

## US PHARMACEUTICAL FIRM MANAGES DATA PROTECTION GROWTH

### BUSINESS OVERVIEW

This large bio-tech company headquartered in New England was founded in 1993 with a vision that still drives true today, to transcend the limits of medicine. The company believes that by applying the methods of leading science to the art of drug discovery, they will develop breakthrough products that will fundamentally change the practice of medicine for years to come.

### THE CHALLENGE

The company faced a number of issues as they looked at ways to improve their data protection strategy. Increasing data growth and the higher demands for longer periods of data availability were adding pressure to the existing backup and restore infrastructure. Questions were being asked about their existing backup and restore support contract as it struggled to meet the growing demands of the business.

To add to these challenges, the company was going through a round of SOX (Sarbanes Oxley) auditing and is also regulated by the FDA (Food and Drug Administration) on a regular basis. These external pressures have driven the IT organization to ensure proper data retention processes are in place across the organization. Other issues included:

- The previous support contract no longer met business needs. Escalating data growth had led to increasing backup and restore requirements as the supplier struggled to scale its service to meet these growing restore demands.
- The previous service was completely remote with no onsite support staff, which meant carrying out any restores involved large amounts of internal resources from the internal IT department,

something they had hoped the support contract would eliminate.

- An un-collaborated approach to problem solving between the supplier and the internal IT organization was leading to a lack of ownership for backup and restore issues and, in turn, exposing the business to unnecessary risk.
- A lack of standard operating procedures (SOPs) for regulated business environments meant the company was exposed to unnecessary risks in the event of not being able to recover auditable data.

### THE SOLUTION - HOW GLASSHOUSE HELPED

Massive data growth, fuelled by an increase in new regulations for data retention meant the IT organization needed a solution in place they were confident would scale to meet rising business demand for information availability over the next three years. This requirement opened up the opportunity for GlassHouse to provide a managed backup administration service which is made up of four key components:

- **Backup Reporting and Metrics Portal** provides the IT operation with a web-based system that monitors the success rates of the backups and restores, providing performance monitoring statistics on the infrastructure, as well as metrics on backup asset utilization. This information provides the IT operations with a consolidated view of the business with the ability to drill down by business unit or infrastructure component. Summary reports are sent to the client's backup management team on a weekly and quarterly basis.

- **Backup Quality Audit** provides tools that run a set of scripts that demonstrate consistency in the overall service to the IT organization. These audits, which include capacity and performance metrics for asset utilization and trending analysis, identify successful backup completions as well as provide outlines for a strategic roadmap for the complete backup and restore operations.
- **Remote Enhanced Incident Management** proactively manages any backup and restore issues that could impact any of company's critical business applications. To ensure continued round the clock protection the service includes 24 x 7 remote monitoring and assistance from the GlassHouse Service Operations Center (SOC), allowing the IT organization to offload operationally intensive tasks, such as incident management to the GlassHouse team.
- **Onsite Staff** provide the company with constant access to GlassHouse skills and resources. In such a competitive market place, it can be expensive to recruit, train and retain experienced storage staff. With additional pressures on the IT department to do more with less, justifying the cost of extra resources was challenging. Our on-site staff proactively engage with the in-house IT operations on a number of other projects in order to maintain consistent levels of data protection. For example, when new servers are added to the infrastructure, GlassHouse's on-site consultants work with the in-house team to ensure any new clients receive the same backup and restore service levels as the rest of the supported infrastructure.

To ensure consistency in the service, GlassHouse provides guaranteed service level agreements that include: backup success rates; incident response times; reporting and metrics; monitoring of portal availability; data restore times; and turnaround times to perform restores.

#### BEST PRACTICES

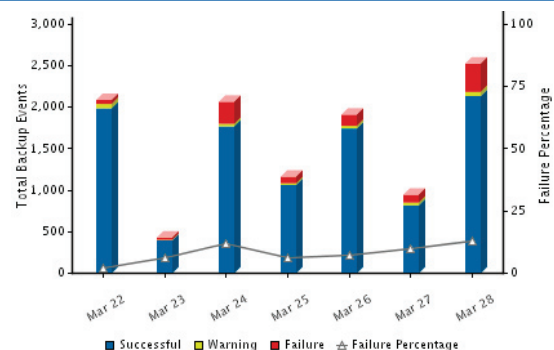
The Standard Operating Procedures and best practice procedures that have been introduced have resulted in significantly higher backup success rates and improved data protection. The backup

success rate has increased from 93% to 98% since GlassHouse began managing the infrastructure. Automation of key backup and restore processes has reduced the amount of manual processes that were leading to frequent user errors under the old support contract.

#### GLASSHOUSE PROVIDES VALUE

- The GlassHouse services are being delivered at the same cost as the previous supplier as well as providing onsite staff, which results in more services and better overall value.
- The company benefits from significantly improved backup asset utilization rates result in more predictable and more manageable backup hardware and software spending patterns.
- The monthly investment made with GlassHouse is scalable based on business demand, enabling the company to re-allocate spending in quieter business periods.

*A snapshot of the customer's environment before GlassHouse took over. (Average 7% daily backup failures)*



*A snapshot of the customer's environment after GlassHouse took over. (Average 2% daily backup failures)*

