

## How to Measure ROI for Online PC Backup and Recovery

### EXECUTIVE SUMMARY

IT managers and business professionals are increasingly drawn to the cost effectiveness of online services to back up and recover corporate data distributed throughout their business on desktops, laptops, and mobile devices. They face the challenge of demonstrating the return on investment (ROI) of making the change from the current methods for protecting data, managing risk, and keeping a distributed workforce productive.

This White Paper helps managers to build a compelling business case for deploying online data protection services rather than continuing current methods of backup and recovery – or implementing other onsite alternatives. In order to show the profitability of reducing operational costs through an investment in Software as a Service (SaaS) backup and recovery, an ROI analysis must:

- Present the changing landscape of business data management, and the challenges this presents for protecting desktops and laptops throughout an organization
- Identify all the costs of current methods (and other alternatives) of data protection
- Estimate the cost savings of online data protection over both current and alternative methods

This paper also highlights additional soft benefits; these are difficult to quantify yet have very real value to the corporation in evaluating any data protection strategy.

Finally, included in this paper is a checklist of cost categories for comparing current methods of savings for adopting an online data protection service.

## **TABLE OF CONTENTS**

<b>Introduction</b>	3
<b>Changing Landscape of Business Data Management</b>	4
Increasingly distributed and mobile workforce	4
Distributed data management: Challenged to do more with less	5
Regulations make no exceptions for distributed data	6
Online data protection is uniquely qualified	7
<b>Calculating the Costs: Current and Alternative Methods of Data Protection</b>	8
End-User Support Costs	8
Costs for Alternative Data Protection Solutions	9
Computer Migration Costs	10
Cost of Asset Loss	10
Estimated Cost of Data Loss	10
<b>The Cost Savings of Online Data Protection</b>	11
Savings in End-User Support	11
Savings Over Alternative Data Protection Schemes	11
Computer Migration Savings	12
Savings in Asset Loss	12
Savings in Data Loss	12
<b>Analyzing the ROI of Online Data Protection</b>	13
<b>Additional Benefits of Online Data Protection</b>	14
Improved Governance, Risk and Compliance (GRC) Program	14
Leveraging the Online Data Protection Vendor	14
<b>Conclusion</b>	15

## INTRODUCTION

Having researched the benefits of online data protection for your organization, you now need to approach management for funding. How do you build a business case that illustrates a compelling return on investment for moving to ongoing subscription fees in a SaaS model for backup and recovery? What is its profitability over the cost of current methods (included in the operation budget) or costs of alternative onsite hardware and software purchases that appear to be one-time only?

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

First, we summarize the changing landscape of business data management that drives the consideration of alternatives to current methods of data protection – namely, the increasingly distributed workforce and growing importance of data residing on desktops and laptops.

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

Finally, we help you estimate the cost savings of online data protection. With this data in hand, you can analyze the ROI of moving to online data protection and show the profitability of reducing operational costs by the investment in a SaaS 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.

## METHODS FOR CALCULATING ROI

In this paper, we examine the profitability of reducing operational costs by the investment in SaaS — as well as additional soft benefits.

In some companies, additional components of ROI calculations for IT 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 (discount rate, internal rate of return, etc.) to adequately present your case.

For more information on these methods, consult online resources such as [www.investorwords.com](http://www.investorwords.com).

## **CHANGING LANDSCAPE OF BUSINESS DATA MANAGEMENT**

Crucial to an online data protection business plan is a clear description to management of the costs and risks to supporting productivity and data protection in a more distributed workforce. Distributed data – on desktops, laptops, and mobile devices – presents different challenges to IT. It is critical to describe how an online data protection system more efficiently addresses these unique challenges.

### **Increasingly distributed and mobile workforce**

For continued productivity, today's workforce is increasingly dependent on access to data "anytime, anywhere." This data-driven workforce is enabled by desktop, laptop, and mobile technology, and becomes more distributed and mobile as companies adapt to business conditions such as globalization, telecommuting, off-shoring, and outsourcing.

IDC estimates that 60 percent of corporate data now resides on distributed systems on laptops and desktops physically located far from the central data center.<sup>1</sup> The most obvious example of this is the tremendous volumes (and business value contained therein) of email.

The number and type of applications employed in the workplace have also proliferated. Though database and email/messaging applications topped a recent ESG survey of the most challenging applications from a data protection perspective, the list also includes document or content management (including collaboration tools such as on Microsoft® Office SharePoint®), file-serving, financials, business intelligence/data warehousing, e-commerce, billing, Human Resources (HR), Client Relationship Management (CRM), video/multi-media, Engineering/Computer Aided Design (CAD)/Computer Aided Manufacturing (CAM), and more.<sup>2</sup>

<sup>1</sup> "It's Not Business as Usual," Cynthia Doyle (IDC analyst, Business Continuity), April, 2002.

<sup>2</sup> "Data Protection Market Trends," John McKnight, Mary Johnston Turner, Enterprise Strategy Group, January, 2008.

### Distributed data management: challenged to do more with less

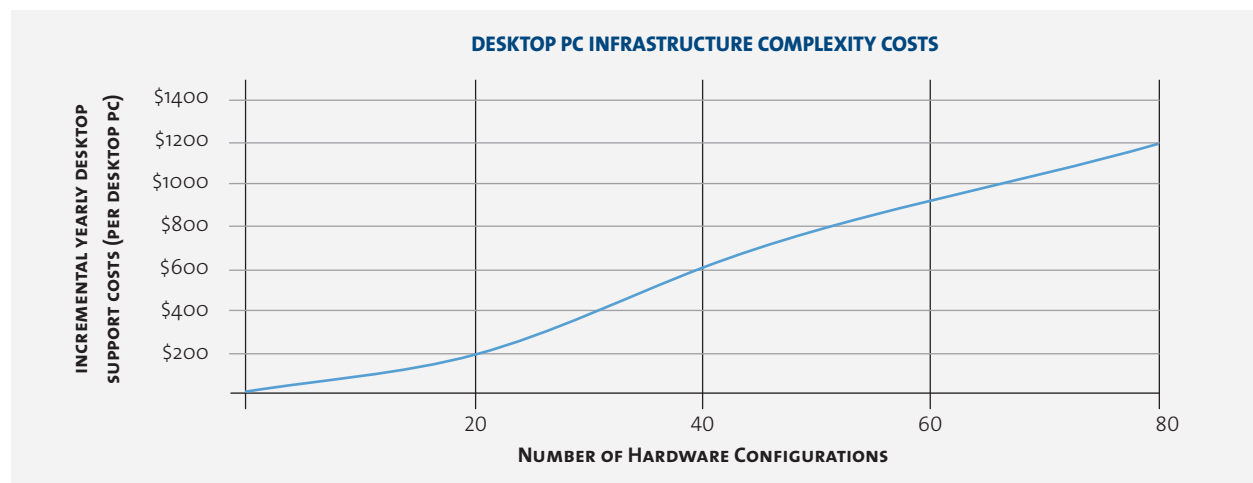
Managing such a variety of applications for a distributed workforce, frequently in remote offices, puts additional burdens on an IT organization. It has been shown support costs for desktops increase in direct proportion to the variety of platforms and applications requiring support.<sup>3</sup> And during times of economic downturn, like any part of the organization, IT might have caps on spending and staffing.

Ironically, economic downturns tend to aggravate the support of distributed data technology in another way. As corporations cut back on desktop and laptop replacements, they hold on to hardware longer. This increases the types of deployed configurations and the volume of qualification testing required of IT. This also directly impacts support costs, frequently just when IT is being asked to “do more with less.”

Keeping workers productive is a basic function of IT. A distributed and mobile workforce, ever more reliant on decentralized data, puts greater pressure on IT to keep technology up and running so workers can remain productive. In effect, there are expanding “points of failure” in regards to protecting worker productivity.

In a constantly changing workforce, including the impacts of acquisitions and mergers, IT staff might not be proportionately extended to accommodate the extra workload. IT becomes increasingly stretched and the risks to the company in reduced productivity, as well as in non-compliance penalties and data breaches, increase.

Concurrently, IT is taking on a greater role in designing and implementing regulatory compliance procedures and systems. These systems protect sensitive data (private and other) and help ensure business continuity. One of the primary measures of compliance is consistency across an organization; compliant data protection procedures must be demonstrably consistent in all locations – hard enough to accomplish within a centralized operation, even more difficult in a physically distributed environment.



**FIGURE 1: THE MORE COMPLEX A DESKTOP PC ENVIRONMENT GROWS, THE MORE COSTLY IT IS TO SUPPORT.<sup>1</sup>**

<sup>3</sup> Wipro NerveWire Study, “New Insights on PC Management: Benefits of Controlled PC Hardware Diversity,” Q1Yo4.

### **Regulations make no exceptions for distributed data**

Though difficult to quantify the risks, non-compliance and actual data loss or breach represent potentially significant hard-dollar costs to the company. For IT, compliance can be a bewildering array of overlapping, even contradictory, regulations. In the U.S. alone, the Better Business Bureau maintains a list of 34 Federal and State privacy regulations.<sup>4</sup>

There were 50 percent more private data breaches reported in the U.S. in 2008 than in 2007, exposing the personal records of at least 35.7 million people.<sup>5</sup> In 2008, a Ponemon Institute survey looked at 43 organizations that suffered a privacy data breach, and reported an average of \$202 spent per compromised record or \$6.6M per incident.<sup>6</sup> These included direct costs such as “hiring forensic experts; notifying consumers; setting up telephone hotlines to field queries from concerned or affected customers; offering free credit monitoring subscriptions; and discounts for future products and services,” as well as indirect costs like customer churn and impact on stock price.<sup>7</sup>

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 Security and Exchange Commission (SEC) endorsed regulations like NYSE Rule 446 and NASD Rules 3510 and 3520.<sup>8</sup> In Europe, disaster risk management and continuity are addressed by Basel II, or The New Capital Accord, among other country-specific regulations.

Again, though difficult to quantify the incremental risk for incomplete or inadequate disaster recovery and business continuity preparedness, the ultimate costs are clear. According to Faulkner Information Services, 50 percent of businesses that lose their data due to disasters go out of business within 24 months. According to the U.S. Bureau of Labor, 93 percent are out of business within five years.<sup>9</sup>

Data regulations generally allow for “no excuses” where information resides, whether paper or electronic, in a data center or on a laptop. This precedent has been made it clear in the U.S. through various rulings concerning the Federal Rules of Criminal Procedure (FRCP), specifically a series of rulings in Zubulake vs. UBS Warburg in 2003-2004. The court ruled not only, “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.<sup>10</sup>

<sup>4</sup> “A Review of Federal and State Privacy Laws”, BBB OnLine, Inc. and the Council of Better Business Bureaus, Inc., 2002.

<sup>5</sup> “Data Breaches up Almost 50%, Affecting 35.7 Million People,” Brian Krebs, Washington Post, January 6, 2009. For a chronological list and description of some of the publicly known privacy breaches, see <http://www.privacyrights.org/ar/ChronDataBreaches.htm#2>.

<sup>6</sup> “Costs of a Data Breach; Can You Afford \$6.65 Million?,” Larry Ponemon, February 4, 2009. <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9127376>

<sup>7</sup> “Data Breaches are More Costly than Ever,” Brian Krebs, Washington Post, February 3, 2009.

<sup>8</sup> “Rules Widen the Scope on Business Continuity,” Steve Stanek, KnowledgeLeader contributing author, November, 29, 2004. These 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.

<sup>9</sup> “Is Your Company Prepared to Recover From an IT Disaster?,” Paul Chisolm, Certification Magazine, February, 2008. <http://www.certmag.com/read.php?in=3310>

<sup>10</sup> A summary and the actual rulings in Zubulake vs UBS Warburg can be found at: <http://www.krollontrack.co.uk/zubulake/>

**Online data protection is uniquely qualified**

Online backup services make company-wide data protection more viable as an IT service. At the same time, online backup services enables IT to focus on managing information and keeping workers productive, rather than managing distributed infrastructure. Several key features make online data protection services uniquely qualified to address the challenges of a distributed workforce.<sup>11</sup>

- Backups are completely automated – the vendor, rather than IT or the end-user, takes on most of the responsibility to ensure the success of backup and 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 IT, 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, especially important in protecting data in remote offices.

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

The immediacy and comprehensive nature of online 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 they consistently achieve their objectives.<sup>12</sup> Online data protection moves data immediately offsite, and recovery from the vendor is dependent only upon the capability to receive the data in “hot-standby” facility or other data center.

The following section, Calculating the Cost: Current and Alternative Methods of Data Protection, helps IT identify and assign value to these cost categories. These costs can then be incorporated in an ROI analysis.

<sup>11</sup> Suggested by “Market Overview: Backup Software-as-a-Service,” Stephanie Balaouras, Forrester, February 20, 2008.

<sup>12</sup> Iron Mountain-sponsored research, September, 2008.

## CALCULATING THE COSTS: CURRENT AND ALTERNATIVE METHODS OF DATA PROTECTION

Currently a company might be using one or more of the following methods to protect distributed business data – or considering one of them as an alternative “step-up” from current methods.

- End-users are responsible for remembering to backup specific data to centralized servers (or their files are synchronized with a centralized file server)
- IT is responsible for recovering data (either from disk or tapes, located onsite or offsite) for restoration to end-users
- End-users are responsible for backup to a local external drive or removable media, and performing their own restores
- End-users in a remote office back up to a local server, which dumps data to a tape backup system maintained by office staff

In preparing the business case showing the ROI of moving to online data protection, you must document the costs in the current method of backup and recovery – as well as any other alternatives that are being considered.

In many cases, these costs might be “hidden” in other departments, or at least not transparently connected to backup and recovery system (or a lack thereof). These cost categories should include:

- End-user support
- Costs for alternative data protection solutions – whether minor tweaks to the existing system or more extensive (and expensive) solutions
- Costs for computer migration
- Costs of asset loss
- Costs of data loss

Each category and its connection to efficient and effective backup and recovery systems is described further below.

### End-User Support Costs

The overall goal of this part of an ROI analysis is to define the annual cost of the time spent supporting a distributed workforce. This should include tasks such as tracking missing backup windows, troubleshooting failed backup jobs, monitoring performance and tape utilization, and compressing recovery requirements. The following support cost categories and factors should be considered:

**Workforce size:** Record the current size (numbers), growth rate, and variety of platforms and applications used by the distributed workforce. These are the basic factors that drive the IT support costs.

**Labor estimates and rates:** What categories of support tasks do you define and how many hours would you estimate are spent on each? Note different support cost structures depending upon which members of the IT staff perform each function.

**“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 the information workers in your company. Remember to include cost when end-users need to divert time from their primary duties to participate in backup and recovery.

All of these costs increase the Total Cost of Ownership (TCO) for each desktop or laptop system in a distributed environment. Without a solid accounting of these costs, any business case based on an ROI calculation would be incomplete.

### Costs for Alternative Data Protection Solutions

Alternatives to the current data protection method might be minor – like adding an external hard drive to a workstation – or they might be more extensive, like installing a tape system for backup and recovery in a remote office. It is important to be comprehensive and consider all of the major cost categories involved in your specific distributed environment, as described in the table below.<sup>13</sup>

**TABLE 1. COST CATEGORIES FOR (NON-SAAS) ALTERNATIVES TO CURRENT DATA PROTECTION METHODS**

<b>HARDWARE COSTS</b>	These include backup hardware capital costs (e.g., external hard drives, tape systems and media, additional servers in the data center), as well as maintenance and support costs of new hardware.
<b>SOFTWARE COSTS</b>	It's important to include all licensing costs – not only for onsite backup software but also for operating system (OS), application server, database and monitoring software required for running backup hardware.
<b>IMPLEMENTATION COSTS</b>	These include the cost of internal or third-party staff to install, set up, integrate, configure, and train staff on new onsite backup solutions.
<b>IT MAINTENANCE &amp; LABOR COSTS</b>	How will support of an alternative data protection solution affect estimated costs of end-user support as calculated in the previous section? There will also be ongoing labor costs of upgrading onsite backup and recovery software – especially software you have customized – and replacing end-of-life software as technology advances.

These costs should be carefully documented and fairly represented in order for management to evaluate against subscription fees for an online data protection service. The hardware costs need to be projected over the expected lifecycle of the solution (e.g., the cost of an external hard drive for each laptop or desktop over a three-year period).

<sup>13</sup> Categories suggested by "Is SaaS Cheaper than Licensed Software," Jason Rothbart, November 21, 2008, downloaded on May 28, 2009 from [www.readwriteweb.com](http://www.readwriteweb.com) archives.

### **Computer Migration Costs**

The typical desktop or laptop computer has a lifecycle of approximately 36 months. Effectively, this means one-third of an organization's desktops and laptops must be replaced every year. For every replacement, IT migrates user data, applications, and custom user 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.

As with end-user support, determine the time spent by IT and end-user in a typical computer migration, and the labor rate of the staff doing the operation. Using the rule of thumb of a 36 month lifecycle, project the annual cost of migrating one-third of the organizations' desktop or mobile systems.

### **Cost of Asset Loss**

An IT best practice is the deployment of asset discovery software to track desktops and laptops in an attempt to "rescue" or eliminate the loss of hardware and software. This is particularly valuable in more distributed environments and physically remote offices. Significantly, most conventional asset discovery software cannot track what is on any given desktop or laptop. In the cost calculations for asset loss, it is important to include the recovery costs for system software.

Analysts estimate about six percent of assets (installed hardware and software) are lost per year. The total cost of ownership for these lost assets, including cost sunk into support and loss in user productivity, should be included in any ROI calculation for current or alternative data protection methods. These costs represent a more accurate cost of the asset loss, since full, rapid system recovery must include software and getting the system back to a productive state. Calculating the cost of the data loss itself is shown below.

### **Estimated Cost of Data Loss**

There are multiple costs incurred from lost business data. As described above, not all data types are created equal, and the loss of private data could entail significant hard costs for customer notifications, legal costs, and penalties, as well as costs more difficult to quantify in the form of damage to brand, customer churn, eroded stock price, etc. There is an opportunity cost to a business beyond what it costs in IT labor to attempt to recover data.

A Gallup poll estimates that two percent of laptops or desktops will lose an average of 1MB per year. An industry white paper revealed U.S. businesses placed an average value of \$10,000 per 1 MB.<sup>14</sup> Using the number of desktops and laptops within your organization, an estimated figure for data loss – distinct from the costs of asset loss or more significant costs due to the loss of private data – can be derived.

<sup>14</sup> The value of business data varied from industry to industry, and the type of data stored on any machine depended upon the role within the organization. \$10,000 is a very conservative figure. "Data Recovery, Performed Remotely," OnTrack whitepaper, 2003.

## THE COST SAVINGS OF ONLINE DATA PROTECTION

As described above, online data backup and recovery services are uniquely suited to address distributed data management. The sections below detail the potential cost efficiencies of an online data protection service.

### Savings in End-User Support

Using the same workforce size, labor times, and rate figures as above, online data protection services can provide significant reductions in desktop support costs and TCO. Online data protection services are easily activated, providing immediate relief for the high costs of desktop and laptop lifecycle management, including support and manual backup solutions. The amount of time spent by IT Help Desks working on desktop and laptop problems is greatly reduced – as high as a 70 percent reduction in mean call time. Even a conservative reduction of 30 percent in the amount of time required to support a desktop or laptop would result in impressive cost savings.

Additionally, as support call times become more efficient, end-user downtime is also lower. Though a “soft” cost, a 25 percent reduction in end-user downtime provides substantial savings in additional worker productivity. If users currently spend time executing and managing backups, there are further savings as productive time is regained – backups and system state captures occur automatically.

### Savings over Alternative Data Protection Schemes

Depending upon the current system for backup and recovery within your organization, and the alternatives under consideration, different categories of costs should be examined in order to calculate savings in moving to a SaaS model.

**TABLE 2. COST CATEGORIES IN MOVING TO A SAAS MODEL (COMPARE TO TABLE 1)**

<b>HARDWARE COSTS</b>	There are no hardware costs (unless you elect an optional additional local appliance for even faster automatic recovery). The cost of the hardware and media, now and in the future, is borne by the service provider. The amount of storage you select for your backup data and retention periods is determined in the monthly subscription fee.
<b>SOFTWARE COSTS</b>	In the SaaS model, not only does the monthly service fee cover use of the basic backup and recovery software, but in the case of some vendors, includes support of a wide variety of platform, email and database support (some vendors do charge separately for plug-ins). These include the cost of internal or third-party staff to install, set up, integrate, configure, and train staff on new onsite backup solutions.
<b>IMPLEMENTATION COSTS</b>	There are none of the costs for implementing onsite data protection solutions, aside from IT deciding the rules of which types of files to back on and how often they should be saved.
<b>IT MAINTENANCE &amp; LABOR COSTS</b>	The monthly subscription fee for the level of service and amount of storage that fits your requirements covers all software costs, as well as upgrades and maintenance. Typically, support is available 24x7 and, while you retain control over the rules of backup and recovery, a large percent of current costs of backup and recovery support is taken on by the service provider.

### **Computer Migration Savings**

An online 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. A conservative estimate of 50 percent savings over current methods of computer migration would be reasonable.

### **Savings in Asset Loss**

Unlike conventional asset tracking software, online data protection services can provide a backup audit feature. Backup audit allows IT to track and recover what system software – the already qualified configuration – was on any given desktop or laptop. Simply having this information can reduce the value of the asset loss in terms of TCO by about 25 percent, conservatively.

### **Savings in Data Loss**

Manual backup solutions have limited effectiveness in preventing data loss, primarily the dependence on end-users to follow proper procedures and regularly back up all the required data. By providing automated, consistent data protection for every desktop or laptop in an enterprise, online data protection services can virtually eliminate the cost of this loss. The potentially significant repercussions, penalties, and other costs for loss of private or other sensitive data are discussed below. Online data protection helps protect the company from costly fines and other risks of non-compliance with privacy regulations.

### ANALYZING THE ROI OF ONLINE DATA PROTECTION

The following table summarizes the costs and savings categories in comparing current, alternative onsite, and online backup and recovery strategies. The ROI, the profitability of reducing operational costs over time (typically annualized), can be clearly demonstrated for online data protection services.

TABLE 3. COST AND SAVINGS COMPARISON CHART			
CATEGORIES FOR CALCULATING COSTS AND SAVINGS WITH ONLINE METHODS (SAAS)	METHOD OF DATA PROTECTION		
	Current Method Costs	Alternative Method Costs	Online (SaaS) Savings
<b>End-User Support</b>	<ul style="list-style-type: none"> <li>Number of desktops and laptops supported</li> <li>IT hourly wage (burdened)</li> <li>IT support hours (annualized)</li> <li>End-user downtime (“soft” costs)</li> <li>Average end-user hourly wage (burdened)</li> </ul>	<ul style="list-style-type: none"> <li>Note: goal of alternative is increase capacity and/ or decrease data loss from current methods</li> <li>Use and care of new equipment and software could increase IT costs and possibly end-user time</li> </ul>	<ul style="list-style-type: none"> <li>Number of desktops and laptops supported</li> <li>Monthly subscription (annualized)</li> <li>30% of current method end-user support</li> <li>25% of current method end-user downtime (“soft” costs)</li> </ul>
<b>Alternative Data Protection Solutions</b>		<ul style="list-style-type: none"> <li>Hardware</li> <li>Software</li> <li>Implementation</li> <li>IT maintenance and labor</li> </ul>	<ul style="list-style-type: none"> <li>Growth in capacity and new technologies included in subscription</li> </ul>
<b>Computer Migration</b>	<ul style="list-style-type: none"> <li>IT hourly wage (burdened)</li> <li>IT support hours (annualized)</li> <li>End-user downtime</li> <li>Average end-user hourly wage (burdened)</li> </ul>	<ul style="list-style-type: none"> <li>Might be the same as for current methods</li> </ul>	<ul style="list-style-type: none"> <li>Included in subscription</li> <li>50% of current method</li> </ul>
<b>Asset Loss</b>	<ul style="list-style-type: none"> <li>6% of the number of desktops and laptops</li> <li>TCO of desktop or laptop (including software)</li> </ul>	<ul style="list-style-type: none"> <li>No change from current methods unless increase in number of desktops or laptops</li> </ul>	<ul style="list-style-type: none"> <li>Back up audit should be included in subscription</li> <li>25% of current method</li> </ul>
<b>Data Loss</b>	<ul style="list-style-type: none"> <li>2% of the number of desktops and laptops</li> <li>\$10,000 per 1MB</li> <li>Note: this does not include private data loss</li> </ul>	<ul style="list-style-type: none"> <li>No change from current methods unless increase in number of desktops or laptops</li> </ul>	<ul style="list-style-type: none"> <li>Online DP saves you 100% of this cost – it is included in the subscription</li> </ul>
<b>ROI (profitability of reducing operational costs)</b>		<ul style="list-style-type: none"> <li>Savings over current method</li> </ul>	<ul style="list-style-type: none"> <li>Savings over current method</li> </ul>

#### Summarizing the Return on Investment of SaaS Online Backup and Recovery

By totaling the cost of the current and alternative methods and comparing them to savings realized by moving to online data protection, you can express the profitability of reducing operational costs (ROI) as:

Annually, the company will spend (price of the annual SaaS subscription) to realize (savings over current method).

## **ADDITIONAL BENEFITS OF ONLINE DATA PROTECTION**

There are additional benefits of online 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 SaaS vendor.

### **Improved Governance, Risk and Compliance (GRC) Program**

Online data protection applied consistently across a distributed workforce with no requirement for end-user interaction can go a long way toward improving a GRC program. The immediacy with which data is moved offsite to a secure location, and ease with which this data can be retrieved, can also make RTOs/RPOs far more achievable.

As described above, the costs of data loss or breach can be significant, including damage to corporate brand, shareholder confidence, and concerns about data privacy from customers and employees. The portable nature of laptops places them at high risk for loss or theft. 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.

If a laptop is lost or stolen, a centralized backup store is essential to help an enterprise judge the scope of potential information exposure. Moreover, enterprises use their centralized, up-to-date backup store of distributed data to understand their legal exposures. Integrating their laptop backup with legal discovery and review tools can help reduce legal discovery costs, and plan for early case assessments.

### **Leveraging the Online Data Protection Vendor**

It is difficult to quantify the benefits gained when IT resources can be redirected to mission-critical business goals. Limited IT resources could be deployed to implement a new CRM system, or update an old financial or accounting system. This value also should be emphasized in any ROI presentation.

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

As they free up IT staff, fully functional, mature web-based tools provided by online data protection services allow IT to better monitor and manage the quality of data protection across the ever changing distributed environment. The experienced and committed service provider is incorporating new tools and adding value to its products. An example might be the automatic classification of distributed enterprise data – classification more granular than Tier 1, Tier 2, etc. This would allow greater efficiencies throughout 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 current methods of onsite backup and recovery, IT managers can build a compelling case for investing in an online data protection service. Careful examination of all these costs shows the ROI – the profitability of reducing operational costs over current or alternative methods. This ROI is based on hard dollar savings in end-user support, workforce productivity, computer migration, asset loss, and data loss.

While harder to quantify, additional benefits have very real value to the corporation. These include a stronger Governance, Risk and Compliance (GRC) Program, mitigation of risk from private data loss or theft, and catastrophic failure in DR or business continuity plans. There also are ongoing benefits derived from leveraging the resources of the online data protection service provider, including taking advantage of the vendor's investment in technology and data protection expertise, and better alignment of IT to 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 3).

© 2009 Iron Mountain Incorporated. All rights reserved. Iron Mountain and the design of the mountain are registered trademarks and Iron Mountain Digital is a trademark of Iron Mountain Incorporated. All other trademarks and registered trademarks are property of their respective owners.



120 Turnpike Road  
Southborough, Massachusetts 01772  
(800) 899-IRON

Iron Mountain Digital is the world's leading provider of Storage-as-a Service solutions for backup and archiving. The technology arm of Iron Mountain Incorporated offers a comprehensive suite of data protection, archiving and intellectual property management solutions to thousands of companies around the world, directly and through a worldwide network of channel partners. Iron Mountain Digital is based in Southborough, Mass with European headquarters in Frankfurt, Germany.