which may mean a number of people with wide-ranging access authority.

Access Authority
It may be that the LAN administrator has access to all system components and data. Determination must be made as to whether or not such access is really necessary and, more importantly, if it is possible to restrict such access without hindering the work. Also note that it is wise to establish a separation of duties between LAN administration and security.

LAN Management Software
As auditors we would like to see this software capable of monitoring and recording network activity including that of the administrator. This is what provides LAN auditability. It is also wise to have such activity reviewed by an independent person such as the security officer.

Policies Governing Access to File Servers
There may well be a valid need for the LAN administrator to have access to file servers in certain circumstances. These, however, should be subject to management policy decisions and should require the knowledge and/or compliance of the responsible user.

LAN Software Updates
This is an important aspect of the function but it can be cumbersome and even dangerous since certain LAN software resides on each user machine. It is better, both

from an efficiency and a control standpoint, if the user has read access to an administration server in order to download changes than for the LAN administrator to have open access to each user system for making these modifications.

LAN Reliability
The auditor may wish to make some assessment of LAN reliability. The LAN management software should provide the basis for such an analysis.

Applications

If we view applications as data or information, then the criticality of that data is what determines the degree of control and reliability the LAN must possess. In auditing the LAN, try as we might, we cannot separate it from the applications it supports. We must also keep in mind that these applications become more complex due to the multi-user nature of most of them. Important elements in assessing LAN applications are as follows:

Understanding the Application
This understanding must primarily be from the standpoint of the criticality/sensitivity of the data processed and the LAN resources utilized.

Multi-user Processing
If the application is multi-user, as it is likely to be, then special emphasis must be placed on controls to prevent simultaneous updating, backup and recovery, and security over access to the server. We should note that some newer operating systems have such capabilities, allowing the creation of duplicate data on another file or even another disk, and can provide data recovery techniques much as we would expect on mini or mainframe systems.

Application Development Maintenance
The nature of LANs lends itself to end-user system development. This is beneficial in that we are able to put the power of the computer directly into the hands of those who need its services. However, as auditors, we must be concerned by the fact that many of these users will not be technically sophisticated and this may lead to control weaknesses within the application. In any event we should ensure that there are strong installation standards with which we can measure compliance.

Copyright Violations
This is a sensitive and somewhat controversial area into which many auditors have been reluctant to delve. However, it does pose an exposure to our organizations and, as such, is something with which we must come to grips. This is particularly true in a LAN environment which compounds the exposure.

Involvement of the LAN Administrator
It is important to involve the LAN administrator in the development of major applications from the standpoint of any necessary reconfiguration or, simply, network traffic. However, the person in this function should, in no way, be responsible for the application. In other words, there should be involvement, but not too much.

Realistic Approach to the Audit

This section will not provide a comprehensive audit programme, as each audit environment is too specific for that. Instead, some suggestions and a general framework for the audit will be presented. These are intended to provide guidance in how to approach this area given the resource constraints which exist. In other words, we must find a way to do a meaningful audit of an area in a two-three week period or even less, that, in many organizations, would require the full-time attention of a technically qualified auditor to provide proper audit coverage.

We might consider the audit of the LAN as an additional complication of application auditing, much the same as with the advent of the database management system. In fact, that is probably a good analogy since LANs, like databases, have application-specific as well as general considerations. They are also similar, since they both have tended to modularize our information system structure further. Consequently, we are faced with a paradox of a partial audit not being meaningful but a comprehensive audit being impossible. The realistic auditor will immediately realize that 100 per cent coverage is not possible. What percentage of effective coverage is eventually achieved largely depends on the auditor and the approach used.

In general, the most viable approach is based on understanding the component parts of a LAN control structure – what is important and what is not – and prioritizing the areas which are important. Knowing this, we break down our audit accordingly and use the most time-efficient procedures possible to test these areas. What this approach sacrifices is time, in the sense that effective LAN coverage is attained over an indefinite period of time as opposed to one point in time.

Organizing the Audit

We must first understand the LAN environment we are in. This includes the nature of the LAN(s), number and location of users, applications processed, and the relative sensitivity of the information processed. This is necessary in order to prioritize or "layer" the audit. Once a priority breakdown is made, we must differentiate between LAN-wide and application-specific aspects. A general priority guideline is to focus first on the LAN-wide considerations, emphasizing policy and management considerations as well as at least one (probably the most critical) application. The application

part of the audit can be prioritized as well. To be more specific, we should consider the following in organizing the audit:

(1) Analyse the criticality or risk of the application(s) being processed via the LAN to be able to set audit scope. As mentioned earlier, it is the criticality of the information processed through the network which, in large part, determines the type and importance of the control structure. Also assess the size of the LAN operation, in terms of numbers of nodes, and users, by functional area, as well as how the LAN is used since this has a bearing on priorities.

(2) With the audit requirements analysis completed the scope of the audit must be set. As with any audit, this is critical. It may be that the operation is too big to approach at one time. Therefore, consideration could be given to splitting up the audit. One suggestion here is to use a layered approach whereby one covers the basic general (usually the most important) controls first, using the most critical application to dictate the level of controls which should be present. Later one would go to the next layer which would be to look at a more specific functional or application level whose specific controls depend on the first layer's general capabilities.

(3) Do not try to go any deeper than your technical expertise will take you. You will learn as you audit. This is another reason for using the layered approach. Also non-technical areas such as the management area tend to be the most important anyway and the area on which everything else depends. There is also the point that, as the auditor, the auditee has to satisfy you, not vice versa. Therefore, do not be intimidated by technical jargon. Make the technician explain in terms you understand.

(4) Although this article assumes the existence of a LAN, it cannot be overemphasized that the audit should get involved as early as possible in the acquisition and installation of the LAN. This is when critical decisions are made, policies decided, and when costly errors can be avoided. (It is also a great time to learn about the network before anything critical is being done with it.) Particular emphasis should be placed on proper requirements analysis and senior management involvement in the process. It is often wise to recommend outside technical input to the decision. These are all steps designed to prevent purchasing an unsuitable LAN.

(5) Make sure that you have your own independent access to the LAN. This is vital as one must work with the network to really understand its intricacies. Also it opens up direct, effective audit testing which can be done from your office.

Breakdown of the Audit

At the same time that the LAN universe in a given organization is being analysed, and the audit scope of it set, it is necessary to establish an appropriate audit breakdown. Fortunately, the breakdown of control areas, as discussed under LAN Control Priorities, fits very nicely. However, to indicate relative priority, they are displayed in a different sequence as follows:

(1) Application(s).

(2) Management/Organization.

(3) Physical security.

(4) Access security.

(5) Transmission security.

(6) LAN administration/support.

It must be quickly pointed out that this priority sequence may change somewhat depending on the nature of LAN usage. Also, several may be considered of equal priority. The sequence is shown simply to provide a starting point.

Audit Procedures and Priorities to Consider

A few points are mentioned here for the purpose of providing some suggestions as to procedures which can provide more coverage with less time and effort and can help get at the key areas:

(1) Send out a questionnaire to all users of the LAN asking them to respond as to the extent and nature of their LAN usage, network reliability, controls in effect, and planned network use. This approach can be effective in communicating indirectly the type of controls which audit expects and can lead to user self-improvement in controls. In other words, this can serve as an extension of direct audit contact or presence.

(2) Test controls yourself. Try to access various servers to find out in practice what you can and cannot do. This type of direct audit testing is effective, educational, can be done on a regular basis, and can be performed from your own office. However, it is wise to inform management that such testing may occur in case access to sensitive data is gained.

(3) Spend time talking to the LAN administrator and request any activity reports which may exist for purposes of review and verification of access capabilities.

(4) Emphasize policy formulation and senior management involvement in LAN activities as the first priority.

(5) Verify physical security by simply touring the installation and observing the ease with which one

can gain access to LAN resources, particularly file and printer servers.

(6) Emphasize the importance of centralized access control and backup capabilities.

(7) Check for bulletin boards or other generally available information which may unnecessarily give away the location and identity of important LAN resources such as file servers.

(8) Consider establishing some regular ongoing procedures such as periodic review of LAN administration logs, security profiles of a particular server, or a physical inspection of a user unit's LAN operation and resources. These can be simply and quickly done but serve to maintain an audit presence.

Summary

Management and the IS audit profession are less and less able to afford the luxury of technical specialists to audit specific areas. Economic reality is forcing the audit profession in general, as well as the IS auditor, to become more generalist in nature. At the same time we have a broader scope of activities to cover. The result of this is that we must find more efficient ways to audit and we must find ways of assessing areas in which we may not be technically competent.

The answer to this problem lies in determining and focusing our attention on the *real* priorities, eliminating items of secondary importance as well as encouraging senior management to insist on strong organizational policies and procedures.

Further Reading

Cole, G., "Implementing Local Area Networks", *Course Materials from the Learning Tree*, Integrated Computer Systems, Culver City, CA, 1986.

Derfler, F.J. Jr and Thompson, M.K., "LAN Operating Systems: The Power behind the Server", *PC Magazine*, 29 May 1990, p. 109.

Dickinson, J., "The Super Servers", *PC Magazine*, 29 May 1990, p . 227.

Gaston, S.J., *Managing and Controlling Small Computer Systems Including LANs*, Canadian Institute of Chartered Accountants, 1992.

Krumrey, A., "LAN Security", *PC Tech Journal*, January 1988, pp. 96-106.

Leghart, P.M., *Emerging PC LAN Technologies*, Computer Technology Research Corp., January 1990.

Reynolds, G.W., *Introduction to Business Telecommunications*, Charles E. Merrill Publishing, Columbus, OH, 1984.

Schweitzer, J.A., "Securing Information on a Network of Computers", *Edpacs*, Vol. XV No. 1, July 1987, pp. 1-8.

Sobol, M.I., "Audit Concerns with Local Area Networks", *Edpacs*, Vol. XIV No. 12, June 1987, pp. 6-9.

The, L., "Can LANs Beat Minis?", *PC Magazine*, 29 May 1990, p. 195.

Dan Kinne is an Information Systems Auditor working for a large international organization and performing a full range of IS audits worldwide.