

Developing a Business Case for Replication Assurance

June 2006

Executive Summary

Business case justifications are required for nearly all new purchases into IT. Different companies tend to place different values on product features based on their industry, size, internal operating procedures, or chargeback practices. Hence, any vendor attempt to build a universal business case for a product offering is difficult at best. A more rational approach is to provide customers with general discovery questions and business case building blocks. This paper discusses the build blocks for building a business case for Onaro's SANscreen Replication Assurance product. By examining the dimensions of return on storage, service quality, and compliance, customers can build a robust business case to justify the investment.

Return on Storage

Return on storage encompasses the category of hard financial savings that Replication Assurance would provide a company. Not all financial impact categories will be applicable for all customers. Chargeback schemes, budgeting processes, contractual commitments to other vendors all impact how much the theoretical savings map to actual savings according to a companies accounting practices.

Capital Cost Reduction

Replication Assurance reduces capital costs through recovery of orphaned LUNs and ports, matching of required replication services with actual replication services, and the enablement of chargeback.

Recovery of Orphaned LUNS

Orphaned LUNs and ports occur regularly in large storage environments as volumes are replicated or set up for replication and never actually used. SANscreen Replication Assurance will be able to identify orphaned replicated LUNs since these LUNS will no longer be associated with hosts or other replicated volumes. To determine the ROI from recovering orphaned LUNs, during the proof of concept the number of identified orphaned LUNs should be counted. The capital cost savings by recovering these LUNs can be calculated. This cost savings is both a one time cost avoidance savings but also an on going capital cost reduction. Each period, orphaned LUNs will be recovered enabling capital cost avoidance.

Chargeback

The second area for capital cost reduction involves the implementation of chargeback processes. Typically in replicated environments, the source data volumes are easily charged back to the host applications. However, replicated volumes add significant complexity to the charge back process. Tracing volumes from their replicated sites back to the host can be a full time job for several people in large environments. Only by viewing these volumes from a service viewpoint from the host can chargeback easily be initiated.

How much is charge back worth from a capital cost reduction standpoint? From Onaro's experience, implementing chargeback can reduce capital costs by a minimum of 10%. Once business units are made aware of their storage costs beyond the cost of source data stores, storage use drops precipitously. The 10% estimate is clearly subjective. Comparable organization specific experience should be applied to determine the cost savings from chargeback.

Operating Cost Reduction

Operating cost reduction occurs from reduction in semi-annual DR exercise labor costs and reduction in general change management operations.

Annual Disaster Recovery Labor Cost Reduction

Most companies conduct an operational check of disaster recovery systems on a semi-annual basis. Most of these tests are accompanied by significant man hours of preparation time followed by days of trouble shooting during the actual test. Replication Assurance reduces the amount of labor operating expense by insuring the disaster recovery services are operating in accordance with the required service levels before the disaster recovery drill. During the drill, Replication Assurance will assist in any trouble shooting, if trouble shooting is necessary at all. In general, a safe assumption is a reduction of 50% of labor hours for each disaster recovery drill.

Replication Change Management

The second area of operational cost savings is related to reducing the time and expense incurred for changes to the replicated environment. Similar to the operating costs incurred by planning and implementing change in a non-replicated environment, costs for change management in a replicated environment can be an order of magnitude higher. Replication Assurance assists in this change management process by providing a solid view of the replication services delivered. Only by starting from a solid foundation can any type of changes occur without storage interruption. Labor cost savings from change management associated with replicated environments has been estimated to be 10% of the total labor costs for the environment.

Return on Assets

Given the asset intensive nature of storage, maximizing the return on this investment is an important financial measure. For replicated environments, specifically disaster recovery environments, the return on assets (ROA) is somewhat binary. Either the environment operates in a disaster or it does not. Either the data is correctly replicated and made available or it is not.

The investment for replicating environments for disaster recovery is very high. Duplicating the arrays and the host environment is an extensive investment. Add in the cost of the data center and the labor costs to maintain both environments and the costs go even higher.

The challenge is to verify that the environments are configured properly. Replication Assurance provides an insurance policy that the investment cost of building the DR environment will yield the right ROA.

How much is this insurance worth?

The easiest formula is to take the cost of Replication Assurance and divide it by the fully loaded cost of the replicated array, SAN and host environments. In general, this cost is less than 2% of the total investment. So put another way – for an incremental 2% of the investment, the ROA for the replicated environment can be significantly boosted.

Service Quality

Return on storage drives hard financial savings. Measuring improvements to service quality generally will not drive hard financial results but may be just as important if they line up with core business objectives for the storage team or IT group.

The largest area of service quality improvement revolves around the reduction in business continuity and disaster recovery risk. The simplest way to build the business case around these areas would be to examine the original business case built for business continuity or disaster recovery. In most cases, Replication Assurance adds a small percentage to the overall investment yet may be the only way to insure that the service quality requirements are met.

Other service quality metrics revolve around replication where data warehousing is involved. Since users expect data warehouses to have fresh data based on agreed upon freshness dates, missing these dates violates service level agreements. Replication Assurance can help meet data warehouse refresh goals.

Compliance

Compliance is the third building block for building a business case for Replication Assurance. Similar to service quality, however, many of these compliance figures will be soft numbers. There are several compliance oriented business case justifications.

The first is maintaining the disaster recovery RPO or recovery point objective. Internal corporate governance and sometimes even external government regulations will stipulate the required RPO. Calculating and maintaining the RPO is extremely difficult without Replication Assurance. There are potential labor costs savings here if the organization has someone working compliance part or full time. If any business cases have been made recently around compliance or are in the process of being made, adding Replication Assurance to the business justification once again is usually a small percentage of the overall investment. However, without Replication Assurance, any investment in compliance may be incomplete.

Maintaining accurate accountability of data access paths and replicated volumes is critical to maintain corporate governance rules around data control. The recent incidents of compromised corporate data highlights this risk. Replicated environments increase the risk of unauthorized data access. The more locations where data is stored, the greater the number of possible points

of access. Replication Assurance provides visibility into the location of all replicated data and highlights any unauthorized host access to this data.

In addition, replicated volumes pose a security risk for other reasons. Once the data is replicated, maintaining control of the replicated data is critical. A replicated volume once created contains recoverable information until properly erased. Understanding which replicate copies have been created is critical to maintaining control of the data and preventing an orphan volume populated with data surfacing in an authorized location.

Conclusion

Business case justifications are required for nearly all new purchases into IT. When building a business case for SANscreen Replication Assurance, examining the return on storage, compliance and service quality areas will provide data for the business justification. Strict financial justification can be determined by examining potential reductions in capital costs, operating costs and return on assets. Service quality improvements and compliance requirements can be used to build the financial justification especially if there is current investment or corporate business objectives aimed at these areas. By examining all areas, a robust business justification can be created for SANscreen Replication Assurance.