

QIAGEN, Inc.

Assessing Disaster Recovery with the Help of Symantec Consulting Services Speeds Time to Deployment by 33 Percent



Data protection and availability are at the priority forefront for QIAGEN, Inc., a life sciences company that supplies nucleic acid (DNA/RNA) sample handling, separation, and purification products to some of the world's largest pharmaceutical, biotechnology, and diagnostic companies. At the same time, like almost any other private-sector enterprise, QIAGEN faces daily pressure to reduce cost while improving productivity. In tackling these daunting challenges, QIAGEN found a trusted technology advisor in Symantec and Symantec Business Partner Applied Computer Solutions, which initially provided a data protection solution and then, more recently, a business continuity solution. These solutions are proving to be right amalgam, as QIAGEN is realizing wide-ranging results—including a 25 percent lower total cost of ownership in IT equating to a 100 percent return on its Symantec software investment within 36 months, 30 percent to 50 percent faster backup times, and exponential growth in data and backup volumes.

Company Profile

QIAGEN (www.qiagen.com), with headquarters in Europe, is the world's leading provider of enabling technologies and products for the sample handling, separation, and purification of nucleic acids (DNA/RNA)

Industry

Life Sciences

Solution

Data Protection
Storage Management
Business Continuity Planning

Close call prompts QIAGEN to investigate business continuity options

As the world's leading provider of enabling technologies for separating and purifying nucleic acids, QIAGEN, Inc., understands the importance of data. So, when a wildfire came within few miles of its primary North American data center facility in California the company realized that it needed to take a close look at how well it could recover its vital business data and resume business operations within a reasonable amount of time in the event of a disaster.

QIAGEN delivers its nucleic acid (DNA/RNA) sample handling, separation, and purification products to top biotechnology, pharmaceutical, and government research organizations such as Amgen, Genentech, Pfizer, Monsanto, and the National Institutes of Health. With more than 1,400 employees in 12 countries and headquarters in the Netherlands, QIAGEN has a field sales force nearly 500 strong and a global distribution network that serves more than 42 countries. The company has data centers in Germany, California, and Maryland that support the complex IT requirements of the life sciences' organization.

In the aftermath of that wildfire, Prashant Vaidya, director of IT for North America Operations for QIAGEN, prompted by a mandate from Global IT Director Stephan Huetzen, began an investigation into the company's disaster recovery preparedness. Since his IT

“What really impressed us about the Symantec proposal was the insight the consultants had into our business.”

Prashant Vaidya

Director of IT, North America
QIAGEN, Inc.

A software standardization solution from Symantec based on Veritas NetBackup and Veritas Storage Foundation software helped reduce backup times by 30 percent to 50 percent.

“We wanted a vendor offering more than just a product. It was pivotal that the technology solution also include partner integration from the standpoint of consulting and ongoing support.”

Prashant Vaidya

Director of IT, North America
QIAGEN, Inc.

team had already successfully deployed a data protection solution based on Veritas NetBackup™ software and a storage management solution based on Veritas Storage Foundation software™, with architectural and implementation assistance from Veritas Consulting (now Symantec Consulting Services), Vaidya felt that Symantec had the consulting expertise to help QIAGEN to pinpoint both short- and long-term business continuity requirements. At Vaidya's request, the Business Continuity Management Practice of Symantec Consulting Services developed a detailed request for proposal (RFP) showing how Symantec would conduct a comprehensive analysis of QIAGEN's business continuity infrastructure and operational processes.

Vaidya and Huetzen were pleased with the thoroughness and focus of the plan. “What really impressed us about the Symantec proposal was the insight the consultants had into our business,” notes Vaidya. “It came right to the point, explained the process step-by-step, and did not offer any extravagant options, which we found refreshing. As a result of a previous consulting engagement, we were aware of Symantec's knowledge and experience in the business continuity space.” In addition, wanting to deploy a software infrastructure capable of supporting a heterogeneous server and storage environment, Vaidya looked to continue leveraging Symantec data protection software. “Since our management had just announced the relocation of North American sales and marketing management and administration from California to Germantown, Maryland, business continuity was also a key reason for our decision to go with Symantec.” After his team had reviewed the proposal, Vaidya gave Symantec the go-ahead.

Building on a history of data protection success

The relationship between QIAGEN and Symantec (formerly VERITAS Software) dates back to the late 1990s, when Symantec partner Applied Computer Solutions, Inc.,

introduced QIAGEN to Symantec. Seeking to help QIAGEN deal with growing data volumes, Applied Computer Solutions offered Veritas Storage Foundation for storage management. “Applied Computer Solutions is joined at the hip with many of our technology vendors, including Symantec,” says Vaidya. “We very much value the long-term, strategic relationship that we've built with Applied Computer Solutions.”

In 2002, wanting to lower total cost of ownership (TCO) while improving overall system performance, Vaidya and his team embarked on exploring different options for standardizing backup-and-restore operations across enterprise-wide data center environments. With a backup-and-restore software infrastructure based on multiple software solutions, including Computer Associates ARCserve, Informix OnTape, as well as Veritas Backup Exec™, Vaidya believed he could affect operational and financial results by moving to a centralized environment.

Accomplishing this objective was not without its challenges, however. The next-generation data protection solution would need to support a highly heterogeneous environment: a server infrastructure consisting of Sun Enterprise servers running the Solaris Operating System and HP/Compaq servers running Microsoft Windows Server; a storage infrastructure comprised of Sun StorEdge disk arrays; and more than 10 different business-critical applications.

Pleased with the track record of Symantec software and the ability of Symantec to deliver a comprehensive solution consisting of product and services, QIAGEN selected Symantec as the primary technology provider for its next-generation data protection solution in early 2002. The heterogeneous support of Veritas NetBackup and the ability of Symantec Consulting Services to coordinate with other technology vendors for deployment, ongoing support, and problem resolutions were key consideration factors. Vaidya

summarizes the reasons for selecting the data protection solution from Symantec: “We wanted a vendor offering more than just a product. It was pivotal that the technology solution also include partner integration from the standpoint of consulting and ongoing support.”

Then, over a period of one month, Symantec Consulting Services worked with QIAGEN, along with teams from other technology vendors, to design and implement a data protection solution for backup and restore based on Veritas NetBackup. The solution centralizes all backup-and-restore operations for QIAGEN and provides vast functionality, including disk staging, parallel backup and restore, and multiplexed backup. QIAGEN is also taking advantage of the product’s support for synthetic backup, which consumes less space on the network and allows for quick restore using a single backup image.

Business continuity management using best practices

In August 2003, Symantec, once again coordinating with Applied Computer Solutions, submitted a final project proposal to Vaidya and his team. They made a final vendor selection in September 2003, chartering Symantec Consulting Services with providing an in-depth analysis of the company’s business continuity strategy. In addition to several architects, with specialized experience in business continuity, the team from Symantec Consulting Services included a project manager, a certified Business Continuity Planner, who used standards and best practices from the Project Management Institute to guide the project from inception to completion. Hugo Gordillo, network operations manager at QIAGEN, North America, also played a key role in working with Symantec Consulting Services, coordinating various project activities within QIAGEN.

Following project planning in October 2003, the first phase of the project was initiated in November 2003, which involved a series of business

SOLUTION AT A GLANCE

Business Drivers:

- Lower TCO for backup and restore, including operational efficiency gains and reduced costs
- Mitigate risks of catastrophic data loss

Technology Challenges:

- Consolidate from multiple backup and restore solutions to standardized, centralized environment
- Improve system performance
- Support for heterogeneous hardware and software environments
- Achieve rapid time-to-deployment for backup-and-restore and business continuity solutions

Solution

- Standardized software infrastructure solution for data protection and storage management

Symantec Products

- Veritas NetBackup™ Enterprise Server
- Veritas Storage Foundation™

Symantec Services

- Symantec Consulting Services, Business Continuity Management Practice
- Symantec Education Services
- Symantec Technical Support

Technology Environment:

- Applications: 10 business-critical applications supporting 10 different business units
- Server Platform: Sun Enterprise servers running the Solaris Operating System and HP/Compaq servers running Microsoft Windows Server
- Storage Infrastructure: Sun StorEdge disk arrays

Symantec Partner

- Applied Computer Solutions, Inc.

continuity management workshops. These brought together key stakeholders from different business units across the company in a roundtable discussion. During the roundtable discussion, various interdependencies and cross-functional synergies were identified and explored in detail. Subsequently, the operational and financial impact of potential interruptions to data availability was delineated. In December 2003, the consulting team from Symantec finalized the results of the workshops, including identification of Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO).

The second phase was initiated at the same time as the results from the first

phase were submitted to Vaidya and his team. This phase involved a technical and architectural review as well as gap analysis of the existing data protection infrastructure. A final assessment report from Symantec Consulting Services was delivered in January 2004. The findings included a Business Impact Analysis that provided a risk assessment profile of QIAGEN’s business drivers and business continuity issues. This analysis identified 10 important applications and 10 key QIAGEN business units with business continuity requirements. The assessment from QIAGEN also compared the operational and financial impact of system disruptions in order to establish RPO and RTO objectives for each business unit and

BUSINESS VALUE AND TECHNICAL BENEFITS

- 100% ROI achieved within 36 months via 25% lower TCO
- 30% to 50% faster backup time
- 25% to 30% growth in data volumes and 25% to 30% increase in backup volumes
- 25% improvement in IT staff productivity
- 33% faster time-to-deployment for business continuity solution with help of Symantec consultants

associated applications. RPO is the point in time to which data must be recovered to resume transaction, whereas RTO is the maximum elapsed time allowed before lack of business function severely impacts organizational operations.

As the Symantec Business Continuity Management consultants worked with Vaidya, Gordillo, and the QIAGEN team to prioritize data, they identified RPO requirements that ranged between no downtime and two days and RTO requirements that ranged from 24 hours to five days. The Symantec consultants also tracked and created an inventory of single points of failure in key IT processes and personnel skill sets, as well as recommended hardware and network connectivity options for achieving RPO and RTO requirements.

Trusted advisor delivers value-add solution

QIAGEN views Symantec as a trusted advisor on the basis that the technology leader has delivered unbiased, strategic support—both architecturally and operationally—related to its data protection environment. Vaidya explains: “One of the key strengths of Symantec Consulting Services is the ability of its consultants to examine an IT infrastructure and then make recommendations on how to redeploy existing resources to reach RPO and RTO targets. The objectivity of the Symantec consultants, including their ability to recommend a business continuity management infrastructure based on heterogeneous software and hardware environments, was pivotal in helping to establish a relationship built on trust.”

Once the team of Symantec consultants completed their analysis and developed their recommendations, they then worked with Vaidya and his team to fashion a comprehensive business continuity solution. QIAGEN had requested a multi-tiered recommendation, so the Symantec architects developed three distinct business continuity options for consideration. Option One, the most comprehensive, specified an RPO of less than 24 hours and RTO of less than 24 hours. It also necessitated an IT environment with both data protection and high availability requirements, with the latter including high availability clustering for server and storage environments. The former posited the need for primary and secondary data center locations, with the secondary site available for system failover in the event of application or data degradation at the primary data center location. Option Two stipulated an RPO of less than 24 hours and RTO of less than 48 hours, with IT requirements including real-time data protection using replication technologies but no high availability clustering. In particular, Option Two would allow QIAGEN to replicate data across its Wide Area Network (WAN), with the recovery site protection data. Option Three, the least aggressive recommendation, pinpointed an RPO greater than or equal to 48 hours. This option allows for tape backups and periodic tape shipments from the primary data center site to the recovery data center location.

“Symantec Consulting Services truly served as a trusted advisor. The [consultants] focused on our core initiatives, helping us to identify pressing vulnerabilities and then recommending exactly what we needed to align our IT and business requirements.”

Prashant Vaidya

Director of IT, North America
QIAGEN, Inc.

“Symantec Consulting Services truly served as a trusted advisor,” comments Vaidya. “In addition to core analysis, the consultants incorporated a wide range of third-party resources into their recommendations. Symantec focused on our core initiatives, helping us to identify pressing vulnerabilities and then recommending exactly what we needed to align our IT and business requirements.” Simply from a time-to-deployment standpoint, Vaidya estimates that the Symantec consultants were able to shave as much as three weeks off of the nine-week engagement—a 33 percent reduction.

Symantec Global Services: A successful track record

The Business Continuity Management consultants from Symantec Consulting Services built upon a legacy of successful services delivered by Symantec Global Services (formerly Veritas Services). Not only did QIAGEN tap Symantec Consulting Services for architectural and implementation assistance when migrating to a centralized, standard data protection software infrastructure in 2001, but the company also leveraged Symantec Education Services for instructor-led and online training courses on Veritas NetBackup and Veritas Storage Foundation software. “We solidified both short- and long-term success for the initial data protection deployment by helping to ensure that our IT staff possessed optimal knowledge of the Veritas software from Symantec,” notes Gordillo.

“The training our IT team received from Symantec Education Services helped enhance operational efficiencies while improving delivery to quality-of-service requirements.”

To help ensure high reliability, availability, and serviceability, QIAGEN has a Basic Support agreement from Symantec. Symantec Technical Support—the support arm of Symantec Global Services—delivers ongoing support to QIAGEN. Aspects of coverage include telephone support for single incident resolution, remote accessibility, and updates and patch releases. The support agreement also includes access to Email Notification Services to appraise QIAGEN of any relevant software upgrades and patch releases and product alerts and information; Support Newsgroups for collaborative interaction with other software users; and Web KnowledgeBase, an online repository of thousands of technical notes, documents, and whitepapers from experts in storage management. “The ongoing success of our data protection solution is tethered to our Basic Support agreement,” says Gordillo. “Symantec Technical Support is our fallback option for both reactively and proactively managing our data protection software infrastructure to optimal quality-of-service requirements.”

Standardization reaps tangible results

The next-generation data protection solution began delivering tangible results shortly after deployment. Standardization to a centralized backup-and-restore facility, including migration from CA ARCserve and other proprietary systems, helped improve backup time by 30 percent to 50 percent. The ability to manage its storage environment on one large tape versus multiple tape libraries is contributing to a 25 percent improvement in IT staff productivity alone. Overall, reductions in software licensing costs and improved operational

efficiencies helped Vaidya and his team to lower TCO by an estimated 25 percent, equating to a 100 percent return on investment within 36 months.

The new software infrastructure is proving highly scalable as well, accommodating a 25 percent to 30 percent growth in data volumes and a 25 percent to 30 percent increase in daily backup volumes since its deployment more than two years ago. “Over the short period of time that the data protection solution has been in production we’ve experienced exponential growth in data volumes—both in terms of the composite and the amount for daily backup,” notes Vaidya. “The Symantec software has scaled seamlessly.”

Recommendations already playing dividends

Outcomes of the business continuity recommendations are still being realized. Opting for a phased approach in deploying a next-generation business continuity infrastructure, Vaidya and his team are in the process of implementing Option Three. “One major benefit of the analysis by the Symantec Business Continuity Management Practice was that we extended our backup cycle from one week to two weeks, with plans to move to monthly backups,” cites Vaidya. “Our IT staff now spends less time managing our backup-and-recovery resources.” Indeed, Vaidya estimates that the IT staff is realizing a 25 percent improvement in productivity today. Vaidya explains: “The business continuity recommendations—architecturally and operationally—enabled our small IT staff to focus on building value-added applications and meeting new business requirements for our customers rather than spending time on developing a business continuity solution.”

“The business continuity recommendations—architecturally and operationally—enabled our small IT staff to focus on building value-added applications and meeting new business requirements for our customers rather than spending time on developing a business continuity solution.”

Prashant Vaidya

Director of IT, North America

QIAGEN, Inc.

Because of the successful business continuity solution from Symantec, including Veritas NetBackup, in its California data center, QIAGEN selected the same solution for its Maryland data center facility. Implementation planning for its deployment is underway. The latter will enable the company to deploy Disaster Recovery Option Three across all of its data center operations in North America.

For Vaidya, the key success factor was the flexibility that Symantec offered. “While Symantec is a well-established technology company, a sustainable business continuity solution is not just about technology. Symantec started with an understanding of our overall business requirements and then began making recommendations focused on actionable results and cost-effective outcomes. In that respect we are quite satisfied with what we received from Symantec.”