Payoff

Businesses that rely on a value-added network to provide information processing and communications services are only as secure as the network itself. The customer should understand the types of processing and control services provided by such vendors, and the potential exposures that use of these networks can entail. This article describes the control issues that must be addressed, the controls required to ensure adequate security, and an approach for assessing the security of value-added networks. The article also discusses the pros and cons of using service auditor reports to assist in evaluating the adequacy of controls.

Introduction

Two distinct and seemingly contradictory trends are apparent in the management of American enterprises in the 1990s. Businesses are becoming increasingly dependent on communications as they distribute their information processing, relocates business operations, and interact directly with suppliers, customers, and competitors. At the same time, these organizations are turning their information processing and communications activities over to servicing companies, a process called outsourcing.

Companies operating computers for others are known as service bureaus. Private companies, the common carrier, have operated communications systems on behalf of others for a century or more; the telephone companies are the best example. Certain vendors of communications services combine the message transmission of the common carriers with the specialized processing of the service bureaus. These are known as value-added networks (VANs).

Control-Related Van Services

VANs offer a number of control-related services that can enhance communications security. These are described in the following paragraphs.

Packet Switching

By breaking long messages into shorter segments, or packets, and sending them over diverse routes within a network, greater advantage can be taken of network availability and diversity. Of course, the network must have the ability to reassemble the packets at the intended destination to reconstitute the original message.

User Identification

Access to and use of VANs should be limited to authorized users. Many VANs offer the capability to restrict the ability to send or receive messages to specific individuals, who must thus be uniquely identified to the network.

Message Authentication

In such applications as money transfer or Electronic Data Interchange, it is essential that messages be correctly transmitted and sent to the intended recipient. This may be ensured by authentication, the process of passing the message, as data, through an algorithm, to produce a result. The result is appended to the message, and the authenticating process is repeated by the recipient. If the two results match, the message is intact and the sender is correctly identified.
Encryption
Encryption is much like authentication, except that the result of the algorithm replaces the message text, instead of being appended to it. This process provides confidentiality of the message as well as integrity. Encryption may be thought of as value-added authentication.

Store-and-Forward Mechanisms
Because communications networks are built of physical components—cables, fibers, satellites, switches—they are subject to failure. Any messages in transit during the failure would be lost. To ensure delivery, many networks store messages in a static device, such as a computer, and then forward them to the recipient. Thus, if the network is interrupted, the message can be redelivered.

Diverse Routing
As further protection against loss of messages, networks are built with multiple, diverse paths for the messages to follow. If there should be a physical breakdown anywhere in the network, messages can follow alternative paths and the network can arrange for bypassing and repairing the network breach.

Application Processing
Such applications as Electronic Document Interchange and electronic mail are carried out as adjuncts to network communications. The VANs often provide these services to their customers.

The Van Perspective on Security
A VAN provides many services that are directly involved in the day-to-day processes of the companies that acquire its services. To that extent, the security of the VAN is a part of the overall security of the customer organization. And yet, the security of the VAN is, for all practical purposes, beyond the customers' control. The security afforded to the customer is no greater than that which the vendor builds for its own purposes or that the customer is willing to pay for expressly.

From the perspective of the VAN vendors, there are three ways to view their responsibility for providing security; as:

- **Operators of a business.** The VANs have a considerable investment in their networks and information processing services. As would any prudent business person, the managers of the VANs must take precautions to protect their assets and the viability of their businesses.

- **Holders and processors of customer information.** As the holders of others' information, the VANs must be able to protect that information while in their possession. This is not only ethics, it is hard-nosed business sense. The managers of all VANs realize that if the confidentiality and integrity of messages transmitted over their facilities are not assured, they will soon enough have no messages to protect at all.

- **Providers of services for a fee.** VANs provide added services if a customer desires a particular service and is willing to pay for it. If many customers want the same service, it will be developed and offered to all on an optional basis. Security is a form of value-added functionality that VANs can, but do not always, provide.

The following sections of this article describe the various types of controls that must be established to protect each of these three areas of responsibility.
Security of VAN Business Operations

The first requirement of VANs, as profit-making entities, is to protect their principal assets: the network, the software used to provide value-added services, and their own data. As such, they have a vested interest in ensuring the availability, integrity, and privacy of their information resources.

Availability.

Vendors generally achieve a very high level of availability. They do so by means of quality control, line diversity and component redundancy, and backup transmission capabilities.

They manage tightly controlled processes to ensure that the operations of the network are not disrupted, either while the network is being maintained or as a result of the changes themselves. This requires testing, checking, and controlled introduction of changes so that the effect of any error can be instantly identified, rectified, or withdrawn. The ongoing capability of the network and its services depends on management's ability to control quality and enforce standards of service.

Recognizing that some percentage of error will survive even the most rigorous quality control, network vendors must plan in advance for failure. They do so by providing alternative routing for the transmission and receipt of messages in the event one pathway becomes blocked, as well as maintaining redundant components, such as switches or frames, that can be used if the primary fails or is taken out of service.

In addition to providing alternate pathways for messages to take, a prudent network operator also provides alternative means of transmitting the messages. Many alternatives exist today, such as terrestrial cable, microwave, satellite, and cellular radio. Although terrestrial lines are the least expensive, they are also the most vulnerable to weather, earthquakes, and man-made disturbances. Microwave transmissions are subject to breakup over water, and satellites occasionally fail. No one means of transmission is invulnerable; that is why network vendors must provide backup transmission capabilities.

Protection of Proprietary Software.

For competitive purposes, the vendors protect their proprietary software from both external intrusion and internal misuse, primarily by means of access controls. The vendors must establish an internal security administrative function to control who has access to specific resources. It is necessary to keep careful control over systems programmers to prevent misuse, innocent or otherwise, over the system software. This is accomplished by limiting the types of privileges functions they have, monitoring all activity, and separation of duties.

Physical Security.

Just as the VAN software must be protected, so too must the physical components of the network. Customers should expect vendors to provide physical protection of their major nodes. Although terrestrial lines are usually routed through shielded conduit, it is not possible to prevent all cable cuts in a far-flung network. This is the reason that the vendors employ store and forward techniques, and why they absorb the cost for backup transmission facilities.

In the same way, they use business continuity and disaster recovery methods to protect their computer installations. Shared Direct Access Storage Device to allow multiple computers to access the same data will keep the value-added services available when a single processor fails. Use of multiple processors provides redundancy of processing capability. It is in the nature of intelligent networks that processing capability is not only multiplied but distributed to diverse locations.
The VAN should have a disaster recovery plan to ensure recovery if an entire facility is damaged or destroyed. Alternate processing sites, regular backups, and off-site storage should be supported. Each location should provide fire and water protection to prevent physical destruction.

**Auditability and Use Monitoring.**

One component of security is auditability, the means of determining how and by whom the network was used. All VANs (in fact, all commercial networks) have this capability, not only for security. Its prime purpose is for billing. In the case of a VAN, the vendor must know which network facilities and value-added services were used, and for how long.

There is software in each node for accounting and billing purposes. Although customers do not usually have access to this software, the vendor will usually cooperate with customers who have a need to review the audit trail after a suspected security breach.

**Security of Customer Information**

Although VAN vendors must protect their businesses, they also recognize that there are distinct requirements for security in an enterprise that takes control of others' resources in the regular course of business. These include ensuring that customers do not receive messages intended for another customer, that they cannot access other customers' data, that their data is protected from the vendor's employees, and that the overall network service is not degraded by the actions of a customer.

**Ensuring that Customers Do Not Receive One Another's Messages.**

VAN vendors ensure that messages are routed correctly by building in redundant destination controls. At each stage in a message's progress from sender to recipient, the network management system constantly checks that the message is going where it is supposed to go. This is particularly the case for packet switching, in which the message must be reassembled after being routed over multiple independent paths.

In some cases, vendors use terminal authentication to ensure that messages are sent to the correct location. This hardware-oriented feature ensures that the receiving device is the intended one. This level of security is not often requested and where available is usually provided for an extra charge.

Depending on the circumstances and consequences of misrouting, network vendors may have a legal or contractual liability to their customers. In financial activities, it is of little use for the sending party to blame a service vendor such as a VAN. The recipient is entitled to compensation, and the originator and the VAN must then settle the damages. Even if the VAN might elude reimbursement, failure to provide the essential service the customer paid for—transmitting messages from one point to another—is a distinct source of customer discontent. In a very competitive marketplace, maintaining customer satisfaction is a key to profitability.

**Ensuring that Customers Cannot Access One Another's Stored Data.**

A considerable amount of information belonging to or about a customer is stored on the VAN's computers. Some of this is for billing purposes, some for message routing; these sorts of data might be of interest to a competitor. But most critical in a VAN environment is the information that is being held for later retransmission (e.g., data in e-
mail and Electronic Document Interchange mailboxes). Attempts to tamper with or disclose such information must be detected and stopped.

To accomplish this end, the VAN vendors use various access control software products, both at the system level (i.e., software such as Resource Access Control Facility and CA-ACF2) and within their databases. The customers must take the responsibility for administering access to their own data. If the vendor performs this service, it is only as an agent for a customer, who retains the responsibility for how its employees use the data. Restricting access to customer data requires the vendor to establish and maintain a naming convention that associates customers with their files. In this way, the access control mechanism can limit the use of those files to individuals within the customer organization.

**Protecting Customers from VAN Employees.**

Because the data transmitted over a VAN may be of significant value, either for the financial assets represented or for the data itself, customers need assurance that their data is safe even from their vendors. Ultimately, there are some employees who can access any resource on the network or the computer system. A VAN would be unmaintainable if that were not so. In an emergency, the management of a VAN allows these employees access even to customer data to continue providing service.

It is at the vendor’s discretion to determine what constitutes an emergency. The vendor should notify customers if the confidentiality or integrity of their data is to be breached, even for valid purposes.

VAN vendors protect their customers from their employees by encouraging the customers to take as much responsibility as possible for their own security. For example, where possible, customer personnel, not vendor staff, should administer access to the VAN.

It is possible to buy insurance against misuse of the VAN by vendor staff, but this is a control of last resort. By the time insurance is invoked, the damage is already done, and the damage may have more than financial consequences.

**Protecting the Network from Customers.**

The vendor should ensure that no one customer can affect the service level of another. Put another way, each customer must be prevented from degrading or preventing use of the network and the value-added services.

In providing computer services, VANs must have strict controls to ensure process-to-process isolation. To each person sitting before a terminal attached to the network, it should seem that he or she is the only user present. Some of this is achieved through access control software, but more by the multi-user capabilities of the operating system on each platform. The primary role of access control software in this case is to prevent customers from reaching system software and files. In some cases, specific hardware or lines are dedicated to specific customers.

While help desks are usually thought of as providing service for confused users, they also have a powerful protective role in securing the VAN. Help desks are often the first to realize that a potential security breach has occurred. Because they monitor the network and the computers in real time, they are in position to detect when system or network resources are being tampered with or misused.

**Security of Fee-Based Services**

The successful introduction of new services often depends on demonstrating their security. This has been shown to be the case with e-mail and especially with Electronic Document Interchange. Expanded network services are made more marketable by making them more secure. If for no other reason, VAN vendors want the good public relations that
come with a claim of advanced security, and a variety of industry standards is pointing the way for them to do so. But if there is no clamor for message authentication or encryption or virus protection, these features will only be available as options, not as standard parts of the service.

**Encryption and Message Authentication.**

Where secrecy is the primary consideration of protecting the information on the network, encryption is the only choice. All other means of protection limit access to the information; only encryption protects the information itself, by rendering it unreadable by the unauthorized. In some cases, the confidentiality of the information has little value but there is great risk if a message cannot be read. For example, if the data in an Electronic Funds Transfer cannot be read, the money cannot be moved. In that case it is better to authenticate the message than to encrypt it.

To the extent that encryption and message authentication are used, the customer must be relied on to make them work. The customer must control the encrypted line, must manage the keys, bear the risk of equipment failure making messages unreadable, and accept the limitations on the ability to communicate with those who do not have such protection. Still, these techniques are the best available to protect the data in transmission. Most VAN vendors will provide encryption or authentication equipment for a fee. The service may also include key management techniques. But it is up to the customer to ensure that they are in place and are used properly.

**Password Protection.**

Passwords are the most commonly used form of security in communications systems. Yet many VAN vendors have found that their customers would like to do away with passwords. Passwords mean keystrokes; passwords mean memorization and inconvenience; passwords mean administration. Thus the VAN vendors must strike a balance between what they know their customers need and what they want.

Many VANs do not enforce any standards of length or structure for passwords, nor do they require their regular change. Some VANs may even fail to prohibit printing passwords in the clear. If customer management insists on protection for the passwords, these features can be made available, but often only at an additional charge.

**Security Reports.**

VAN vendors collect a substantial amount of information about network and service use. In the course of gathering that information, they also get indications of attempted misuse of the VAN. If those attempts harm the vendors’ interest, they must take action themselves. But what of attempted breaches within a customer's own domain? For instance, it is not the vendors' responsibility to detect misuse of an EDI mailbox by a customer's own users or systems.

A vendor would willingly pass along selections from its internal security reports if a customer could make use of them to manage its own security. This is easier to do when access to customer information is controlled by a commercial access control software package. But in many cases, the information a customer would need to manage its own internal security must be provided through custom coding and reports. Creating these reports, in turn, may require special fees to be charged.

**Segregation of Test and Production Environments.**

Keeping developers out of production processing has long been recognized as an important means of ensuring security. This may be especially difficult for such VAN
applications as EDI in which customer development staff are constantly devising new automated interfaces to the VAN's services.

Some VANs will allow (and many encourage) separate test and production facilities on the network and on the computers. In effect, this is like having two separate contractual arrangements with the VAN vendor. It is then the customer's responsibility to keep developers out of the production environment, through policy, password control, and enforcement. Although having two separate sets of services does not increase a customer's use of the VAN, some do charge additional fees for this segregation, for their administrative costs.

**Van Features That Create Exposure**

As conscientious as VAN vendors may be, they are also under pressure from customers to provide features that are detrimental to security. Security practitioners should be aware of such features and discourage their use.

**Auto Logon Terminals**

Many customers view passwords as an unnecessary nuisance. To do away with them, it is possible to have an intelligent terminal or microcomputer sign itself on when it connects to the network. Thus, anyone with access to the device has access to the VAN and its services. Individual accountability is lost and so, potentially, is the confidentiality of the data displayed on the terminal.

**Directed Signons**

Many VANs offer the facility of a directed signon, which takes the uninitiated user through all the steps needed to establish connection with the VAN. As a result, the hacker, as well as the new user, finds it much easier to learn how to access resources, even those for which he or she has no authority.

**Optional Access Control Software**

Many VANs have either acquired or developed access control software to manage user identification, rule-based access to resources, audit trails, and protection of system resources. However, for those customers who find passwords too burdensome, the vendor may make the access control software optional. In other words, where security is available, the vendor may be pressured to turn it off.

**Forever Fixed Passwords**

VAN vendors make it possible for a customer to bypass the change process and never have to change the initial password given to the customer's staff. Over time, the confidentiality of these passwords degrades, but there is little evidence of concern on the customer's part until security is breached.

**Assessing Van Security**

VAN customers should assess the security provided by their vendors. Such a review may be difficult to perform and may be best done by an independent third party. The assessment should address the following categories of control objectives:

- **Authorization.** The managerial practices that ensure that all access to the network, by both customers and VAN employees, has been approved.

- **Access Control to the Network.** Limitations on the ability of unauthorized users to access the network.
- **Access Control to Processes.** Restrictions on the value-added services a customer may use and that VAN employees may affect.

- **Access Control to Functions Within Those Processes.** Restrictions on particular functions within the services.

- **Auditability.** The ability to monitor and reconstruct activity on the network.

- **Recoverability.** The ability of the VAN to provide uninterrupted service, or if interruptions occur, to recover rapidly.

- **Systems Development and Maintenance.** The processes by which the network and its software are implemented, maintained, and upgraded.

- **Operational Controls.** The procedures by which the network is operated and controlled.

The following sections discuss these control areas in more detail

**Authorization**

The vendor should establish procedures for adding and maintaining users on the network. Such procedures control who is allowed access to the network and its underlying computer systems and the kind of accesses assigned to different users. These procedures must be performed by a vendor when adding a new customer. Thereafter, the customer should perform administrative procedures for its own users.

There should be a help desk or other interface to ensure that the network is used as intended. The help desk is often the first to recognize that an operations problem is actually caused by a security weakness or even a breach. These customer interface personnel are in effect the first line of defense for security.

There should be internal processes to control access or use of network services by vendor personnel. Formal authorization procedures provide assurance that access is granted only after review of appropriate supporting documentation. This is the basis for prevention of unnecessary and unauthorized access being assigned to internal personnel. The most significant restrictions should be placed on network engineers and systems programmers.

A vendor's organizational functions should be well documented to ensure appropriate segregation of duties. Documentation of functions instructs users of the system as to their proper activities, so that no one can completely dominate any process. The pattern of control and the functions allowed to personnel should be embodied in policy and standards with regard to security and control. Documentation of these procedures ensures that standards are applied thoroughly and consistently.

**Access Control to the Network**

There should be access control over operating systems on host and node processors where the value-added services are applied. These controls should address the implementation, testing, maintenance, and administration of those operating systems. This provides a reliable method of mediating access to the system and by extension to the network so that unauthorized users are not allowed on it.

Network access controls should be used to control communication processing and delivery of messages. These controls include terminal authentication and personal authentication by means of smart cards and challenge/response systems.
Monitoring and surveillance capabilities should be used to detect attempts to gain unauthorized access to the system. Attempted breaches of the network's security should be detected as soon as possible so that appropriate action can be taken.

**Access Control to Processes**

Access to network software should be limited to authorized individuals. This ensures that only people who are familiar with the network and are trusted individuals are able to modify its software. Even trustworthy individuals can make mistakes and in a commercial network environment error can be very harmful.

**Access Control to Functions Within Processes**

Network features should restrict users' ability to read, write, delete, and create messages and transactions. For example, a user who does not need to make changes to a static billing file but who does need to view it from time to time can be given read privileges but not write privileges. Data and transactions entered onto the network should be checked for authorization, accuracy, and completeness.

**Auditability**

Sufficient audit trails should be produced to enable users and the network service to reconstruct activities on the network and to recognize attempts at unauthorized activities in a timely manner. Internal audit, quality assurance, or a similar internal function should advise the management of the VAN of the current status and effectiveness of security controls.

**Recoverability**

The VAN vendor should strive for the highest possible level of continuous service. The physical resources of the network should be adequately safeguarded. The VAN should be provided with adequate physical security over computers and network hardware, stored data, and documentation to prevent unauthorized destruction, modification, disclosure, or use.

Plans for restoring full service in a natural or manmade disaster should be developed and tested. The disaster recovery plan should be both feasible and testable, and those tests should occur frequently.

**Systems Development and Maintenance**

VAN vendors should employ a formal system development methodology for the development and maintenance of network software. This should include procedures to ensure that changes to network software are authorized and restricted to approved changes. Moreover, these procedures should be defined to help ensure that all changes to software are requested by authorized individuals and are restricted to the changes that are requested. Processes should be included in the systems development life cycle for maintaining as well as developing applications. This ensures that security and control are addressed whenever changes are made to the network software.

Independent functions should be assigned responsibility for ensuring the integrity and security of network software. Such a separation of duties in the development and deployment process is critical to a trustworthy VAN operation.

Network software should be well documented and the documentation itself protected. In particular, the security and control features of the software should be documented. Documentation provides a base of knowledge which can be referenced in the future when
changes need to be made. It is also needed when knowledge of the security controls which exist within the network is required.

**Operational Controls**

There should be processes to secure data at the points of capture and during transmission to and from a VAN's computers. This helps to ensure that data is not intercepted by unauthorized users while it is being entered or routed to its destination. Network controls should be implemented to ensure that messages are received as sent, are complete, and are correctly routed.

**Third-Party Assessments**

Many VAN vendors make Service Auditor Report available to their customers. These reports, developed by accounting firms, are obtained by the VAN vendors on behalf of their customers. There is a degree of self-interest in this. By publishing the results of an audit, vendors can keep the customers' internal and external auditors from requesting access to their facilities to satisfy themselves concerning security and control in the VAN. The customers' auditors can turn to one source for satisfaction, and the vendor is not besieged by numerous requests for the same information.

Because value-added networks are, by definition, the property of a vendor, it is particularly difficult for a user to determine just how much (or how well) security is provided. The VAN vendor is unlikely to allow users to conduct a first-hand examination of premises or review its procedures for acquiring and monitoring lines. The vendor might open its doors for a single customer, but is unlikely to make it a general policy to allow access to all customers.

For all practical purposes, the only viable option available to most VAN users is reliance on the opinion of a third party—not the third party that operates the VAN but rather an independent assessor who has the access that the user would want if allowed. In all likelihood, this third party will be an independent accounting firm. Many communications specialists could perform such an assessment, but only accounting firms have generally accepted standards by which their opinions may be judged.

**Service Auditor Reports**

In the US, those standards and procedures are contained in a document released by the American Institute of Certified Public Accountants (AICPA), entitled “Reports on the Processing of Transactions by Service Organizations.” Because it is the seventy in a continuing series of standards, it is known as Statement on Auditing Standards (SAS) 70. It would be reasonable for a VAN customer to be concerned about the opinion on security offered by an accountant; how well versed, after all, is an accountant in communications security? However, other accounting standards require that the work be performed by individuals with the requisite expertise to make their opinions meaningful. All Big Six accounting firms—Arthur Andersen, Coopers & Lybrand, Deloitte & Touche, Ernst & Young, KPMG Peat Marwick and Price Waterhouse—employ such specialists. Smaller firms may also have such specialists, but for all practical purposes, external assessments of VANs under SAS 70 are performed only by the Big Six.

Even though all the accounting firms must adhere to the same standards, each firm may interpret them differently. Each follows different practices in determining whether security and control objectives have been met and the degree of evidence to prove the point. Moreover, there are two types of assessments. One, known formally as a Report on Policies and Procedures Placed in Operation and informally as a Type 1, requires only that the controls in question are demonstrably in operation. The other, a Report on Policies and
Procedures Placed in Operation and Tests of Operating Effectiveness, also known as a Type 2, requires the assessor to prove not only that the controls are in operation but that they actually are being complied with and are effective. While a Type 2 review is more valuable, many vendors choose only to have a Type 1 review performed. In fact, many VAN vendors, seeing little demand for security assessments, do no have them performed at all.

From the point of view of the customer, there are certain shortcomings to a Service Auditor Report, as these third party reviews are known. The vendor selects the criteria or control objectives under which the review is to be conducted. However, according to SAS 70, the auditor must agree to the comprehensiveness of the vendor's selected objectives. The review is in effect only at a point in time (Type 1) or over a period of time (Type 2) that has necessarily passed by the time the customer reads the report. SAS 70 is intended to apply to service bureaus, and in a sense that is what a VAN is, a communications rather than a processing service. But the requirements of the standard are focused not on the exigencies of network operation but rather on computer operations.

Most critically, the intended audience for a service auditor reports is the external auditors of the VAN's customers. As a result, the basis of the review (depending in large measure on the vendor and the auditor) is likely to be accounting controls rather than communications controls. As a result, the reader must interpret many of the observations made by the assessors to determine the overall security of the VAN.

Nonetheless, a service auditor reports is a review conducted under generally accepted standards, and it is of necessity comprehensive. This is because the auditor is being asked to attest not to the existence of specific security controls but to the overall system of controls, including security controls. The fact that a VAN vendor has made the expenditure to have a review performed indicates a clear mandate to implement controls. If there is a serious shortcoming in the attainment of a particular objective, the auditor is obliged to report it to the VAN's customers. Obviously, the vendors do not want negative observations about their services and so take the necessary steps to correct the conditions noted.

In summary, a service auditor reports is an attested survey of a VAN's security and controls. It is recommended that customers request these reports from their vendors.

Using A Service Auditor Report

The service auditor reports should be treated with healthy skepticism. It is not enough that controls meet an auditor's objectives, they must meet the customers' as well. Even though all security objectives have been met in the aggregate, it is still possible that the cumulative effect from non-critical weaknesses might constitute a serious security problem. Unfortunately, an service auditor reports is simply a report, and not a mechanism to effect changes if a customer is not satisfied with the network service's security and control.

Despite these shortcomings, this report can be a valuable tool if properly used and interpreted. The following paragraphs describe the key elements of the report.

The Opinion Letter.

The opinion letter is intended for accountants and need not concern most customers. However, the words except for in this letter indicate failure to achieve some control objectives. The letter also establishes the dates for which the opinion is in effect.

Network Description.

This section is, in fact, not written by the auditor but by the VAN vendor. It is the set of assertions that the auditor subsequently attests to. This is a concise technical overview of hardware, software, protocols, interfaces, and other information about the
VAN that enables a customer to determine that appropriate use is being made of the available network service features.

**Description of Policies and Procedures.**

This is the core of the report, the detailed description of the security controls. It tells what the service is doing to provide internal controls. From the point of view of the customers these security features are an extension of their operations and thus of their security system. Just as the determination of the adequacy of security is keyed to the achievement of stated control objectives, so too customers should consider their own objectives and whether these are being met.

This section of the report also gives some indication of the availability of external security and control features customers may take advantage of. Most critically, this section also identifies weaknesses that might prevent meeting a control objective.

**Client Considerations.**

In all cases, a vendor's security must fit within a customer's system of controls. A service auditor reports provides a guide to network features that are available to a customer and that should be considered as part of an organization's system of control. The report also points out security features that are made optional by the vendor and which should be taken advantage of. This section effectively places the burden on customers to incorporate available security and control measures and to carry out the appropriate tests of security.

**Conclusion**

Value-added networks are becoming an increasingly important component of business operations, providing both information processing and communications services. The customer for these services places itself at risk if it simply assumes that the network vendor's controls are adequate. This article provides a checklist of controls that should be implemented by the vendor and a method for assessing vendor compliance.

**Author Biographies**

Steven J. Ross

Steven J. Ross, a senior manager in the New York office of Deloitte & Touche, is a specialist in information systems security and control. He has implemented computer security systems for banks, government agencies, and industrial organizations, and has performed numerous assessments of systems security. He has published and lectured widely in the areas of information security and EDP auditing.