Planning for the Security of Local Area Networks

Lorne A. Dear
Frederick Gallegos

PAYOFF IDEA. Many organizations rely on vendors to provide network security; others add security measures after their networks are installed. Neither approach effectively controls network data security. Instead, organizations should plan for network security while planning the network itself. This article explores how security planning fits into the network development process.

PROBLEMS ADDRESSED

Private and public organizations are installing local area networks (LANs) to realize the production and cost benefits they provide. Many of these LANs however, are not adequately secured. Most vendors put little effort into security, concentrating instead on rapid throughput, high expandability, and other DP capabilities, and few organizations take the time to adequately secure their networks before installing them. As a result, critical data is jeopardized.

This article provides a plan for securing network data. Figure 1 presents the eight steps of this plan; this article concentrates on the first four steps and briefly describes the remaining four.

INITIAL NETWORK STUDY

The first step is to conduct a study of network needs and market offerings. Any such study, regardless of its breadth or complexity, requires:

- The establishment of a planning team
- Senior management support
- Recognition of the need for security planning
- Survey of capabilities of available LANs

To ensure acceptance of the network, the planning team should include representatives from every group that will be affected by the LAN—future users, management, the information resource manager, and system analysts. Outside

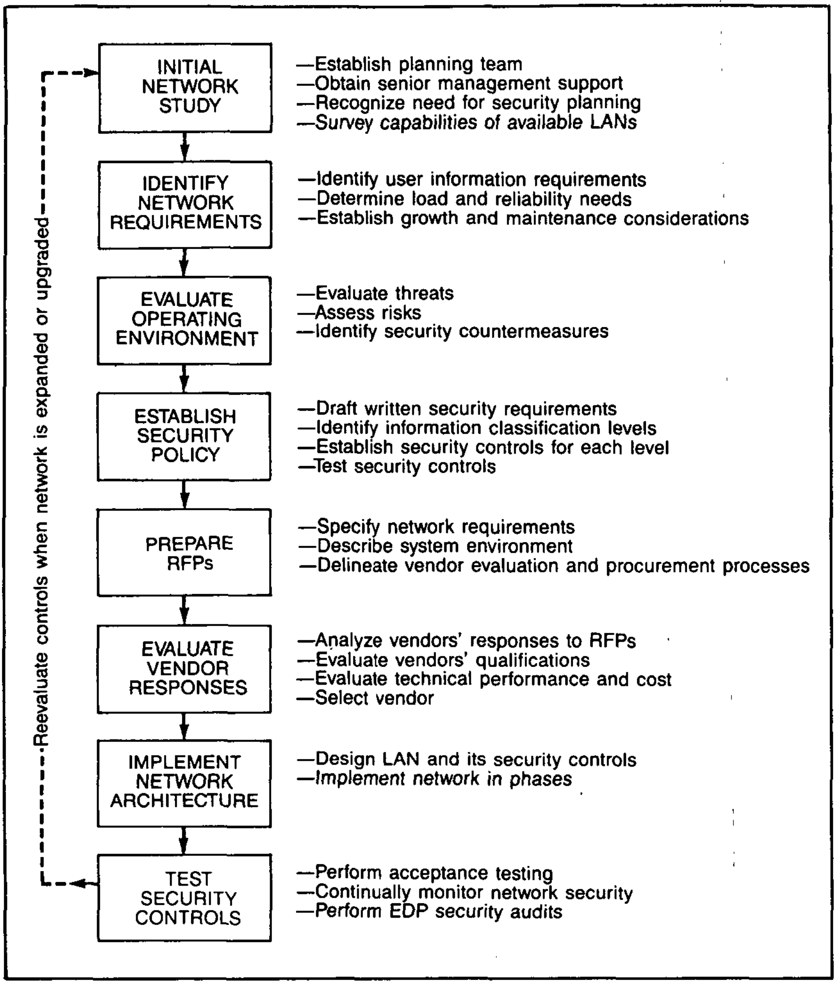
INITIAL NETWORK STUDY
—Establish planning team
—Obtain senior management support
—Recognize need for security planning
—Survey capabilities of available LANs
IDENTIFY NETWORK REQUIREMENTS
—Identify user information requirements
—Determine load and reliability needs
—Establish growth and maintenance considerations
EVALUATE OPERATING ENVIRONMENT
—Evaluate threats
—Assess risks
—Identify security countermeasures
ESTABLISH SECURITY POLICY
—Draft written security requirements
—Identify information classification levels
—Establish security controls for each level
—Test security controls
PREPARE RFPs
—Specify network requirements
—Describe system environment
—Delineate vendor evaluation and procurement processes
EVALUATE VENDOR RESPONSES
—Analyze vendors' responses to RFPs
—Evaluate vendors' qualifications
—Evaluate technical performance and cost
—Select vendor
IMPLEMENT NETWORK ARCHITECTURE
—Design LAN and its security controls
—Implement network in phases
TEST SECURITY CONTROLS
—Perform acceptance testing
—Continually monitor network security
—Perform EDP security audits
Reevaluate controls when network is expanded or upgraded

Figure 1. Security Planning Model

consultants should be included as needed. The team's goals should be established in writing and approved by senior management.

Senior management support is critical for the network's development. A management representative should serve on the network team—not necessarily as a chairperson, but as an equal member, offering management's perspective and, more important, informing management of the team's decisions. To hasten network development, management should approve the team's reports or recommendations, as quickly as possible.

Senior management and the planning team should plan for LAN security from the outset. When a team plans for security as it develops the network, it can secure each network component; adding security to a system after development is more costly and rarely successful.

The planning team should conduct a survey of commercially available LANs, concentrating on the following four areas:

- Applications and services—The types of information that can be processed and the transmission, storage, and processing of this information
- Topology—The manner in which the switching nodes, peripherals, and transmission links are connected (e.g., star, ring, bus, and mesh networks)
- Protocol architecture—Which of the seven layers of the International Standards Organization (ISO) protocol model are included
- Transmission medium—The physical connection between the network nodes (e.g., twisted-pair wire, baseband and broadband coaxial cable, optical fiber, microwave)

The results of this survey provide a context for developing and evaluating the organization's network and security requirements.

IDENTIFICATION OF NETWORK REQUIREMENTS

Having learned the capabilities of available networks, the planning team must next determine the organization's network needs. These needs can be divided into:

- Information requirements
- Network load and reliability needs
- Growth and maintenance considerations

Information requirements include network applications, services, and specifications. The team can determine applications needs by reviewing the functions that will be performed on the LAN and the equipment that is currently used to perform them and by asking users what additional functions they need the LAN to perform. In addition, the team must determine what network services are needed (e.g., electronic mail, teleconferencing) and what physical requirements (e.g., space and placement of equipment) are necessary to accommodate them. The team must also determine requirements for response times, interfaces (e.g., input and output characteristics), types of transmitted information (e.g., data, video, voice), and support equipment (e.g., terminals, printers, file storage units).

Load and reliability requirements must be established. Traffic volume and data arrival rates determine many aspects of network design. The team must establish network throughput requirements and tolerable delays (for transmission and protocol processing) and plan for connectivity between nodes (e.g., by designing data flow diagrams of traffic, query and response procedures, and message streaming). The team must also determine which network elements to back up and establish acceptable file transfer error rates and the acceptable number and duration of node failures.

Network growth and maintenance requirements also affect planning. The team must establish requirements for network capacity and protocol architecture so that the network can support additional nodes, new applications, and different types of traffic (e.g., voice or image). Maintenance must be planned for because its costs often exceed those of the network itself. The team may decide to purchase network monitoring equipment and stipulate that hardware and software meet industry standards so that replacements can be bought off the shelf.

While identifying network requirements, the planning team should also consider network security and privacy needs. Observations on these needs form the basis for the next stage of network development.

EVALUATION OF THE OPERATING ENVIRONMENT

During this stage, the planning team evaluates potential security and privacy risks in the operating environment. Networks pose more risks than centralized computer systems because of the telecommunications links that connect the nodes. Therefore, the physical security, access controls, and other measures used to secure centralized computer systems should be applied to networks, along with additional communications security measures.

To select the necessary network security measures, the planning team should:

- Evaluate potential threats in the network environment
- Perform a risk assessment
- Choose appropriate security measures.

Threat Evaluation

The planning team must identify the individuals and the environmental factors that could threaten the network and the ways in which the network could be compromised. Threats can arise from authorized users, unauthorized users, or the environment.

The five ways in which authorized and unauthorized users can threaten the network are shown in Figure 2. The first two—release of message content and traffic analysis—are passive methods of network attack. In a passive attack, an intruder learns about the network's traffic flow by observing the length, frequency, and source or destination of messages as they flow along the network.

The last three methods are active attacks, in which the intruder attempts to

Potential Threats	Mode	Detectable?	Countermeasures
Release of message content	Passive	No	Encryption, node protection
Traffic analysis	Passive	No	Encryption, masking frequency and length and origin/destination patterns
Message stream modification	Active	Yes	Encryption, communications protocol for reliability
Denial of message service	Active	Yes	Request and response protocols
Initiation of an unauthorized connection	Active	Yes	Encryption key management

Figure 2. Potential Threats of Authorized and Unauthorized Users

modify, duplicate, or alter messages, delete or delay messages, gain access to network nodes without proper identification, or violate time-integrity checks on network equipment.

Environmental threats must also be evaluated, especially when network telecommunications links extend outdoors.

Risk Assessment

To perform risk assessment, the team should rank security threats according to their potential effects and their probability of occurrence. A detailed description of risk assessment is beyond the scope of this article (other articles in *Data Security Management* address this subject). The planning team, however, should carry out a detailed risk assessment and, based on the relative weight of each threat, determine which risks are unacceptable. For these threats, security countermeasures must be implemented.

Identification of Security Countermeasures

This article does not address the physical and administrative controls of network nodes. These controls resemble those used to secure centralized computer systems and include controls for personnel screening, area or terminal access, and protection against fire, theft, and destruction of media. Instead, this article discusses internal measures necessary to control network telecommunications links.

One of the greatest threats is unauthorized network access between nodes. Data or protoçol controls should be encrypted to offset this threat (see Figure 2). No standards exist, however, for the placement of such countermeasures. The ISO has developed a model with seven layers of communications protocols, shown in Figure 3. The ISO does not recommend any security methods but suggests that encryption take place at layer 6 (i.e., the presentation layer) and states that encryption could also occur at layer 3 (network) or 4 (transport). It also acknowledges that additional security controls could be placed at layer 2 (data link).

Similarly, the National Bureau of Standards (NBS) developed the Data Encryption Standard for use on selected applications by federal agencies, has not recommended any security control requirements for the various protocol layers. Although it has not identified which ISO protocol layers should be used for encryption, it has suggested, that layer 2, 3, 4, or 6 or any combination of these could be used.

Despite the lack of standards, significant security control could be placed in each layer. The following paragraphs briefly describe security at each of the four layers discussed by ISO and NBS.

Layer 6 (Presentation). At the presentation layer; data is transformed for end use. For example, instructions in this layer can interpret the meaning of exchanged data, oversee data entry and display, or control data structure. Because of its interpretive and data control features, the presentation layer can be an appropriate place to include security controls—for example, controls over what data can be interpreted or displayed can be built in so that only designated users can retrieve data.

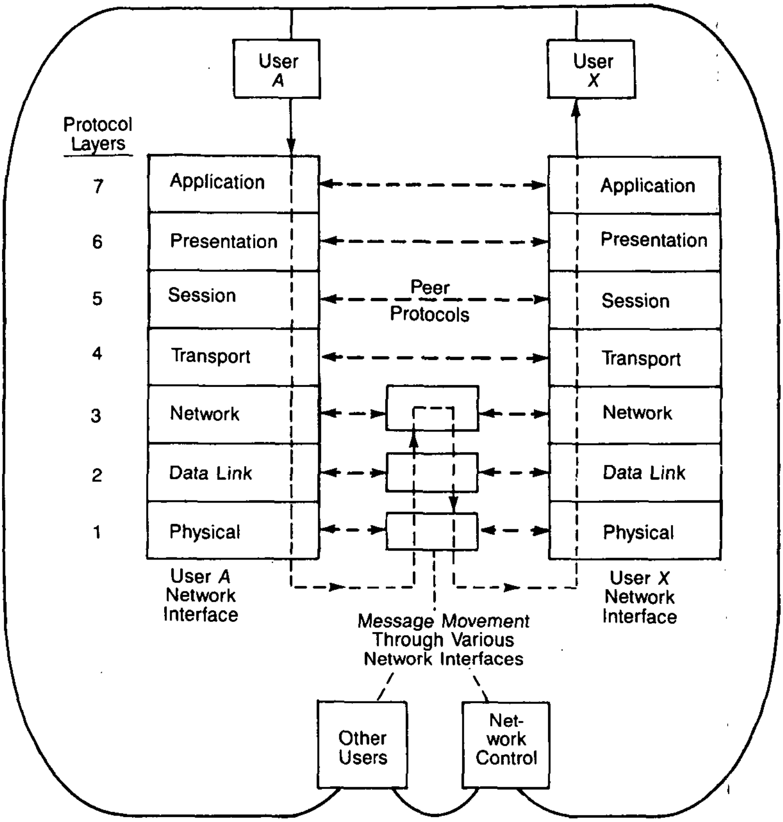

Figure 3. ISO Model for Software Protocols in LANs

Layer 4 (Transport). The transport layer provides end-to-end transportation of messages from one network node to another. Instructions at this layer break down a message into packets and address and forward these packets to the receiving node, where the packets are acknowledged and reassembled into the original message. The transport layer may be the best layer for security measures because the message can be protected from source to destination. At this layer, access controls can authorize or deny connections according to security constraints. In addition, accounting controls can maintain a record of transactions. Encryption and decryption can protect the message and the addresses of the sender and receiver. Finally, when messages are acknowledged, the security level of the receiver can be verified.

Layer 3 (Network). This layer controls packet routing and switching within the network and to and from other networks. Controls over network connections, logical channels, segmenting and sequencing, and data flow can be placed in this layer. Additional security controls can be added later.

Layer 2 (Data Link). This layer provides node-to-node (or link-to-link) control of the data flowing across the circuit. Approximately 70 percent of all error handling occurs in this layer. Data transfers are controlled by frame sequencing, flow synchronization, abnormal condition recovery, or identification exchange. Encryption can be used to protect the message as it flows between network nodes by decrypting messages when they are received and reencrypting them before they are sent to the next node. Multiple-node encryption and decryption hides the source and destination of messages as well as the messages themselves; however, successful access to any node could allow an unauthorized user to read messages traveling to that node.

Additional Security Controls. Other countermeasures can be employed to further secure network data. Messages can be broken into individual packets and sent over several communications lines so that the compromise or loss of any one packet will not necessarily jeopardize the entire message. In addition, using frequency-division multiplexing to send these packets ensures that someone monitoring one frequency cannot pick up the entire message. Combining these two methods, with or without encryption, can provide an exceptionally high level of security.

If the planning team chooses to use data encryption, it should also use key management to prevent unauthorized users from gaining and maintaining access to a link. Key management involves the use of cryptographic keys maintained on a separate microcomputer tied to the network; users are approved for keys by request. For example, senders can request the microcomputer to verify that the intended receiver is authorized to receive data and then establish a connection between the two nodes. This connection lasts only as long as the message.

ESTABLISHMENT OF A SECURITY POLICY

After the planning team identifies and evaluates network security requirements, the team should put its recommendations into writing. A network security policy based on an analysis of security threats, risks, and countermeasures can help clarify the organization's security goals to users and to potential vendors. Three steps to establishing a sound network security policy include:

- Clearly stating network security requirements
- Identifying the various levels of information processing and security controls for each
- Testing controls

Written security requirements must specify which objects (e.g., nodes, files) can be accessed by which subjects (i.e., users or nodes). Every object must have an access control label that identifies its security class and method of access. Subjects must be identified and authorized for specific access methods; accesses should be recorded and maintained for audit. The hardware and software that perform security control functions should be able to be evaluated independently, and all security control functions should be protected from tampering or unauthorized change.

Written security requirements should also define all levels of information classification (e.g., unclassified, internal use only, or confidential) and identify the security controls required for each level.

After security requirements and the controls for the various classification levels have been identified, an implementation scheme should be prepared and tested for feasibility. The control methods should be checked for redundancy and uncontrolled areas. Modeling software may be of assistance.

PREPARATION OF REQUESTS FOR PROPOSALS

After the security policy passes its tests, requests for proposals (RFP) can be developed. These documents should specify network requirements in terms of services, traffic, reliability, growth, and maintainability. Performance specifications should be stated in measurable terms (e.g., mean time between failure, percentage availability of node equipment). A clear description of the system environment should be included that details how the LAN will be configured, what it will do, and how it will fit into the organization. For internal use, the team should delineate how vendor responses will be ranked and the procurement process that will be followed.

EVALUATION OF VENDOR RESPONSES

Once the planning team receives the vendor bids, it must evaluate them. The team can be broken into smaller groups to ensure objectivity, and additional personnel (e.g., technical experts) can be added to some groups. The groups should conduct a quantitative analysis of each vendor's ability to meet stated requirements, weighing results according to the relative importance of each requirement. The groups should also evaluate the vendor's experience and reputation for dependability. Finally, a technical performance and cost evaluation should be performed. The planning team may also decide to perform benchmark testing on proposed LANs to test security controls, among other functions.

IMPLEMENTATION OF NETWORK ARCHITECTURE

During this stage, the LAN is designed and implemented. The planning team should review vendor progress, paying particular attention to security controls. The team may wish to ask EDP auditors to review available documentation and compare it with the existing system; such a review should continue throughout implementation. Implementation should occur in phases so that control can be exercised and users can grow accustomed to the new system.

TESTING OF SECURITY CONTROLS

Security controls at all levels should be tested before the system is accepted; after the network passes these tests and is accepted, it should be regularly monitored. When the network is expanded or upgraded, security must be reevaluated; some or all of the steps involved in designing an LAN may need to be retraced.

RECOMMENDED COURSE OF ACTION

Security measures should be built into a network as it is developed. The organization must establish a planning team to identify network requirements, establish a security policy, prepare RFPs and evaluate vendor responses, implement the network, and test its security controls. After the network is installed, the organization must continually monitor network security controls. If the network is expanded or upgraded, the organization should retrace the steps in this article to reevaluate network needs and establish expanded security controls.

Lorne A. Dear is a program manager in the Information Technology Division of the Air Force Audit Agency, where he researches Air Force information system policies and programs, manages several audit managers who conduct Air Force–wide information systems audits, and acts as a liaison to senior Air Force officials. Dear has an MBA in EDP auditing from the California State Polytechnic University, Pomona.

Frederick Gallegos, CISA, CDE, is an auditor for the U.S. General Accounting Office, Los Angeles, and a lecturer for the computer information systems department of California State Polytechnic University, Pomona.

Recommended Reading

Allen, B. "Role of Access Layers in Local Area Networks and Factors for Consideration." *Communications News* 19 (September 1982): 110–111.

Becker, H. B. "Data Network Security: Everyone's Problem." *Data Communications* 9 (September 1980): 60–72.

———. *Functional Analysis of Information Networks: A Structural Approach to the Data Communications Environment.* Melbourne FL: Krieger Publishing, 1973.

Conrad, J. W. "Outlook on Local Area Networks." *Data Processing Management* (September 1982): report 6-02-06.

Denning, D. E. "Secure Personal Computing in an Insecure Network." *Communications of the Association for Computing Machinery* 22 (August 1979): 576–82.

Denning, D. E., and Denning, P. J. "Data Security." *Data Processing Management* (May 1980): report 1-03-09.

Edwards, R. W. "State-of-the-Art Developments in Software, Hardware, and Telecommunications Security." *Data Processing Management* (November 1983): report 1-03-13.

Gasser, M., and Sinder, D. P. "A Multilevel Secure Local Area Network." *Proceedings of the 1982 IEEE Computer Society Symposium on Security and Privacy.* Los Angeles, 1982.

Klein, M. H. *Trusted Computer System Evaluation Criteria.* Department of Defense Computer Security Office, 1983.

Martin, J. *Security, Accuracy, and Privacy in Computer Systems.* Englewood Cliffs NJ: Prentice-Hall, 1973.

Turn, R. *Advances in Computer Systems Security.* Dedham MA: Artech House, 1981.