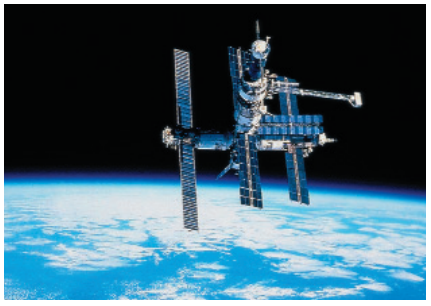
Using Virtual Private Networks to Gain Competitive Advantage

Outsourcing can be a booster rocket in the race to patent and market innovative products



PHOTODISC INCORPORATED

In the pharmaceutical industry, time-to-market is everything. Companies race to innovate, receive a patent, reach the market, and finally, garner a profit — all before product exclusivity has expired. This fast-paced drive to success means that pharmaceutical companies must use every advantage to get ahead. However, few companies have the resources required to evaluate and implement all the available opportunities, and few companies possess the networking-savvy personnel required to maintain communication technologies.

Because communication technologies are so intricate, outsourcing the maintenance of these technologies is a favorable alternative. Contract services providers can better serve their customers by offering virtual private networks (VPNs). A VPN enables a business to securely connect remote users, branch offices, business partners, and customers using encrypted connections over a public network such as the internet. Pharmaceutical companies can use VPNs to gain an advantage in such a highly competitive and regulated industry. By understanding how VPNs work, pharmaceutical companies can benefit from this technology (in regulatory compliance for example). Contract services providers should consider several alternatives when evaluating VPN solutions.

Mark Tuomenoska *is chairman and founder of OpenReach, Inc., 660 Main Street, Woburn, MA 01801, 781.933.7580, mark@openreach.com. Contributing editor* ***Jim Miller*** *is publisher of* Bio/Pharmaceutical Outsourcing Report *(B/POR). PO Box 8163, Springfield, VA 22151-8153, 703.322.4971, fax 703.503.4506, info@pharmsource.com, www.pharmsource.com.*

Benefits of VPNs

VPNs offer individual users and computer systems secure communication when using the internet. Special-purpose VPN software is used to guarantee the authenticity and privacy of data as well as the identity of the people communicating — a function that allows companies to take advantage of the low-cost and ubiquitous nature of the internet while ensuring the security of the information.

Companies that use VPNs can experience a number of benefits.

Increased speed and flexibility. VPNs operate independent of the underlying telecommunications infrastructure. As a result, they can be deployed quickly using any internet connection. A collaborative investigation between two companies can be established in minutes and maintained for months. New acquisitions can be brought online by using the VPN as either a temporary or permanent solution.

Improved security. VPNs guarantee the identity of individuals and systems, ensure the privacy and integrity of transmitted information, and limit the access of each participant to the resources that are authorized for use. Rather than build security into each application and service individually, VPNs build security into the communications infrastructure only once for all applications. External and internal communications also benefit from this security implementation.

Increased regulatory compliance. By offering a VPN solution with a built-in public-key infrastructure (PKI), contract services providers can ensure that their clients' companies comply with 21 CFR Part 11 requirements for electronic records and signatures. Because PKI identifies and authenticates network users and encrypts and decrypts data (using digital keys, certificates, and signatures), it ensures that the communications meet full regulatory compliance.

Greater resiliency. VPNs provide a layer of insulation between networked services and applications and the physical transport network. This insulation allows companies to change one part of the system without affecting the other. This function has become particularly important considering the recent carrier bankruptcies (of network providers, for example), which prove that the viability of large service providers can no longer be guaranteed. Unlike legacy data networks that are provided by a single carrier and are, therefore, subject to the fortunes of that carrier, a VPN allows network managers to diversify their telecom portfolio and to quickly implement changes if they are required.

Jim Miller's Outlook

The outsourcing industry and Wall Street were taken by surprise when **Quintiles Transnational** (www.quintiles.com) founder and chairman Dennis Gillings made an offer to privatize the company.

Quintiles announced in October that Gillings had formed a new entity, **Pharma Services Company** (Research Triange Park, NC) that had made an offer to buy the outstanding shares of Quintiles for $11.25 per share. The stock had traded below $9.00 per share the day before the offer. The Quintiles board of directors appointed a special committee of independent directors to assess the offer. The committee then hired investment bank **Morgan Stanley** to advise it.

The management buyout was to be financed through a combination of debt and equity. Pharma Services Company arranged an equity commitment of $298 million from **One Equity Partners LLC**, the private equity arm of **Bank One Corporation**, and debt commitments totaling $620 million from **Citicorp North America, Inc.**, and **Salomon Smith Barney, Inc.** Gillings owns or has options for 7.3 million shares of Quintiles stock, or about 6% of shares outstanding, and management controls about 8% overall. However, in November, Quintiles rejected the proposal as "inadequate."

The drop-off in stock price reflects both general concerns about the outsourcing industry's prospects considering the current retrenchment among pharmaceutical companies and the particular problems faced by Quintiles. The company has seen its revenues erode steadily since late 1999. Corporate revenues were dragged down by problems in the contract sales business even as contract research revenues improved. Quintiles's profits have been volatile, despite several efforts to cut costs. Management has been working to overcome problems in staff turnover and service quality but has not tried to narrow the focus of service offerings as competitors such as **Covance** (www.covance.com) have.

In an effort to get better returns from its service businesses and pharmaceutical expertise, Quintiles initiated a new strategy in 2001 that takes an at-risk position in client companies. The company provides equity and debt financing for select companies through its **PharmaBio Development** investment unit and fronts salesforce startup costs for certain contract sales clients. In return, Quintiles earns fees for services and royalties from product sales with future royalties estimated to be from $500 million to $1 billion.

Many analysts believe that PharmaBio has added a substantial level of uncertainty to Quintiles's future prospects, making it difficult to project future performance and therefore stock value.

Patheon Purchases a U.S. Site

Patheon (www.patheon.com) fulfilled a major strategic objective with its recently announced purchase of the **Aventis Pharmaceuticals** (www.aventis.com) manufacturing and development site in Cincinnati, OH. The transaction was expected to close on 31 December 2002, assuming no problems arise during due diligence.

The acquisition provides a U.S. base of operations for Patheon's Pharmaceutical Development Services (PDS). In recent months, Patheon executives have emphasized the need for a U.S. site for PDS because they cannot recruit enough scientists to the Toronto area to achieve their business growth objectives. PDS grew 70% in the 2002 fiscal year and garnered revenues of $25 million in the first three quarters of the year.

Continued on page 30

Improved performance. The development and deployment of new pharmaceutical research and modeling applications continue to drive demand for network capability and performance. VPNs can take advantage of the overcapitalization and build-out of the internet protocol (IP) industry to provide performance that exceeds that of conventional networks. A VPN allows a company to harness the power of these public networks for private-enterprise communications.

Reduced costs. VPNs help reduce costs because they use the internet rather than private data networks. By using a VPN, companies can save 30–50% on domestic communications and 40–90% on international communications and, at the same time, gain better performance and increased reliability than they had with legacy networks.

How VPNs Work

A VPN consists of four basic elements: VPN gateways, VPN remote-access software (RAS), VPN management and authentication systems, and IP transport services.

VPN gateways are computers that initiate and terminate secure connections called tunnels. Tunnels can be established between two gateways, in which case the gateways secure traffic for an entire network, or between gateways and individuals who are using VPN RAS. VPN gateways are used in stand-alone or a combination configuration, and both versions support router and firewall functions. The stand-alone gateway is ideal for a large research center that already has IP infrastructure (such as a router and firewall). A combination VPN gateway is ideal for small offices with a minimal IP infrastructure.

VPN RAS. VPN RAS is used by individual PCs and personal digital assistants to establish secure connections to VPN gateways and is ideally suited for mobile users and individual extranet partners. Two types of VPN RAS are available: internet protocol security (IPSec) and secure socket layer (SSL). IPSec RAS is a "heavy" client VPN (it requires software to be loaded onto each user's PC and provides a more secure connection than an SSL.) IPSec RAS can be installed on individual PCs to provide transparent connections to corporate resources. For example, when the VPN connection is made, the device has access to all resources on the local network, such as printers, servers, applications, and other PCs, as though they were physically located in the building.

SSL RAS is a "light" client VPN (it does not require software to be loaded onto

Jim Miller's Outlook

Continued from page 29

The deal is also important because the Cincinnati facility has larger-scale manufacturing capabilities than Patheon's Canadian sites, which will enable the company to bid competitively on large-volume products. The transaction will add 11 new commercial manufacturing relationships to Patheon's portfolio because Aventis had already established 10 contract manufacturing relationships at the facility. However, even with the 10 contracts, the site's use rate was just 50%, and capital investment was sufficient only to maintain the plant's operations and regulatory compliance.

The deal has the hallmarks of a typical Patheon facility acquisition, especially the very favorable price for assets ($35 per ft^2, including the equipment but excluding the 120,000-ft^2 warehouse.) The five-year supply agreement with the seller includes products manufactured at the site. Patheon will invest $23 million in the site in the next three years, including $13 million for the expansion of the PDS facility and a new information system and $10 million for sustaining investments. Favorable financing from state and local government agencies will help reduce the ultimate cost.

Outsourcing Revenues Strong

Contract research and manufacturing organizations continued their strong performance during the third quarter of 2002, with double-digit revenue increases still the rule (see Table 1). As has been the case for nearly two years, preclinical research activity is leading the way, driven by a big early-stage pipeline and changes in sponsor outsourcing practices.

Contractor results also are being helped by continued acquisition activity. Recent examples include the acquisition of clinical CRO **Barton & Polansky** by **Icon Research** (www.iconus.com), preclinical CRO **Springborn Laboratories** by **Charles River Laboratories** (www.criver.com), and central lab **Virtual Central Laboratory CL** by Covance.

Although the acquired companies are small in relation to their acquirers, their performance has had an immediate positive effect on the acquiring companies, which can be seen when comparing the acquirers' quarterly results with those of the previous year.

In the clinical research arena, the numbers suggest that some major market-share shifts are in the works. Several companies such as Quintiles, **Kendle** (www.kendle.com), **AAI** (www.aaipharma.com), and **Omnicare** (www.omnicare.com) had single-digit or no growth, and **PPD** (www.ppdi.com) and **Icon** had growth rates that were double the mid-teens average for all contractors. ***BPI***

Table 1. CRO third-quarter revenues and growth rates

	Revenue[a]	Percent Change
AAI International	19.6	−17
Albany Molecular	19.0	24
BioReliance	21.6	16
Cardinal Health PTS	354.0	18
Charles River Laboratories	84.6	16
Covance	221.0	13
Icon Clinical Research	46.9	29
Inveresk	55.9	19
Kendle International	41.0	4
LSR	30.0	16
Omnicare CRO	34.0	8
Parexel	119.4	17
Patheon	108.7	26
PPD	146.0	35
Quintiles	458.8	−1

[a]in U.S. milion dollars

individual PCs) that uses the device's web browser to establish a secure connection to a VPN gateway. With SSL RAS, the gateway provides secure, but more-limited, access to local area network resources such as email, file browsing, web-enabled applications, and some client–server applications.

Authentication and management systems. Often overlooked aspects of a VPN are the management and authentication systems. Such a system includes three basic capabilities: configuration and management, authentication and authorization, and monitoring and alerting.

Configuration and management. Many VPN gateways include rudimentary management capabilities that allow companies to configure the server and set up connections. These capabilities are fine for small networks with a limited number of gateways but cannot accommodate large implementations because they require network managers to make individual configuration changes to each device. Companies that have more than five to 10 locations or extensive partnerships will require a global centralized management system.

Authentication and authorization. To comply with 21 CFR Part 11 requirements, companies must authenticate and authorize users and data, as well as encrypt data in transit, to ensure the integrity and parity of electronic documents and signatures as compared with traditional paper-based versions. Although VPN gateways and RAS use encryption technology to maintain the privacy and confidentiality of information in transit, they are only half the security equation. VPN authentication and authorization systems guarantee the identity of individuals and gateways and govern the resources available to each.

Many types of authentication systems exist, including user IDs and passwords, secure tokens, biometrics, and digital certificates. When deciding which system to use, you should consider two factors: the level of required security and how important it is for end users to ensure that the systems are properly implemented. If using authentication is complicated or cumbersome, users will look for ways to circumvent the system, which can compromise network security.

Many companies that require heightened security use digital certificates for VPN authentication. Digital certificates provide high levels of security, but can be completely transparent to the end user. The only caveat is that although they allow easy access to the end user, digital certificates often require more support from the IT department, which is another reason to outsource VPNs.

Monitoring and alerting. Contract services providers must ensure the availability, health, and performance of the

network. The task of monitoring and alerting becomes increasingly difficult in a broadly distributed and diverse environment in which problems can arise — from users entering the wrong password, to gateways being improperly configured, to physical connections slowing or failing altogether. Most VPN gateways include simple monitoring and alerting functionality that notifies IT staff if a problem arises. In addition, VPN systems can be easily integrated into common network management systems such as HP OpenView (www.openview.hp.com).

IP transport services. Another benefit of VPNs is the ability to use an IP connection virtually (from dialup to wireless to DSL to cable to T1 to fiber optic) to establish a secure connection.

VPN Alternatives

When offering VPNs to their customers, contract services providers should consider various options to determine what is best for their customers while still keeping in mind the breadth of their own capabilities. Four types of VPN solutions are roll-your-own (RYO), traditional carrier services, independent managed service providers (MSPs), and VPN overlay services. In each instance, the VPN elements remain the same; however, trade-offs may be necessary in time-to-deploy, physical outreach, security implementation, budgets, and required IT resources.

RYO VPN. Numerous vendors sell all the elements that are required to build a VPN. The benefit of the RYO approach is that the contract services provider is in complete control of the network, from its design and implementation to its daily management. The RYO solution also requires a contract for internet connections, which serve as the transport for the VPN. Although this approach provides the greatest control, it requires significant capital and labor costs to implement the network and to maintain it.

Carrier services. Nearly every major telecom carrier offers VPN services. These services come complete with the VPN systems and internet connections, offering one-stop shopping and simplifying operations. With carrier services, the carrier is responsible for the network's design, implementation, and management. These services can reduce capital and labor costs but at the expense of company control. VPN connections are limited to locations within the carrier's service area, which may not encompass international locations or may prevent connections to strategic partners who subscribe to the services of another carrier. Contract services providers should consider these factors when providing this option to customers.

MSPs provide the ease of implementation associated with carrier services but with more flexibility. An MSP includes all the labor-intensive tasks of setting up and operating the VPN, but does so independent of the physical transport. Most MSPs maintain contracts with several carriers and can select the most appropriate carrier on the basis of coverage, availability, and cost. In some cases, the MSP can even incorporate the capital charges into the contract as a component of the services offered, thereby eliminating labor and capital costs.

The downside of the MSP approach is that companies lose control of their network policies, a drawback similar to that of carrier services. When IT managers must make changes, they must call the MSP, and the MSP makes the change for the customer. The MSP itself is a contractor — a very specialized one. Therefore, it is possible to partner with an MSP so that the customer has only one contractor to work with; however, the extra time required for communication between the third party and the client often makes this an unwieldy option. Instead, companies are better served by contracting directly with the MSP and using their regular contract services provider for all other outsourcing needs.

Overlay services providers. VPN overlay service providers operate like VPN MSPs. Both provide implementation and management services for the customer, but VPN overlay service providers accomplish these tasks by using sophisticated technology and automation tools, which can result in low overall costs. In addition, overlay services providers give companies direct control of network topology and policies instead of causing them to depend on the MSP to make changes. The drawback of an overlay service is that the company still must procure and manage transport services from a telecom carrier. Unlike the MSP option, a partnership between overlay services providers and contract service providers is more feasible and probably the best option of the four solutions. With this option, contract services providers have more control, a wider reach than with carrier services, and less technological maintenance than with a RYO VPN. Overlay service providers offer the most service for the least work.

Benefiting from Collaboration

VPNs give pharmaceutical companies a competitive advantage by allowing research laboratories and strategic partners to be connected quickly and securely, by supporting real-time collaboration that shortens the drug discovery timeline, and by reducing operating expenses. These benefits maximize profits and contain the cost of healthcare. Contract services providers can better serve their customers by providing a VPN option that increases flexibility, speed, resiliency, security, performance, and regulatory compliance — a cost savings of up to 90%.

A VPN provides a complete networking infrastructure that includes components such as servers, software, authentication systems, and management controls. Companies that want a high level of control can build their own VPN by purchasing the components and designing, implementing, and managing the network themselves, or they can use contract services providers to work with other service providers to reduce capital and labor costs.

The RYO VPN approach provides a company with ultimate control yet requires significant labor and capital costs to implement and maintain the VPN. Carrier services include a VPN system with telecommunications connections but may pose limits on the locations that can be part of the VPN. MSPs allow a company to select from multiple carriers to ensure appropriate coverage but leave the IT staff without direct control of users or network policies. Finally, VPN overlay services providers offer contract services providers the control of an RYO solution without the labor requirements. Overlay service providers use technology and automation tools that simplify complex management tasks; however, companies have to contract their own telecommunication services. ***BPI***