IRON MOUNTAIN®

WHITE PAPER

LIVEVAULT®

LiveVault®

HOW TO MEASURE THE ROI OF CLOUD DATA PROTECTION

Contents

EXECUTIVE SUMMARY

The goal of server backup and recovery is to ensure that a company can recover from varying degrees of failure, from the loss of individual files to a disaster affecting an entire system. Success is measured by how quickly the company can recover (Recovery Time Objective or RTO), as well as by how small the loss of worker productivity is (Recovery Point Objective or RPO).

A recent study shows that a majority of mid-sized companies do not meet their own RTOs and RPOs for recovery of their most critical server data: databases, financials, and email messages. Many of these companies are seeking alternatives to tape backup, because independent analysts confirm that more than 50 percent of all attempted recoveries from tape fail due to errors in the backup process. In fact, the percentage of total data capacity stored on near-line tape systems declined from 48 percent in 2007 to just 27 percent in 2010 ("*Data Protection Market Trends*," John McKnight and Mary Johnston Turner, Enterprise Strategy Group, January, 2008).

Cloud backup and recovery services for servers enable small- to mid-sized companies, and remote offices of larger companies, to reliably meet their RTOs and RPOs. They help protect critical server data at a lower cost than traditional tape systems that require onsite IT professionals to operate and maintain them.

METHODS FOR CALCULATING ROI

In this paper, we examine the profitability of reducing operational costs by the investment in cloud security – as well as additional soft benefits. In some companies, additional components of ROI calculations for technology projects include:

- Net Present Value
- Opportunity Cost
- Payback Period

It is important to check with Finance on practices in your company and, if needed, work with Finance to get the additional data you need (such as discount rate or internal rate of return) to adequately present your case. For more information on these methods consult online resources such as www.investorwords.com.

This white paper helps managers demonstrate the profitability of reducing operational costs in server backup and recovery through investment in cloud server data protection (subscription), rather than traditional backup methods. Comparative cost categories used in calculating this ROI are summarized in a convenient checklist. These include capital costs of hardware and software as well as ongoing monthly costs for maintenance, media, labor, and offsite storage of backup data.

INTRODUCTION

Having researched the benefits of cloud data protection for your organization, you now must approach management for funding. How do you build a business case that illustrates a compelling return on investment (ROI) by moving to the regular subscription fees of a cloud model for server backup and recovery? What is the profitability of a cloud model, compared to the cost of current methods (included in the operations budget) or to the costs of alternative onsite hardware and software purchases, which appear to be onetime only?

This paper presents a methodology that will help you demonstrate not only the technological benefits of the service that you are proposing, but also the business requirements, financials, and "soft costs" that make a compelling argument for moving to cloud data protection.

First, we summarize the key issues that drive the consideration of alternatives to current methods of server data protection—the most important being the achievement of Recovery Time Objectives and Recovery Point Objectives to minimize loss in worker productivity due to process or system failure.

Next, we identify the costs of current methods (and other alternatives) against which management will want to evaluate your proposal for cloud data protection. These include, for example, the cost of either continuing current methods of backup or "beefing them up" with investment in more onsite data protection software and hardware.

Finally, we help you estimate the cost savings of cloud data protection. With these estimates, you can analyze the ROI of moving to cloud data protection and show the profitability of reducing operational costs by the investment in a cloud implementation. In addition, you can show additional soft benefits that, although difficult to quantify in financial terms, have very real value to a corporation and should be considered in any data protection proposal.

KEY ISSUES IN SERVER DATA PROTECTION

Small to medium businesses, and the remote offices of larger enterprises, are increasingly turning to cloud backup and recovery services for server and application data protection. The major factors driving cloud backup are:

- An increasingly distributed workforce depends on 24x7 access to business data stored on servers. Maintaining their productivity requires a solution that meets Recovery Time Objectives and Recovery Point Objectives.
- The price and predictability of a secure cloud subscription model are attractive compared to more costly and cumbersome tape backup systems. The subscription model is also a more scalable solution that helps IT to do "more with less."
- The challenges are increasing of meeting more stringent compliance requirements for protecting private information and ensuring business continuity.

ACHIEVING RTOS AND RPOS FOR MAXIMUM PRODUCTIVITY

The information and applications required to run a small- or medium-sized business, or the remote office of a larger company, run on a variety of server platforms, ranging from physical systems running Windows®, Unix®, and Linux® to virtual servers (such as VMware®). These platforms may be multi-purpose, or may be designed to host specific applications (such as Microsoft Exchange or SQL Server). Unlike desktops and laptops, servers typically run 24x7 to provide access for distributed users, frequently in distant locations.

Servers store a wide variety of data types from different applications. Server data can be classified by its impact on business operations:

- Mission critical: producing revenue or customer-facing
- Business critical: supporting cross-organization functions
- Operationally critical: important to individual departments

The goal of backup and recovery is to ensure that a company can recover from varying degrees of server data failure (from individual file loss to an entire system) in the optimum timeframe (RTO), as well as to recover a version of the data that results in minimal loss of productivity (RPO).

For small to medium business and remote offices, cloud server backup and recovery services help companies meet these two objectives better than traditional tape backup methods. Such traditional methods require onsite IT professionals to run and maintain them, as well as to access them to recover from server failure. Cloud services support a wide variety of server platforms and data types. Also, cloud server backup and recovery services entail little or no upfront cost, with predictable monthly costs over the course of the service contract.

SATISFYING COMPLIANCE: CHALLENGED TO DO MORE WITH LESS

Meeting RTOs and RPOs for critical business information on servers places additional burdens on those responsible for backup and recovery. During times of economic downturn, companies may have caps on technology-related spending and staffing.

Ironically, economic downturns may actually increase the effort necessary to adequately protect server data. As corporations cut back on server replacements, they hold on to hardware longer. This may increase the types of deployed configurations to support (older as well as newer platforms) and the volume and types of qualification testing required. Server platforms in new locations added through

acquisitions or mergers also have an impact on backup and recovery support costs, frequently just when IT is being asked to "do more with less."

Though difficult to quantify, the risks of non-compliance, actual data loss, or breaches represent potentially significant hard-dollar costs to the company. According to Faulkner Information Services, 50 percent of businesses that lose their data due to disasters go out of business within 24 months, and, according to the US Bureau of Labor, 93 percent are out of business within five years ("*Is Your Company Prepared to Recover From an IT Disaster?,*" Paul Chisholm, Certification Magazine, February, 2008. http://www.certmag.com/read.php?in=3310).

As a result, IT is taking on an ever-greater role in designing and implementing regulatory compliance procedures and systems. These systems protect sensitive data (private and other), flag unusual or non-compliant activities, produce documents and records for audit purposes, and help ensure business continuity.

Cloud services can relieve much of the burden of server data protection—both backup and recovery requirements—by offloading these functions to the service provider's staff and resources. These services automatically transfer critical data offsite and offer better response time for recovery, at less expense, while providing greater security for information through encryption in transit and in storage.

Regulations make no exceptions about where server data resides. Beyond data privacy obligations, there are additional regulations governing disaster recovery (DR) and business continuity requirements. The Sarbanes-Oxley Act (SOX) of 2002 makes specific mention of continuity procedures. For the financial industry, business continuity is singled out in regulations endorsed by the Security and Exchange Commission (SEC), such as NYSE Rule 446 and NASD Rules 3510 and 3520 ("*Rules Widen the Scope on Business Continuity,*" Steve Stanek, KnowledgeLeader contributing author, November, 29, 2004. These rules were initiated in the aftermath of September 11, 2001, when NASD surveys indicated many of its member companies were ill-prepared with basic business continuity procedures.). In Europe, disaster risk management and continuity are addressed by Basel II, or The New Capital Accord, among other country-specific regulations.

Data regulations generally allow for "no excuses" where information resides, whether paper or electronic, in a data center or on servers in remote offices. This precedent has been made clear in the US through various rulings concerning the Federal Rules of Civil Procedure (FRCP), specifically a series of rulings in Zubulake vs. UBS Warburg in 2003-2004. The court not only ruled "*the defendant to produce, at its own expense, all responsive email existing on its optical disks, active servers, and five backup tapes,*" but later, having found several of these tapes to have been destroyed, issued sanctions against the defendant (and counsel) for not adequately implementing a legal hold on the data (A summary and the actual rulings in *Zubulake vs. UBS Warburg* can be found at: http://www.krollontrack.co.uk/zubulake/).

In contrast, providers of cloud data protection services allow businesses to automatically assign the appropriate retention period to different types of data,

reducing error in meeting compliance regulations. Services with historical catalogs allow organizations with minimal technical staff to meet discovery requirements faster and more accurately than by using tape solutions.

One of the primary measures of compliance is consistency across an organization. Compliant data protection procedures must be demonstrably consistent in all locations. This is hard enough to accomplish within a centralized operation, and even more challenging with servers distributed in remote offices. Use of cloud server data protection from a global service provider, employing consistent procedural best practices across their customer base, helps companies demonstrate consistency in their data backup and recovery processes.

CLOUD DATA PROTECTION IS UNIQUELY QUALIFIED

The previous section introduced a number of ways that cloud data protection enables IT to focus on managing information and keeping workers productive, rather than on managing backup and recovery tasks in a diverse and distributed infrastructure (Suggested by *"Market Overview: Backup Software-as-a-Service,"* Stephanie Balaouras, Forrester, February 20, 2008.)

- Backups are completely automated. The vendor, rather than IT, takes on most of the responsibility to ensure the success of backups, restores, and prevention of data loss.
- Security is maximized. Data is immediately stored offsite, with encryption ensuring data privacy in transmission and in storage.
- Demonstrable, consistent best practices in data protection are in place globally and maintained by the vendor, according to the rules of the customer, to accommodate variations in regional environments.
- The cost and effort of maintaining, updating, and extending the infrastructure for data protection is borne by the service provider rather than the customer, which is especially important when extending data protection systems to remote offices.

An cloud data backup and recovery service can increase the coverage and frequency of automatic backups with minor impact on IT-related capital expenditures and operating expenses. Broader, more frequent, and more consistent protection reduces the risks to worker productivity, as well as the risk of repercussions for non-compliance.

The immediacy and comprehensive nature of cloud backup can also address Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) within a DR or business continuity plan. Though a majority of companies do establish their own RTO/RPO goals, few feel that they consistently achieve their objectives (Iron Mountain-sponsored research, September, 2008.). Cloud data protection moves data offsite immediately, and recovery from the vendor depends only upon the capability to receive the data in a "hot-standby" facility or other data center.

The following sections help companies identify and assign value to these cost categories. These costs can then be incorporated in a Return on Investment (ROI) analysis.

CALCULATING THE COSTS: TAPE BACKUP SYSTEMS

Many companies continue to back up server data to tape—and continue to invest in these solutions. With tape-based backup and recovery, IT is responsible for the following tasks:

- Backing up to a tape-based system, then storing the tapes onsite or transporting them to offsite storage. In a remote office, non-technical staff may be required to perform this work.
- Recovering data from tapes for restoration to end users or in response to discovery requests.

When preparing the business case showing the ROI of moving to cloud data protection, you must document the costs of a tape-based backup and recovery system. These cost categories should include:

- Tape backup and recovery software
- Software implementation, maintenance, and technical support
- Tape backup hardware, maintenance, and media
- Labor, whether performed by in-house staff or by contracted services
- Offsite backup tape pickup, storage, and maintenance

All of these costs increase the Total Cost of Ownership (TCO) for each server (at a central location, as well as remote offices) and are described briefly in the sections below. They should be carefully documented and fairly represented in order for management to evaluate the ROI of subscription fees for an cloud data protection service.

TAPE-BASED BACKUP AND RECOVERY SOFTWARE

In calculating the total cost of software solutions designed to back up server data to tape, it is important to include all licenses required. These may include the following:

- Backup agent software (for each server protected)
- Database server agents (one per database server protected, such as, Oracle® or SQL Server)
- Open file managers (software specifically designed to back up files that are open)
- Plug ins for other types of servers (such as, Microsoft Exchange)
- Other add-ons or extensions required to support unique needs in your server environment (such as encryption software, if not included in the backup software license, to protect tapes being shipped offsite)

As a capital expense, the cost of software licenses may be depreciated over a specified number of years, in keeping with a company's accounting practices.

IMPLEMENTATION, MAINTENANCE, AND TECHNICAL SUPPORT

Implementation of new tape backup software involves a certain number of hours (perhaps days) incurred by internal (or third-party) staff to install, set up, integrate, configure, and train staff on backup and recovery procedures.

Annual software maintenance and support fees may be charged as a percentage of the software cost or as a flat fee. However, tracking down and installing fixes for bugs, and communicating with the vendor technical support team, should also be factored into the TCO of software. In addition, the ongoing labor costs of upgrading backup and recovery software, especially software that has been customized, must be calculated.

When purchasing software licenses, it's important to consider where the software is in its life cycle—how many revisions has it gone through?—and to anticipate that, at some point, it may be necessary to purchase a major upgrade, or even a replacement product, when the software reaches end-of-life. This will entail not only additional direct costs, but the cost in productivity of user downtime.

TAPE BACKUP HARDWARE, MAINTENANCE, AND MEDIA

Hardware for onsite backup systems may include automated tape libraries, tape drives, tape cartridges, or other media ("*Market Overview: Backup Software-as-a-Service,*" Stephanie Balaouras, Forrester, February 20, 2008)—and may also require additional memory for each server being protected, as well as additions to network infrastructure. Capital costs may be depreciated over the life of the hardware, typically 36 months.

As with software, hardware maintenance may be charted as a percentage of the total hardware costs (for instance, 15 percent). Alternatively, it may be necessary to track the warranty periods for different servers supported and estimate the annual support contract post warranty—estimating maintenance cost as an annual dollar amount.

Media for backing up server data should also be calculated with unit cost (for instance, $50 per tape) multiplied by the number of tapes required to meet RTOs and RPOs. For calculating cost over time, tapes are typically replaced each year.

LABOR ASSOCIATED WITH TAPE-BASED SYSTEMS

The overall goal of this part of an ROI analysis is to define the annual cost of the time spent protecting server data, and for achieving target RPOs and RTOs. However, the total should also include the productivity of those who use the data protection. The following support cost categories and factors should be considered:

LABOR ESTIMATES AND RATES: Determine the burdened hourly rate for the direct labor of in-house staff. Note that there may be different internal rates applied, depending upon which members of the IT staff perform a specific type of function.

- For ongoing daily tasks, estimate the hours per month for tasks required to protect a single server, such as running backups, tape management, reviewing logs, and tracking down causes for backup errors.
- Next, project the hours spent per month recovering or restoring files for users (both end users and requests for discovery).

- Some categories of tasks are performed on a periodic basis, for example, performing functional tests to validate that backups run correctly and that data can be restored an acceptable amount of the time.

Some companies contract with outside vendors to run tape backups. This does not include the cost of offsite tape storage and maintenance, covered below.

NUMBER OF SERVERS PROTECTED: Record the current size (numbers), growth rate, and variety of platforms and applications currently installed to use for labor estimates. As corporate data grows, so will the support requirements for additional servers to hold the data. Remember to include servers in remote offices.

SERVER MIGRATION COSTS: A server has a life cycle of approximately 36 months. Effectively, this means that one-third of an organization's servers must be replaced every year. For every replacement, technical staff must migrate user data, applications, and custom settings from the old system to the new one. The process varies within organizations, but the overarching goal is to minimize downtime and bring workers back online as quickly as possible.

Determine the time spent by technical staff (and end-users) in a typical computer migration, and the labor rate of the staff performing the operation. Using the rule of thumb of a 36-month lifecycle, project the annual cost of migrating one-third of the organization's desktop or mobile systems.

"SOFT" COSTS: There are "soft" costs that reflect user downtime and loss of productivity. Work with Finance to determine the burdened cost for one hour of lost time using an average for employees regularly using server data.

OFFSITE BACKUP TAPE PICKUP, STORAGE, AND MAINTENANCE

If your company uses a service to pick up backup tapes for offsite storage, estimate the service costs based on the frequency of pickup, costs of storage, and charges for maintaining your backup tape collection. Include a reasonable estimate for the number of times you typically need to request a recovery tape during one year.

THE COST SAVINGS OF CLOUD DATA PROTECTION

Cloud data backup and recovery services are uniquely suited to address server data protection and offer the following benefits:

- Backup is completely automated.
- Freed from performing backups, IT personnel can become better aligned with business goals.
- Server data moves to an offsite location.
- The service leverages the vendor's infrastructure and expertise.

The sections below detail the cost efficiencies of an cloud data protection service.

SAVING SOFTWARE LICENSING COSTS

In the cloud security model, a monthly service fee is charged for each server protected, rather than the capital cost of acquiring software licenses for specific servers.

Some cloud services include the protection of a wide variety of platforms, email, and databases in their subscription. However, as with licensed software for tape backup, some cloud service providers also charge separately for agents and plug-ins, such as for open file support.

SAVINGS IN IMPLEMENTATION, MAINTENANCE, AND TECHNICAL SUPPORT

There are no costs for implementing cloud security data protection solutions, aside from a company's time in deciding which types of files to back up, how often to back them up, and how long to retain them. Any costs to manage the life cycle of the backup and recovery software used in the service (including fixes and upgrades) are borne by the service provider, rather than its customers. It is also worth noting that there are additional benefits in end-user uptime, because most cloud backup and recovery services are engineered to minimize performance hits during backup by using snapshots, filters, and delta engines.

SAVING BACKUP HARDWARE, MAINTENANCE, AND MEDIA COSTS

There is no hardware cost involved in cloud backup and recovery services, unless you elect to use an optional additional local storage appliance for even faster automatic recovery. The service provider bears the cost of the storage devices and infrastructure, now and in the future, as its customers grow.

Storage fees for your backup data (per your backup schedule and data retention rules) are included in the monthly subscription fee. Service providers are incented to seek increasingly less expensive forms of storage (such as cloud storage) to keep their own—and their customers'—costs low. Economies of scale are also passed on to customers in the form of lower, more competitive rates.

SAVINGS ON LABOR

LABOR ESTIMATES AND RATES: The monthly subscription fee for the level of service and amount of storage that fits your requirements typically includes 24x7 technical support by staff specializing in backup and recovery.

Many (though not all) service providers offer Service Level Agreements that ensure successful recovery. However, data on backup tapes is often unrecoverable. Independent analysts confirm that over 50 percent of all recoveries will fail because of errors in the backup process ("*Data Disaster Recovery for Small and Medium Businesses*," Iron Mountain White Paper, 2006).

Unlike the laborious task of tracking errors in tape-based backups, cloud services provide automatic detection of problems at any stage of backup or recovery. Service provider staff initiates corrective action and proactively notify customers, often through email alerts. A web-based management portal allows customers to manage and monitor the entire backup and recovery process and audit users anywhere and anytime.

NUMBER OF SERVERS PROTECTED: As noted previously, most cloud data protection services will charge per server protected—but they also offer discounts as the amount of storage of centralized backup data increases.

SERVER MIGRATION COSTS: An cloud data protection service that includes full system backup, in addition to data backup, reduces the time required to migrate user systems from hours to minutes. This is an important feature to consider in evaluating an cloud service provider—many service providers backup and restore only data, not full systems. A conservative estimate of 50 percent savings over current methods of computer migration would be reasonable.

SAVING OFFSITE BACKUP TAPE PICKUP, STORAGE, AND MAINTENANCE COSTS

With automatic, immediate backup to an offsite, highly secure location, there is no additional cost to transport data offsite. In addition, cloud service providers typically use the highest security possible, employing encryption in transit, storage, and retrieval.

However, it is important to scrutinize the physical security of the data centers of the service provider (just as it is with a tape vaulting company). The vendor should possess a high-level security rating and all data should be mirrored at a second location.

ADDITIONAL BENEFITS OF CLOUD DATA PROTECTION

There are additional benefits of cloud data protection that are difficult to quantify in hard dollars, but should be included in a credible business case analysis. Broadly stated, these are improved compliance capabilities, and the benefits of leveraging the data protection commitment and expertise of the cloud vendor.

IMPROVED GOVERNANCE, RISK, AND COMPLIANCE (GRC) PROGRAM

Cloud data protection applied consistently across all server locations with minimal requirements for technical staff interaction can go a long way toward improving a GRC program. The immediacy with which data is moved offsite to a secure location, and the ease with which this data can be retrieved, can also make RTOs/RPOs far more achievable.

The costs of data loss or breach can be significant, including damage to a corporate brand, loss of shareholder confidence, and concerns about data privacy from customers and employees. This risk is driving firms to not only back up their data to protect against data loss, but also to employ automated endpoint security solutions that combine intelligent encryption with enterprise-controlled data destruction.

Integrating server backup with legal discovery and review tools can help reduce legal discovery costs, and enable better planning for early case assessments, perhaps even helping to avoid legal action.

LEVERAGING THE CLOUD DATA PROTECTION VENDOR

With an cloud server data protection service, IT resources can be better aligned with business goals, such as implementing a new CRM system, or updating an old financial or accounting system. Though difficult to quantify, this value also should be emphasized in any ROI presentation.

ANALYZING THE ROI OF CLOUD SERVER DATA PROTECTION

The table on the following page summarizes the costs and savings categories in comparing tape-based, onsite server backup and recovery with an cloud service. The ROI, the savings associated with the reduction of operational costs over time (typically annualized), can be clearly demonstrated for cloud data protection services.

METHOD OF DATA PROTECTION		
CATEGORIES FOR CALCULATING COSTS AND SAVINGS	TAPE-BASED SERVER BACKUP AND RECOVERY (current system or proposed new system)	CLOUD SERVER BACKUP AND RECOVERY MONTHLY SUBSCRIPTION FEE
BACKUP AND RECOVERY SOFTWARE	Capital costs of software (to be depreciated) include: • Backup agent software (for each server protected) • Database server agents (one per database server protected, such as Oracle or SQL Server) • Open file managers • Plug ins for other types of servers (such as Microsoft Exchange) • Other add-ons or extensions required to support unique needs in your server environment	• No capital costs for customer – service provider bears all capital costs of software • Monthly subscription includes: unlimited use of backup and recovery software as a service for all servers, with data stored in a central location, accessible anywhere, anytime Note: Be certain to verify that the service provider does not charge additional fees for protection of specific types of data or platforms
SOFTWARE IMPLEMENTATION, MAINTENANCE AND TECHNICAL SUPPORT	• Number of servers supported • Burdened hourly rate of IT or 3rd party hourly charges for implementation hours • Hours downloading fixes and upgrades • Software maintenance fees • Soft cost of user down-time during scheduled maintenance	• Immediate implementation • No software maintenance or technical support costs • No charges or downtime for upgrades
BACKUP HARDWARE, MAINTENANCE AND MEDIA	• Capital cost of tape drives, auto loaders and extra server memory (to be depreciated) • Annual hardware maintenance fee • Annual cost of media	• No capital costs to customer—costs borne by service provider • Predictable license and service pricing based on the number of GBs or servers of protected data • No annual hardware maintenance or media fees
LABOR, WHETHER PERFORMED BY IN-HOUSE STAFF OR CONTRACTED SERVICES	• Burdened hourly rate of IT times hours (or service charged by third party) to perform: • Daily backup tasks • On-demand data recovery from tape • Server migration	• Includes automated data protection on scheduled or continual basis • Includes immediate recovery anytime, anywhere • Includes 24x7 alerts and monitoring • Includes restoration of complete server online to any location, or from an optional onsite appliance
OFFSITE BACKUP TAPE PICKUP, STORAGE AND MAINTENANCE	• Cost of 3rd party service to get backup data offsite, store, and maintain it for a year	• Includes immediate offsite protection • Includes encryption of data in transport and storage • Includes assured, immediate, granular data recovery Note: Be certain to verify that service provider offers catalog of historical version and flexibility of retention schedules
TOTALS	• Total monthly cost of tape backup for daily server data backup, protected offsite on a periodic basis with 50-60 percent reliability of successful recovery from tape	• Total monthly cost of cloud continual server backup and recovery stored immediately offsite with assured, secure recovery 24x7

SUMMARIZING THE RETURN ON INVESTMENT OF CLOUD BACKUP AND RECOVERY. By totaling the cost of a tape-based backup and recovery solution, and comparing it to savings realized by moving to cloud data protection, you can express the profitability of reducing operational costs (ROI) as: Annually, the company will spend (price of the annual cloud subscription) to realize (savings over tape-based backup and recovery)

There are more obvious cost benefits in leveraging the vendor's existing infrastructure for storing data (with costs spread over thousands of customers) than making one's own capital investment and dedicating resources. But continued savings are also realized as service providers themselves invest in new capacity and technology to remain competitive. It is the vendor who incurs the variable capital and operational expense necessary to adapt their infrastructure to meet the requirements of new applications and platforms. Their customers enjoy more predictable costs, at a fraction of these expenditures, through utilizing economies of scale.

As they free up IT staff, fully functional, mature web-based tools provided by cloud data protection services allow staff to better monitor and manage the quality of server data protection across the company. The experienced and committed service provider is incorporating new tools and adding value to their products. An example might be the automatic classification of distributed enterprise data, classification more granular than, for example, Tier 1, Tier 2, and Tier 3. This would allow greater efficiencies throughout the data management lifecycle, from optimizing storage for critical data to searching for and recovering data as part of eDiscovery.

CONCLUSION

By documenting specific cost categories in tape-based methods of onsite backup and recovery, IT managers can build a compelling case for investing in an cloud server data protection service. Careful examination of all these costs shows the ROI—the profitability of reducing operational costs—of cloud services over tape-based backup and recovery methods.

While harder to quantify, additional benefits have very real value to a corporation. These include a stronger Governance, Risk, and Compliance (GRC) Program, mitigation of data risk, and stronger DR or business continuity plans. There are also ongoing benefits derived from leveraging the resources of the cloud data protection vendor, including taking advantage of the vendor's investment in technology and data protection expertise, and better alignment of IT resources with strategic business goals.

For additional assistance on assessing costs and identifying additional benefits in your specific business environment, contact Iron Mountain Digital at 800-899-4766 (option 2).

IRON MOUNTAIN®

120 Turnpike Road, Southborough, MA 01772

Iron Mountain Digital is the world's leading provider of Storage-as-a-Service solutions for data protection and recovery, archiving, eDiscovery, and intellectual property management. The technology arm of Iron Mountain offers a comprehensive suite of solutions to thousands of companies around the world, directly and through a worldwide network of channel partners.