26

CHAPTER TWENTY-SIX

Auditing Telecommunications and IT Communications Networks

ALTHOUGH AN INFORMATION TECHNOLOGY (IT) auditor's internal controls review emphasis over the years has been on the general controls surrounding system's operations, often consisting of servers, storage devices and other components, or controls over individual application, IT telecommunications and their related internal controls are sometimes ignored or bypassed. However, this is also is a major area of IT internal control risks and vulnerabilities. While IT systems have been connected to local and external telecommunications devices since the earliest days of IT systems, technologies today are rapidly changing as we move to paperless, Internet-based systems. While the term telecommunications historically has referred to IT networked connections using classic telephone systems connected together with wires and cables, today technologies have expanded to a wide range of networked technologies, virtual private networks, and wireless systems.

This rapid adoption of global enterprise telecommunications systems in recent years has transformed the concepts of enterprise physical and logical IT security boundaries. Although some industries, such as financial services, have been using private telecommunications networks for many decades to connect their trading partners electronically, the current use of Internet-based systems has now resulted in the major usage of intercompany networks across many industries to electronically integrate trading partners as well as the emergence of public networks, including the Internet, for intercompany connectivity.

This use of telecommunications networking to integrate enterprises electronically brings such benefits as a rapid access to all levels of information, improved communications, reduced costs, increased collaboration with business partners, improved customer service, and an unprecedented ability to conduct effective electronic commerce. However, it also presents enterprises with a new set of IT internal control and security concerns.

With today's integration of networks between enterprises to facilitate electronic commerce, simple solutions to IT telecommunications security are no longer appropriate or possible. This chapter identifies some key security risks, internal controls and best practice countermeasures for controlling the connection of proprietary enterprise networks to one or more external parties over private or public wired and wireless networks.

The concepts covered in this chapter are broad and a more detailed discussion would require a full reference book of guidance materials for a more thorough internal control and security-based description and discussion. Many of the concepts discussed in this chapter also support or expand the Chapter 9 discussion on evolving internal controls issues that include wireless networks. This chapter provides a high level introduction to IT telecommunications systems and networks with an emphasis on such areas as virtual private networks (VPNs), intrusion detection systems, related security and their internal controls. This chapter's objective is not to make an IT auditor a telecommunications expert, but to provide a general IT auditor-related background information on some important telecommunications and IT network components.

NETWORK SECURITY CONCEPTS

While IT auditors are not responsible for designing the telecommunications networks, as installed at their enterprises, they should have a good understanding of these network components. An IT auditor should have an objective of evaluating an enterprise's IT telecommunications security strengths and weaknesses as well as the internal controls in place. While IT auditors will normally encounter telecommunications systems as mechanisms to manage and transmit data, these common concepts and terminologies apply to voice, data, video and other systems network technologies. Exhibit 26.1 describes a simple telecommunications circuit between a transmitter across a network

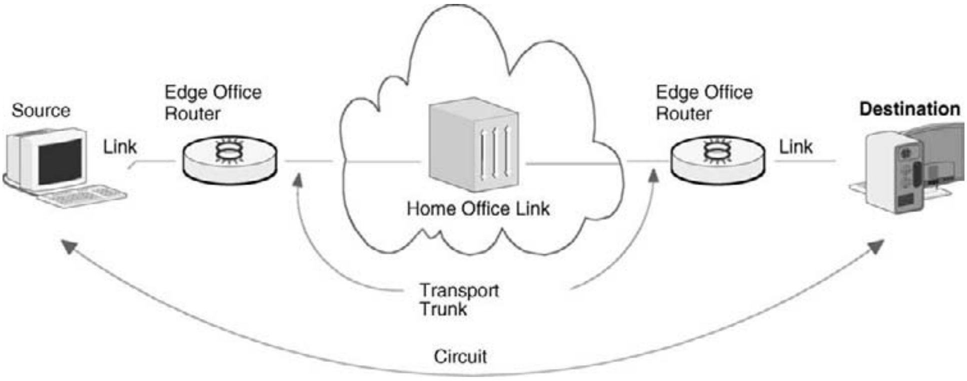

EXHIBIT 26.1 IT Network Components

involving multiple links and switches. Some of the terminology concepts supporting an IT telecommunications network include:

- **Transmitter.** Sometimes known as the send or source, this is the network component that originates a network information transfer. It might consist of a data terminal, voice telephone, host computer system, or video camera.
- **Receiver.** Sometimes known as the sink, target or destination device, a network receiver accepts the transferred information. Similar to transmitters, receivers can operate in different forms of media.
- **Circuit.** This is the logical, and often physical, connection between two or more elements in a network. Network circuits may be used for either access from an outside customer or customer premises to the edge of the network or for transport within it.
- **Link.** A two-point segment of an end-to-end circuit, such as from a terminal to a switch. The same term is used for telephone networks, but we will think of it here as a connection to IT equipment.
- **Trunk.** A telecommunications circuit used for sharing among multiple users and with any usage contention managed by network switching devices. For example, in an office telephone system a central office trunk connects the central office ''switchboard'' to the telephone company central office.
- **Channel.** A one-way connection between a telecommunications transmitter and receiver. A channel is a logical connection over a physical circuit to support a network communication.
- **Switch.** A network device that establishes, maintains, and changes logical connections over physical network circuits. A common example of a switch is a Private Branch Exchange (PBX) to establish telephone and telecommunication connections within an enterprise office.
- **Network.** The fabric of elements that work together to support the transfer of information. A telecommunications network can include everything from the transmitters to the switches. When a network extends beyond an office—such as with its local PBX—to other components, we often think of it as a wide area network (WAN).

The terminology and equipment supporting IT telecommunications networks has its origins in classic voice telephone networks. Although there have been many technology changes over time, many of these concepts have not changed all that much.

Data networks are generally configured as dedicated, switched, or virtual circuits. Dedicated circuits are used for a single user, although the source devices may be connected through a single office local area network such as a LAN, WAN, or other connections. They offer their users the advantage of a high degree of availability and specified levels of capacity, quality, and security. Traditionally, dedicated IT networks have been connected to large IT data centers that communicate intensively; similarly, many large enterprises with multiple locations have used dedicated circuit networks to tie together multiple locations.

Switched circuits are connected through an IT network through one or more intermediate switching devices. This configuration was traditionally established in the form of telephone central office PBX exchanges, where circuits are shared on demand

and as available. This configuration often results in significant operating efficiencies, and most data and voice calls today are carried over switched circuits, although the trend is to virtual circuits. The following sections outline some other key IT telecommunications concepts that are important for IT auditors.

Network Routers

Routers are physical or hardware devices that join multiple wired or wireless networks together. Whether on a wired or wireless network, a router connects networks and ensures that information does not go where it is not needed. This is crucial for keeping large volumes of data from clogging connections and making sure that information does make it to the intended destination. Routers are extremely important and useful in dealing with separate computer networks, joining them and passing information from one to the other and, in some cases, performing translations of various IT language protocols between the networks. A router also protects networks from one another, preventing the traffic on one from unnecessarily spilling over to the other.

As the number of networks attached to one another grows, the configuration controls for handling traffic among them grows almost exponentially, and the processing power of the router is increased. Regardless of how many networks are attached, though, the basic operation and function of the router remains the same. Since the Internet is one huge network made up of tens of thousands of smaller networks, its use of routers is an absolute necessity.

Although they are necessary, routers can introduce some security risks because they can present a potential abuse as a detectable launching point for incursions into IT networks. However, a router can also buttress the network it services against even sophisticated attacks, or at worst, it can offer a vulnerable target from which to reach invalid or private devices that otherwise would be unreachable.

An enterprise's IT functions and its network administration is responsible for installing and configuring router devices. This involves establishing and maintaining some detailed security tables to manage the device. The network administrator who seeks to secure a network must consider the role played by the external routers in enforcing the security of the local networks. However, much of this security role is performed by router hardware vendors, often with security functionality that contains a high level of sophistication.

An IT auditor often does not need to know the technical details of how an enterprise's routers are managed and configured. Rather, the auditor should look for documentation and best practices supporting good IT security environment controls in the IT systems configuration. These basic concepts were discussed in Chapter 19. An IT auditor performing an IT general controls review should meet with the IT network administration function and assess the router related internal controls environment by asking questions and gathering information in the following areas:

- Are the routers installed currently up to date on their system versions and revisions?
- Are router tables actively managed and updated when required?
- Is there management and coordination between network and other connected routers within the enterprise?

- Have controls been implemented to limit access to the services by which a router can be managed?
- Have software filters been installed in routers to prevent such functions as the Denial of Service (DOS) transactions or obviously spoofed traffic?
- Do the installed routers deny all incoming traffic to critical hosts, such as firewalls or the firewall management console or deny all outgoing traffic, except that with a source address internal to the network? This outgoing filter is essential to prevent the protected network from becoming an unwitting amplifier in a network attack.

Routers are key elements in the IT network security environment. If installed at a high level, an IT auditor should recognize their role and function in establishing a secure and well controlled IT network environment.

Firewalls

Besides basic physical security for an IT site, firewalls are the next most important aspect in controlling digital access into and out of the enterprise's IT network. They are a means of controlling the points of connectivity to the outside world, typically through the Internet. Firewalls were introduced in Chapter 20 and illustrated there in Exhibit 20.4, and we discuss them here from the perspective of IT telecommunications security.

The basic function of a firewall is to establish a protected boundary between outside information sources such as the Internet and internal IT resources. Sometimes this inside is referred to as the ''trusted'' side and the external Internet as the ''un-trusted'' side. As a generality this is all right. However, there are security risks and this rule of thumb is often not specific enough.

A firewall is a controlled barrier mechanism to control network traffic into and out of an enterprise intranet. Firewalls are basically application specific routers. They run on dedicated embedded systems such as an internet appliance or they can be software programs running on a general server platform. In most cases these systems will have two network interfaces, one for the external network such as the Internet and one for the internal intranet side. The firewall process can tightly control what is allowed to traverse from one side to the other. Firewalls can range from being fairly simple to very complex.

When installing firewalls, the enterprise IT security function should develop a comprehensive understanding of the system network and application architecture prior to their implementation. Knowledge of what must be permitted into and out of the network is an essential prerequisite to have an understanding of what must be excluded from the network. When this step is omitted, firewalls may be configured to ensure continued systems connectivity but also face the risk of improper network intrusions. The root cause of any knowledge gap here is often organizational schisms between applications, the system and the network administrators. It is often best to overcome these issues by involving all these parties in discussions to establish the required network traffic.

As with most aspects of IT security, deciding what type of firewall to use will depend on factors such as traffic levels, services needing protection and the complexity of rules required. The greater the number of services that must be able to traverse the firewall the more complex the requirement becomes. The difficulty for firewalls is distinguishing between legitimate and illegitimate traffic. An IT auditor should look for a requirements study in any evaluation process here.

The most basic protection a firewall provides is the ability to block network traffic to certain destinations, but an enterprise and its IT auditors should understand what firewalls do protect against and what protection do they not provide. If configured correctly, firewalls can provide a reasonable form of protection from external threats including some denial of service (DOS)[1] attacks. If not configured correctly they can be major security holes in an organization.

Similar to our discussions regarding routers, an IT auditor will typically not be an expert on the configuration and technical details surrounding installed enterprise firewalls. However, the auditor should look for some thoughtful study and analysis in installing enterprise systems firewalls as well as ongoing vulnerability analysis. Firewalls are important but are not the major panacea to IT network security. IT auditors should avoid the common misconception: *"I have a firewall—I'm safe."* Firewall vulnerabilities exist, and if a firewall is the only layer of defense, the enterprise can be as vulnerable to a knowledgeable attack as if it did not have one. An IT auditor should always look for multiple layers of network security controls when reviewing IT telecommunications networks.

EFFECTIVE IT NETWORK SECURITY CONTROLS

As a first step to undertaking the design or implementation of an enterprise IT network, an IT auditor should understand the enterprise's network security configuration and its internal control architecture. As part of this understanding, there is a need to understand the key concepts that should be considered when designing and implementing a security infrastructure to support an enterprise's communication needs and allow it to transact business securely in today's IT environments. The IT network security infrastructure should apply equally to pre-existing connections and to new initiative connections. As always, the network should be protected based on the risk it represents to the enterprise.

The network perimeter configuration is shown in Exhibit 26.1 as the cloud-shaped area surrounding the home office links and the internal trunk connections. It is often a first point where some form of security and traffic filtering should be implemented. This is often the first system that is accessed by external parties, and IT network controls depends on the enterprise, the type of connection and the sort of data or information that is being transmitted over the IT network. As a result, there should be many combinations of countermeasures and connections at this perimeter border to enhance IT internal controls and network security.

A common driver of security within enterprises is their IT security policy, and this policy should conform to relevant standards, such as ISO 27001 discussed in Chapter 18. The policy should define the IT network and security responsibilities within an enterprise and the key information assets that are required to be protected. A formal and well-understood policy here should guide the guiding security principles to be adhered to within the enterprise.

A key concept of any enterprise security program or facility is its depth. That is, there should be multiple layers of defense mechanisms that have to be circumvented to gain access to internal information assets and resources. Perimeter security, while important, must be supported by a strong internal security foundation. A single thin layer of perimeter security generally does not protect an enterprise adequately. Once a way is found through or around that thin layer of security, the security system can become ineffective.

The best source of examples for this multiple-level security concept can often be found in controls outside of just the technology-based areas. An IT auditor can think in terms along the lines of how does a traditional bank or any enterprise protect its assets? While the bank may be located in a sturdy building with bars on the windows and guards by the doors, a typical bank has any other additional levels of controls such as alarm systems, closed-circuit television, account reconciliations and, of course, a vault. Such a security system has been designed to ensure that if one layer is bypassed, there are several more layers either to trap the intruders or to make it easier to identify and subsequently apprehend them. In summary, the controls should make the risk of being caught higher than the reward for penetrating the security network.

Using our same bank analogy, any enterprise should protect its information assets as well. It should set limits on who can access enterprise applications and how they are allowed to update or use them. There should be security configured in multiple layers of defense for these, such as filtering routers, firewalls, what are called demilitarized zones and intrusion detection mechanisms. All these controls should work together to ensure that if one layer of security is breached, there will be another layer with different characteristics that either will protect the enterprise's assets or assist in detecting the intrusion.

This concept of a perimeter security defense applies to all enterprises. Many network security controls have been discussed in Chapters 19 through 22 on IT security risks and threats. In some environments, this can be a very major but often highly technical issue for some IT auditors and certainly for many members of general management. With regular and periodic reports of IT network intrusions and other improper activities, we are constantly reminded of the threats here. However, enterprise professionals often ignore these security risks and regularly move more and more of their activities to Internet-based and other IT network systems. While there are many different security systems and controls here, we will focus and briefly discuss the importance of effective intrusion detection systems and virtual private networks, both areas that IT auditors frequently encounter in their IT general and applications controls reviews.

Intrusion Detection Systems

Whether a neighborhood jewelry shop, a used car parts lot filled with rusting old cars, or a branch bank, virtually every type of enterprise needs some type of burglar alarm or intrusion detection system (IDS). The jewelry shop may have a burglar alarm bell that rings on an outside pedestrian street, the car parts lot may have the proverbial junkyard dogs to scare off intruders, and the bank may have sophisticated alarm mechanisms. We install these systems because there is always someone who may want to improperly take something from the facility or to break into protected boundaries. IT networks face similar risks of improper intruders and have the need for some type of IDS.

An IDS is a specialized software tool or hardware device that monitors an IT network and system activities for malicious activities or policy violations. These types of systems monitor transaction traffic and other events occurring in an IT system or network and analyze them for signs of possible incidents, including IT security policy violations or imminent threats of violation, acceptable use policies, or standard security practices.

IDSs operate as either network-based or host-based IT systems. The latter were discussed in Chapter 20. In a network-based IDS, sensors are located at network borders or choke points in the network to be monitored. The sensor captures all network traffic and analyzes the content of individual packets for malicious traffic. It operates as an independent platform that identifies intrusions by examining network traffic and monitors multiple hosts. Because of all of the variations in traffic, network monitoring requires more than just an easy "Here's a problem – Let's fix it!" approach. Exhibit 26.2 describes some of the IDS control procedure issues and approaches that an IT auditor should understand.

Terms are used by IT network security specialists to describe IT network security concepts and controls.

Alert/Alarm
An effective system will have mechanisms to provide signals suggesting that it has been or is being attacked.

True Positive
Alarms that highlight or produce a legitimate intrusion detection system attack.

False Positive
An event that signals an intrusion detection system to produce an alarm when no attack has taken place.

False Negative
A failure of an intrusion detection system to detect an actual attack. This is perhaps the most serious concern in an intrusion detection system as an attack is taking place but alarms are not signaled.

True Negative
When no attack has taken place and no alarm is raised. An IT security function should be satisfied with this level of messages.

Noise
Data or interference that can trigger a false positive. Careful tuning of any intrusion detection system should have an objective of eliminating such noise.

Site Policy
The guidelines within an enterprise and its IT function that control the rules and configurations of an intrusion detection system.

Site Policy Awareness
The need for an enterprise intrusion detection system administrator to dynamically change system rules and configurations in response to changing environmental and intrusion threat activity.

Confidence Value
A value an enterprise places on its intrusion detection system, based on past performance and analysis, to help determine its ability to identify an attack effectively.

Alarm Filtering
The process of categorizing attack alerts produced from an intrusion detection system in order to distinguish false positives from actual attacks.

EXHIBIT 26.2 Intrusion Detection Terminology

An IDS will be configured as either a passive or reactive system. In a passive system, an IDS sensor detects a potential security breach, logs the information and signals an alert on a console and for the owner. When these types of passive systems are installed, IT auditors often have internal control concerns. Enterprise IT security often fails to actively review such monitor reports for potential problems, and even worse, take corrective action in a timely manner. A reactive system can also cause problems. Here, the IDS responds to the suspicious activity by resetting the connection or by reprogramming the firewall to block network traffic from the suspected malicious source. This can happen automatically or at the command of an operator.

Though they both relate to network security, an IDS differs from a firewall, discussed previously, in that a firewall looks outwardly for intrusions in order to stop them from happening. Firewalls limit access between networks to prevent intrusion and do not signal an attack from inside the network. An IDS evaluates a suspected intrusion once it has taken place, watches for attacks that originate from within a system and then signals an alarm.

On the other side of the coin on such network security systems, intrusion *prevention* is the process of performing intrusion detection first and then attempting to stop detected possible incidents. Combined intrusion detection and prevention systems are primarily focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators. In addition, an enterprise may use such a system for other purposes, such as identifying problems with security policies, documenting existing threats, and deterring individuals from violating security policies. IDSs, particularly with strong prevention tools, have become a necessary addition to the security infrastructure of nearly any enterprise.

Intrusion detection and prevention systems are important elements of any IT network security architecture. An IT auditor should gain an initial understanding of the types and nature intrusion detection and prevention controls installed in an enterprise's IT network. Exhibit 26.3 outlines some IT audit control procedures as part of a general controls review of IT network security processes. In general, an IT auditor should seek determine if effective processes and tools have been installed and are used effectively. As transactions volumes increase and network threats continue an IT auditor should look for effective preventive and detective controls here.

Virtual Private Networks

Today many enterprises have remote offices and employees working from their home offices, both of which must gain access to their corporate network on a regular basis to perform their daily business. In the past, the traditional solution here was to use dedicated or leased lines for communicating with remote locations or branches, all relatively high cost solutions. VPNs usually offer significant cost savings over long-distance communication costs.

Instead of requiring the enterprise's offsite workers or business partners to install long-haul dedicated links or dial-in long distance to the corporate modem bank, a VPN enables remote users to connect to the enterprise's network, simply by placing a local call to their Internet service provider (ISP) or by using existing broadband connections.

1. Meet with the IT security function to understand the nature and status of any IT intrusion detection systems (IDS) installed.
   a. If IDS products are in place, gather documentation to understand their status and features.
   b. If there is no IDS capability, discuss reasons—from a risk perspective—why such tools have not been implemented.
2. Use IT network diagrams to identify and document locations of the IDS components.
   a. Do IDS components appear to be located at key IT network choke points?
   b. Has the same IDS technology been installed on servers and other host systems?
   c. Does the IDS appear to cover all areas of potential IT transaction activity, including business process systems and personal IT networks?
3. Based on discussions with IT security management, is the installed IDS a passive or reactive system?
4. Review and understand the nature of established intrusion prohibition rules, and assess whether they appear consistent with other systems and business operations.
5. If a passive type of IDS, review a sample of monitor logs to assess the nature of any reported intrusion violations.
   a. Meet with people and review systems responsible for monitoring intrusions, and determine whether they are following consistent and comprehensive procedures.
   b. Select several reported intrusion violations—systems or people—and assess the appropriateness of correction and remediation procedures.
   c. Determine that intrusion violation rules are reviewed and updated on a regular basis.
6. If the IDS operates as a reactive system, develop an understanding of the system rules and actions.
   a. Select a sample of IDS-based corrective actions and determine if the actions appear correct.
   b. Review processes in place to review and update components of the reactive IDS.
7. Review IDS procedures for handling such matters as false positives, and assess whether handling appears appropriate.
8. Review supporting software or consulting contracts for managing and maintaining the IDS, and assess whether it is actively managed and regularly updated.
9. Determine that appropriate processes and procedures are in place to change IDS sensors or system components due to enterprise network or system changes.
10. Meet with appropriate members of management to assess whether they appear to understand the risks and nature of the installed IDS.

EXHIBIT 26.3 Intrusion Detection and Prevention IT Audit Control Procedures

In either case, the remote users then can connect to the corporate network via the ISP and the Internet.

The main reason why an enterprise would consider implementation of a VPN over the Internet is the potential to realize significant cost savings over time. While the initial installation costs of a traditional solution such as dedicated or leased lines for communicating with remote locations or branches would be roughly the same as a VPN solution, a VPN will quickly yield cost savings. In addition, there can be significant cost savings by carrying other traffic, such as voice messages, over the Internet as well.

There is a strong need for the protection of information in transit for these remote access locations, and effective IT telecommunications security over these branch network connections or internal networks is essential. Enterprises that have remote

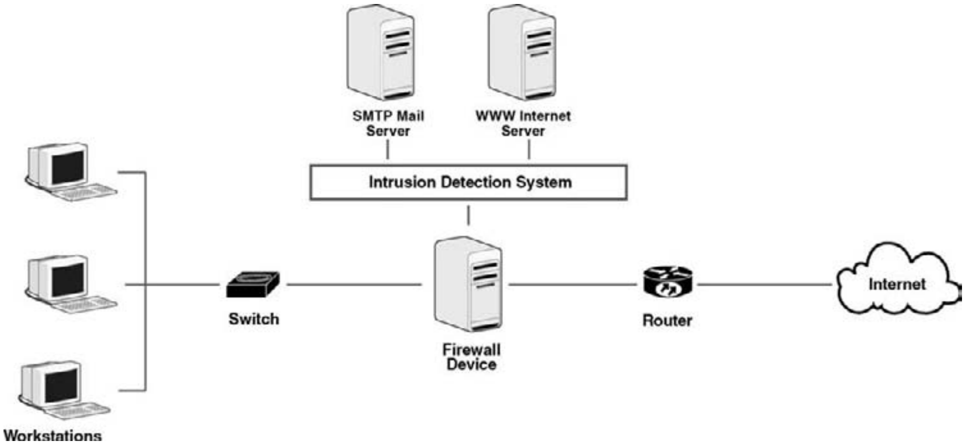

EXHIBIT 26.4 VPN Configuration Integrated with Firewall

users had historically requested that their employees use their personal telephones in dial-up connections to access the corporate network. However, there are weaknesses and significant security vulnerabilities in the use of dial-up connections. While dial-up telephone access connections usually represent the lowest cost and simplest solution, VPN connections are becoming increasingly popular. Their aim is to provide the remote user with a simple means of becoming part of the corporate network. Once connected, the remote user can use network resources as if physically in the office and connected to the corporate network.

VPNs allow remote users to connect through the Internet with a dial-up modem or a high-speed solution, such as cable or asymmetric digital subscriber line (DSL). Many users today use DSL lines or wireless connections to connect their home computers to the Internet, and a VPN allows them to link with their enterprise network. As with any network connection, a VPN solution can be a security risk if not properly configured and maintained, although it has many advantages over the traditional dial-up connection.

Although there are multiple ways to configure and implement a VPN, Exhibit 26.4 shows a VPN configured with a firewall. Remote users may use the home computer DSL lines or other connections to enter the Internet. A transaction addressed and directed to the enterprise router then passes the activity to an installed firewall. The network activity would then have to pass through an intrusion detection barrier before reaching enterprise systems and servers. This is a simple system diagram with only one firewall access gate, a potential single point of failure; many other configurations are common as well.

VPN Risks

A VPN should normally be configured as a secure, private communication link or tunnel between two or more devices across the Internet. The VPN system can be either a computer running VPN software or a VPN enabled router special device. It allows a home computer to be connected to an office network or can allow two home computers in different locations to connect to each over the Internet. A VPN is a very good IT telecommunications approach, but it comes with some risks from an internal controls perspective.

Properly configured, VPN data travels across a public network like the Internet in a secure encrypted manner. If anyone ''listens'' to the VPN communications, they will be blocked because VPN data should be encrypted. However, any VPN faces a major security risk if that encryption software has not been properly installed, tested, and monitored. An IT auditor when reviewing a VPN's internal controls should look for evidence of an adequate enterprise IT security function assessment of their security and legal risks arising out of using VPNs, and a strong implementation of controls to protect data while they are entering the VPN as well as at the point on leaving the VPN. The failure to secure information while unencrypted over a given network path could result in confidentiality, integrity, non-repudiation, and/or availability issues.

Most small- to medium-sized enterprises will usually contract with a third-party vendor to help them install, configure, and even sometimes manage their VPN. However, reliance on third-party service providers could result in risks such as the choice of an inappropriate provider, lacking strong VPN-based governance and management processes. Based on our Chapter 7 discussion on IT infrastructure controls, there should be active measuring and monitoring of service level agreements (SLA) and metrics supporting the VPN.

Any VPN can cause some major risks to the enterprise if there has been an inadequate backup and redundancy strategy when implementing it. The Exhibit 26.4 VPN illustration is an example. Although many VPNs have been implemented following that type of configuration, there can be risks associated with a failure to provide redundancy or back up and both a lack of reliability, inadequate capacity, and the lack of confidentiality on operation parameters or data. An IT auditor should meet with IT management and its security functions and assess whether adequate attention has been given to assessing VPN risks and well as adequate risk protection procedures.

AUDITING A VPN INSTALLATION

Although this chapter has discussed a variety of IT telecommunication issues, VPNs are relatively new and represent an important area for an IT audit internal controls review. Before launching any VPN review, an IT auditor should obtain some technical and configuration knowledge of the VPN installation to be reviewed as well as an understanding of such technical areas as the encryption technologies used, network security architecture, and security technologies. On a high-level, much of this information can be found in other chapters in this book, and a Web search can yield even more. As part of the audit-planning process, an IT auditor should initially perform a high-level risk assessment, gathering requirements for the VPN configuration.

As discussed in all IT audit reviews, the responsible IT auditor should clearly define the scope and objective of the VPN review. In addition, all affected stakeholders should be explicitly identified as part of the planned audit's scope. Any key concerns of the stakeholders should also be included, as appropriate, in the scope and objectives of the

1. Meet with IT management to understand responsibilities for managing VPN operations. If a third-party vendor is used, establish or obtain right-to-audit privileges.
   a. Document and understand proposed VPN technology, such as VPN model, VPN architecture, VPN configuration/topology and planned VPN usage.
   b. Assess whether expected VPN benefits are being achieved.
2. If the VPN has been implemented within the last year or is still being developed, review project status reports, management approval, budget documents, project plans, and other status reports to determine whether the VPN is being launched in a well-controlled manner.
   a. Evaluate the actual implementation of the technologies against the plans, and identify any deviations.
   b. Discuss the VPN with members of operating management, and assess whether their expectations are being met.
3. Review the actual VPN development contracts, SLA and metrics measures that were agreed on, and assess whether well-controlled procedures are being followed.
4. Evaluate the actual security architecture and encryption technology implemented for conformance with the approved VPN design.
5. Document the current or planned VPN, and determine that it meets approved project plans.
   a. Confirm whether the solution is certified to conform to one of the PPTP, L2TP, or IPSec protocols.
   b. If the VPN is primarily developed in-house, identify the persons responsible for VPN operations, and assess whether training appears adequate.
6. Evaluate the VPN redundancy and backups established, and determine whether they are consistent with enterprise disaster recovery plans and good operating practices.
   a. Through a review of VPN operations, determine that their redundancy and backup facilities are functioning appropriately.
   b. Determine that appropriate security tools and processes are in place for such things as virus checking and intrusion detection.
7. Evaluate the adequacy of the VPN testing and migration processes to assess whether they address all kinds of users and cover such things as capacity, bandwidth, access control, and encryption in an appropriate manner.
8. Determine that the implemented VPN and its technology are being used as intended.
9. Evaluate the progress of the VPN implementation with reference to its appropriateness and adequacy to mitigate the risks—security risk, third-party risk, business risk, implementation risk, and operating risk.
10. Determine that the VPN and its usage are in conformance with enterprise and other good security policies and procedures including strong data classifications.
11. Determine whether third parties accessing the VPN via extranets have signed the relevant security and confidentiality agreements and are complying with the same.
12. Ensure that SLAs and metrics, including quality of service assessments, are measured, monitored, and escalated on a regular basis for timely actions.

EXHIBIT 26.5 IT Audit Steps for a Review of VPN Internal Controls

review. Also, in case the VPN review scope includes third-party providers, the IT auditor must assure a right to audit clause was included in their contracts. The audit should then be scoped and launched consistent with the objectives of the review.

The responsible IT auditor should gather and study the available VPN documentation, such as business systems documentation, contracts, service level agreements and log reports. Discussions with stakeholders and service providers as well as observations can be used in gathering, analyzing, and interpreting the collected VPN data. Where appropriate, the IT auditor should test significant processes and functions in the VPN environment to verify that they are performing as intended.

Particularly if this is a relatively new VPN installation, other information gathering items that should be included in the review are:

- Requirements for the proposed VPN solution, including any cost-benefit analyses, as well as evidence of business and IT approvals
- The proposed VPN technology, such as hardware models, VPN architecture, and the network configuration and topology
- The VPN security architecture and features, including its encryption technologies
- VPN redundancy, disaster recovery and backup facilities
- Documentation supporting the selection process for the choice of the service provider as well as supporting project management materials and monitoring mechanisms
- The VPN service provider contract, supporting SLAs and metrics
- Statutory requirements, if any, that needs to be fulfilled for this VPN

Based on these gathered materials, an IT auditor should launch a review of the enterprise VPN. Exhibit 26.5 outlines IT audit steps for a review of an enterprise's VPN system. In performing this review, the inferences and recommendations should be based on an objective analysis and interpretation of the data. The results of this review should include audit report findings and recommendations for corrective actions.

NOTE

1. Denial of Service (DOS) Attack. A malicious attempt to make a computer resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DOS attack may vary, it generally consists of the concerted efforts of a person or people to prevent an Internetsite or service from functioning efficiently or at all, temporarily or indefinitely.