Value of Cloud Security: Vulnerability

Leviathan Security Group

leviathan
security group

limitless innovation. no compromise.

Introduction

This paper will examine the notion of vulnerability of data storage—the exposure of data storage options, both in world-spanning cloud storage services, and in localized datacenters, to threats in setting up and operating reliable, redundant, and resilient data services. We are particularly interested in the requirements for building data storage services in response to localization laws. These are proposed laws in a few countries that would require that all data produced by or on behalf of a nation's citizens be stored within that nation's boundaries. Since storage services in response to these laws have not yet been created, we will use the exercise of setting up single-corporation data storage solutions as a small-scale experiment for the larger, more difficult challenges of doing so for all of a nation's data.

In order to explore the notion of vulnerability as it relates to cloud security, we have enumerated the characteristics of commonly available cloud storage platforms in terms of cost, capacity, access management, reliability, redundancy, resilience, backup capability and operations. Wherever possible, we have used quantified measurements and qualified measurements. This created a baseline from which we can compare commonly installed local storage solutions.

Utilizing a combination of this baseline, information on common SMB installations, and limited anecdotal information gathering, we have provided documented models to illuminate the true vulnerability of local storage as utilized by a significant majority of small and medium businesses. The inclusion of assumptions, quantified and qualified measurements of the two significant environments (cloud and local) in several variations will provide a basis for clarity on the capability of each to resist attack.

We provide a comprehensive analysis of the two models, and enumerate their characteristics in a largely quantified fashion, to produce a baseline describing a clearly-delineated secure storage solution. With a completed baseline in hand, we have provided a documented model for each of local storage and cloud-based storage enumerating the direct costs of maintaining a solution within a changing vulnerability landscape.

Secure Storage: A Definition

A secure storage solution is one that reliably stores data and allows authorized users to quickly access that data, while also preventing those unauthorized from doing so. In addition to authentication and authorization, the solution must also offer offline and online backup functionality, as well as resilience from both natural disasters and hardware failures. Ultimately, the solution must protect the confidentiality, integrity, and availability of all data.

Assumptions

All organizations, no matter their line of business, consume storage. As the business grows, so do their storage requirements. This analysis will compare the average costs of implementing and maintaining a locally hosted storage solution versus the costs of storing data in the cloud. Of course, a true cost comparison is difficult to accomplish at a generic level as every organization has different storage requirements and every organization also has different in-house capabilities. To ensure that we provide a fair comparison we will use three different storage scenarios outlining the storage requirements for three different organization sizes; small (50 employees), medium (500 employees), and large (2500) employees. When considering each storage scenario and to further ensure an equal comparison the following assumptions for all scenarios are made:

1. ORGANIZATION CAPABILITIES - A mature organization will be able to accomplish day-to-day IT related tasks in a more cost-effective manner than one with immature capabilities. This analysis will assume that all organizations are performing at a consistent level of maturity. We will assume that each organization is operating at a Capability Maturity Model (CMM) Level 3, defined as "all processes are clearly defined, repeatable, and consistent across the organization."[1]

2. NETWORK - For the purpose of this analysis, it will be assumed that all organizations, regardless of size, will have Internet connectivity as well as a basic local area network (LAN) in place. We will however, assume that there are costs associated with remote access to data, whether in the form of a VPN solution for local solutions, or increased bandwidth costs for the cloud.

3. ALLOCATED STORAGE - While it is understood that all organizations determine their per user storage allocation based on a diverse set of variables, many of these variables are difficult to predict. In order to ensure that we have a fair comparison, we will state that all users, regardless of organization size will require 300GB of storage per user, including both individual working capacity and storage required for the organization as a whole.

4. ORGANIZATION SIZE - In order to effectively compare costs associated with hosting data in the cloud to those involved in self hosting, we have created three arbitrary scenarios involving three different fictional organization sizes: small (50 employees), medium (500 employees), and large (2500 employees).

5. DISK PERFORMANCE - It is assumed that traditional spinning-disk hard drive performance (with caching enabled) is sufficient for the company to use. We have not specified SSD arrays within the document, as enterprise-grade SSD technology is significantly more expensive than traditional hard disk solutions.

6. DATA CONSUMPTION - For every terabyte of data stored, users will on average read 400 gigabytes and write 400 gigabytes of data per month.

7. SECURITY CAPABILITIES - It is assumed that all organizations, due to performing at a maturity level of 3, have the necessary people, process and technology in place to handle their organizational information security needs.

8. BACKUP CAPABILITIES - We have calculated and listed the cost of sufficient backup capabilities to perform a monthly full backup of each organization with daily incremental backups. In addition, we have added the cost of 10 extra backup tapes (or other media), as necessary.

Storage Scenarios

As described above, a number of scenarios are necessary to understand the variability of cost when considered at different scales.

1. **SMALL CONSULTANCY LLC**

   Small Consultancy LLC provides business consulting (non-IT) in North America, and has 50 employees, most of which are based at its one corporate location. Of these 50 employees, it is typical that 20 will be off-site on any particular day, either undertaking sales and marketing activities, or working on existing customer engagements. The nature of Small Consultancy LLC's work means that when employees are at a customer location, they are unlikely to connect back to the office during the work day, and will work offline on their corporate-issued laptop, although many will synchronize files from home using the company's in-house VPN service upon their return from the customer premises. The remaining 30 employees work from the office location, however it is not uncommon for staff to work from home and connect to the corporate network via the company's in-house VPN service.

   The company's corporate location houses a small server room where all corporate computing resources are housed, along with the entire network and telephony infrastructure; patch cables are run from the server room to desks for connectivity. Small Consultancy LLC has a dedicated IT staff that is responsible for the setup, maintenance and operation of all systems located in the corporate office.

   Small Consultancy LLC has implemented Active Directory to handle user authentication and authorization to servers and file shares. The corporate VPN capability uses a separate two-factor authentication product for authentication.

   The average file storage consumption per user is 200GB per user, and a further 100GB per user has been allocated by management for growth, for a total of 300GB per user. Thus Small Consultancy LLC requires 15TB of storage space. Storage requirements

will be provided by a Network Attached Storage (NAS) device that is only accessible via the corporate LAN (or remotely via VPN).

2. **Mid-Sized Regional Inc.**

Mid-Sized Regional Inc. has 500 full-time employees distributed between a main office and four field offices. Their business model requires very few users to work off-site, but WAN bandwidth is consumed for normal staff file access use, as the field offices are connected to the main office via site-to-site VPNs running over the Internet.

On the occasion that employees do leave the corporate locations, they must use a corporate-issued laptop and connect to the corporate office via a client-to-site VPN service which uses two-factor authentication.

The company's main corporate office houses a datacenter-like infrastructure; field offices, where necessary, house small server rooms for local resources such as telephony, door locking and networking infrastructure. Active Directory, databases and file storage, however, are centralized in the main office datacenter facility, with authentication and authorization being provided by Active Directory Infrastructure.

Core switches are used to carry data between local network segments and remote locations, while access to the internal desktop network is provided predominantly via cabled connections run from distribution switches. There are some wireless access points in the office, but they are not part of a corporate architecture; they are instead residential-class access points, installed to fulfill a requirement for tablet use within the Marketing department.

Storage needs will be met via an enterprise class storage and server configuration, with the necessary performance upgrades to handle 500 users. The current average consumption of file storage by users is 250GB per user. Mid-Sized Regional Inc. currently has 150TB of storage space (200GB per user), leaving 50GB growth per user before file storage is considered inadequate. They are currently investigating options for replacing/upgrading their NAS or moving to a cloud-based solution.

3. **Big Corporation Inc.**

Big Corporation Inc. has 2500 employees distributed between two corporate offices, six field offices, and some employees who work from home. Additionally, the company has rented space in two datacenters.

The corporate offices house server rooms for local facilities such as building management systems, telephony, Active Directory and print. The majority of operations exist in datacenters, housing central file storage, databases, enterprise applications and core network capabilities, including the hub for inter-office VPN connectivity.

The inter-office VPN links use the Internet for connectivity as distance makes point to point links cost-prohibitive; the VPNs use the datacenter facilities as a primary and secondary hub site. Due to the centralized nature of most applications, there is little to no need for communications between offices and so there has been no effort to explore meshed connections. Internet connectivity for web browsing, email, etc. is provided via a breakout point at each of the datacenters to remove control of content filter and firewall decisions from offices, leaving VPN traffic the sole consumer of WAN bandwidth at office locations. Remote users must use VPN clients and two-factor authentication for remote access.

Users have a current profile quota of 300GB each, and thus Big Corporation Inc. requires 750TB of storage space. A replicated pair of storage devices are used, with one located at each datacenter to aid in disaster recovery.

Solution Architecture

The following outlines the solutions we have selected for each storage scenario. Please note that while we used specific software and hardware manufacturers for the purpose of obtaining accurate pricing, we do not endorse any particular vendor. As is commonly the case in real-world purchasing, the vendor that was able to provide the most accurate and timely pricing for a solution that met our needs was selected.

1. **SMALL CONSULTANCY LLC**

   Small Consultancy LLC requires a solution that provides 15TB of storage accessible from the LAN, either by being physically in the office and plugged in to the network, or via a VPN solution.

   For support needs, Small Consultancy LLC is satisfied with next-business-day replacement parts and available support during working days/hours. In order to accomplish this, the following has been scoped:

   Storage Server — Dell PowerVault NX400

   - 1.8Ghz Xeon Processor
   - 2 500GB Drives (RAID 1)
   - 8 3TB Disks with a RAID 5 Controller
   - 8GB Memory

   The 2 500GB hard drives will be in a RAID 1 configuration (mirrored) to offer redundancy for the Operating System and any other storage required for the system itself. A RAID 5 card is installed to offer resilience against drive failure and performance gains over using a software RAID implementation. The 3TB disks will be configured to provide at least 15TB of data with redundancy and recovery abilities.

   Windows 2012 R2 will be used for the operating system, while backup needs will be handled by a Drobo 5D system configured

to offer 20TB of backup storage space that will be managed by Symantec Backup Exec.

In order to protect clients and servers from malware, Symantec Endpoint Protection will be leveraged. To facilitate the centralized management of the malware protection solution, an additional Windows 2012 R2 license will be required, which will run on a Dell PowerEdge R320 server.

This system satisfies Small Consultancy LLC's immediate storage needs, while leaving room for expansion as required.

For the costs associated with Small Consultancy LLC, please see Table 3 - Table 6.

2. **Mid-Sized Regional Corp**

Mid-Sized Regional Corp requires a storage solution that provides 150TB of storage accessible from the internal LAN as well as for VPN users. For support needs, Mid-Sized Regional Corp requires 7 days a week, 24 hours a day support with a 4-hour replacement part guarantee. In order to accomplish this the following has been scoped:

Storage Server — Storinator Redundant NAS (2)

- Intel Dual-core i3-3240
- 8GB RAM
- 2 — 500GB Drives (RAID 1 - Operating Systems / Boot)
- 90 — Seagate 4TB Disks

Backup Solution — Tandberg Data T160+ Tape Library

- Dell PowerEdge R520 Server
- Microsoft Windows 2012 R2
- 83 LTO-6 Backup Tapes

The backup solution provides enough space for a monthly full backup as well as for daily incremental backups. In addition, spare tape media has been scoped to account for bad media or other failures. In order to meet these backup requirements, 2 Tandberg Data Tape Libraries will be connected together.

Malware protection will be handled by another Dell PowerEdge R520 server, with Symantec Endpoint Protection installed on all clients and servers.

This solution meets Mid-Sized Regional Corps immediate storage needs, while leaving room for expansion as required.

For the costs associated with Mid-Sized Regional Inc., please see Table 7 - Table 10.

3. **BIG CORPORATION INC.**

Big Corporation Inc. requires 750TB of total storage space to meet its needs. Storage will be housed in two datacenters that are also used as a common VPN endpoint for all traffic, be it from other offices or from remote workers.

Support requirements are 7 days a week, 24 hours a day with a 4-hour replacement part guarantee.

750TB of storage represents a significant footprint at the data-centers, and is accomplished with the following:

Storage Area Network — Petarack High Availability SAN

- 2 — Intel Xeon E5 Sandy-Bridge Processors
- 512GB of memory
- Dual head units for redundancy
- Dual network cards

Backup Solution — Tandberg Data T160+ Tape Library

- Dell PowerEdge R720xd Server
- Microsoft Windows 2012 R2

- 203 LTO-6 Backup Tapes

The backup solution will require multiple (5) Tandberg Data T160+ libraries interconnected, and will provide a monthly full backup as well as a daily incremental backup.

Malware protection is handled by a single Symantec console managing Symantec Endpoint Protection on all clients and servers. The management console will be installed and run on a Dell PowerEdge R725xd.

This solution meets Big Corporation's immediate storage needs, while being flexible enough to expand as needed. Note that expansion of the backup and malware solution may require moving to a more distributed architecture involving multiple servers, instead of a single server for each as scoped here.

For the costs associated with Big Corporation Inc., please see Table 11 - Table 14.

Vulnerability

When comparing storage solutions it is important to not only compare the financial impact of each solution, but also the intrinsic vulnerability of the solution.

Many companies store sensitive information on their file storage solutions; this includes not just information on staff and customers, but also intellectual property which could carry catastrophic consequences for an organization if it were to be lost or fall into the hands of a competitor.

Before we examine the categories of threats that face businesses considering localized storage, we should consider the nature of the security problem. Security is often compared to an arms race—a constant grind of building the newer, the better, and the more effective. This comparison is inaccurate. The traditional conception of an arms race is that neither side is actually deploying its weapons until an advantage is gained, and so as long as both sides stay evenly matched, neither side will be attacked. Unfortunately, a modern understanding of vulnerability as a field is far different.

Modern methodologies allow attackers continuously to probe the trust boundaries of any organization, which means that rather than waiting for an overwhelming advantage, an adversary will exploit any temporary lapse. Temporary lapses are, however, inevitable in almost any organization. Maintenance activities, such as security patching and updates, perimeter rules changes, and the addition or subtraction of, or change to, any network device will cause cracks to appear in the security of any organization. Preventative measures, such as "intrusion detection systems," are brittle, and their alerts must carefully be monitored in order to derive value from them; this is particularly difficult given an environment of a continuous war of attrition in which the attackers are many, and the defenders few.

Ultimately, beyond specific categories of threats as discussed below, companies considering storing their own data, rather than using a cloud-based storage medium, must realize that in addition to the direct

costs that are discussed above, they must make a significant and continuous investment in tools, training, and personnel charged with guarding the business' most significant assets: its knowledge. The defense, like the adversary, must be continuous, growing, and tireless; anything less will not suffice.

Common Threats

The following threats are common to all modern compute environments, be they in-house or outsourced, or off the shelf or bespoke.

Process Failure

All organizations, especially those who are operating at a capabilities maturity level of 3, have processes, be they for vulnerability management, user management, or even just day-to-day health monitoring. In order for the storage solution to remain secure, all processes must be functioning in an effective manner. A failure in any established process may mean a failure in security controls.

Preventing this sort of failure comes down to resources. Organizations using a local storage solution must ensure that IT departments are sufficiently staffed and retain the necessary security knowledge and skills.

Malicious Insider

Not only do organizations need to worry about having sufficient staffing in place to support all business processes, but staff must be trusted not to act in a malicious manner. This, of course, is a difficult problem to solve; however, organizations should ensure that administrative access is limited to those that require it, and that all access is closely monitored.

Hardware/Software Failure

The storage solutions outlined in this document are designed to provide a level of resiliency and disaster recovery. However, in the real world, not all solutions are created equal; without proper disaster recovery planning, a hardware or software failure may result in excessive down-time and/or data loss.

Cloud solutions are not immune to hardware failures, so just like for local storage, any solution should be designed to offer resiliency and recovery. Spare hardware should be readily available, and manufac-turer maintenance guidance should be followed. Of course, a large-scale cloud provider is more likely to be equipped to handle this sort of threat than most organizations who build their own storage solu-tions.

Authorization or Authentication Failure

Any data storage solution may suffer a failure to correctly control user authentication or authorization. There are some differences to the impacts of the scenario between classes of storage, however. With local storage, a user may be able to bypass file access control mechanisms through subverting the storage perimeter—for instance, by physically accessing a storage machine, or by obtaining superuser access to a storage machine also used for other purposes. Those particular types of attacks tend to be difficult in cloud-based storage. However, due to the nature of cloud storage under certain legal regimes, data stored with a cloud provider may be easier for a government order made without due process (such as a subpoena) to obtain; as such an order would go to the provider, rather than to the customer, the customer might not be informed that their authorization boundaries had been breached. (With on-site data storage, a customer would be physically in control of their data, and thus much more likely to notice the presence of, for instance, uniformed officers demanding access.) Each solution has different risks in this category, and a company's particular threat model might deter-mine which risks are more concerning.

Cloud-Specific Threats

These threats are largely limited to cloud-based storage scenarios, and are not seen as commonly in a completely internal environment.

Lack of Monitoring & Audit Capabilities

A key component to any secure storage solution is the ability to audit all file level access. Not all cloud providers provide this ability to a customer, which leaves a large gap in security posture. Before picking a cloud provider over local storage implementations, a customer must be sure that the provider can meet all audit and logging requirements.

Problems with Internet Connectivity

In the event of an Internet connectivity failure, users are unable to access Cloud resources. Of course, this also means that in a locally implemented solution that remote users also would not have access via VPN; however, the outage only impacts remote users in the local scenario, while it impacts the entire organization in a cloud solution.

Local Storage Threats

These threats are specific to local storage, and distinct in that they do not impact cloud-based storage. Typically this is because the scale of cloud storage solutions dilutes these problems to such a degree that the impact to any single customer is so negligible that it would not be noticed.

Loss of Local Knowledge

In a local storage implementation scenario, there is always the potential for employee turnover in IT departments. If knowledge of the storage solution is not well documented or understood by multiple employees, that knowledge may be lost when employees leave.

Facilities Disaster

A local disaster such as a fire or power outage, as well as larger regional disasters such as earthquakes or floods, may cause local outages and even data loss.

Equipment Scarcity & Price Fluctuations

As manufacturing conditions change, pricing and availability of replacement equipment may become an issue. For example, in 2011, a flood in Thailand caused a production shutdown that substantially increased the cost of hard disks for many months. As local storage implementations are not buying equipment at the same scale as cloud providers, these changes in pricing have a much higher impact.

Geographic restrictions to support

In some cases, an organization who has built their own local storage solution may not be in a geographical area where onsite support is readily available. For example, most hardware storage vendors offer a 4-hour response time for emergency technical support. The local organization may be in an isolated enough area that meeting this 4-hour window is not possible. Cloud providers, however, are more immune to this problem as they typically keep qualified support engineers on staff and onsite.

Management

One significant challenge that modern organizations face is complying with retention requirements, destruction requirements, and other all-data policy regulations. For governments, these might exist in the form of open records and personally-identifiable information laws; for businesses, these could come from health information regulations, tax laws, or a host of other policy sources. Any group might also be subject to discovery and retention orders coming from litigation, where whole swaths of documents may have to be preserved, and failure to do so could trigger criminal penalties.

For these overarching policy changes, cloud storage can provide significant advantages. Cloud providers often include powerful policy tools that allow automatic retention or destruction of documents, including API-level access that allows programmatic changes in response to organizational needs. For local storage, these tools must be built or bought as an additional layer of software on top of the storage infrastructure, and oftentimes cannot be made retroactive (that is, they can only affect documents whose entire lifecycle exists within the document management system, and cannot be used to affect others). In general, the advanced data management capabilities already present within many cloud storage solutions make this not-uncommon business challenge manageable without the expense of building or buying a document management solution on top of a storage solution.

Conclusion

This analysis has focused on the cost of the first three years of owner-ship of a local storage solution, as contrasted with the cost of three years of a cloud storage solution. Within those constraints, the cost of cloud computing for a small organization is slightly cheaper than building an in-house storage solution. For medium and large organiza-tions, cloud storage solutions turn out to be slightly more costly than local solutions.

The costs described in this document, however, are not the only costs that need to be considered by an organization. First, a local storage solution will at some point need to be replaced in its entirety, as tech-nologies change and the old systems become cost-ineffective to main-tain; this will result in a significant capital expenditure, as well as the downtime, training, and installation costs associated with any major new system. By contrast, with a cloud-based storage solution, there will be no similar major cost milestones—and over time, as new tech-nologies make large-scale storage less costly for the cloud provider, it is likely that the per-unit cost of cloud storage will decrease. Indeed, since we began this analysis, Microsoft has announced that OneDrive prices for home users will decrease by more than 73% per gigabyte in some cases,[2] and Google announced that Google Drive will charge just $5/user/month extra to upgrade storage from 30GB to 1TB, a 33-fold expansion.[3]

In addition, the pricing in this document assumes that an organization's future needs are predictable. In the event of unforeseen expansion of storage needs, such as that following a significant acquisition, an orga-nization with local storage could need to purchase major upgrades or new storage systems just to meet existing demand, whereas an organization using cloud storage would only increase its monthly cost. The pricing also relies on an organization's being able easily to source both equipment and capable staff to secure that equipment; if either of those fails to be true, then the costs of running a local storage solu-tion will escalate rapidly.

The conclusion to draw from these data is that a simple price calculation—even one that contains significant detail and technical depth, such as

that seen in this paper—cannot be the deciding factor for organizations with significant storage needs. **An organization should consider its predicted rate of expansion (and to what extent it is able accurately to predict its expansion), its technical requirements, its appetite for capital outlay, its ability to establish a long-term supply chain, and its ability to recruit adequate technical and security personnel as criteria equal to or more significant than price.**

Tabular Data

All data in these tables was current as of September 10, 2014.

Feature Comparison

On a scale of 0-3 we have scored each of the solutions.

- 0 = absent
- 1 = tolerable
- 2 = sufficient
- 3 = preferred
- U = Unknown or insufficient detail to perform accurate analysis

Local Storage

The scenarios represent real life localized storage solutions; the scores are derived by assessing those solutions against what we believe to be the preferred solution for each scenario.

- **COST** - solutions are scored according to the price. Note cost does not denote value for money.
- **CAPACITY** - Providers are scored for the capacity offered per user. 3 denotes more capacity than is currently required.
- **ACCESS MANAGEMENT** - Scored on the available integration to an existing infrastructure in the scenarios. A fully Active Directory integrated solution would score 3.
- **RELIABILITY, REDUNDANCY, AND RESILIENCE** - In many ways these three areas are intertwined. These scores are based on features such as geographic distribution of multiple copies of data, ease, and automation with which failover to another host or region occurs and likelihood of doing so.

- **BACKUP CAPABILITY** - Is scored independently of reliability, redundancy, and resilience as this refers not to backup in case of equipment failure, but the retention and restoration of data in case of user error. 3 refers to complete backups with near-instant recovery times.
- **OPERATIONS STAFFING** - Refers to the number of employees dedicated to operations, if they are 24x7 or business hours only and geographic distribution.
- **MEAN TIME TO FIX** - Is scored based on data surrounding the mean (average) time to recover from failure.

The comparison is shown in Table 1.

Cloud

The cloud vendors selected do not constitute an exhaustive list of cloud storage providers; they do however offer a representative sample of prices, pricing models and capabilities. By using this cross section of providers we feel that we are able to suitably represent Cloud Storage service providers, as a whole.

Scores are based on the advertised capabilities for providers; this does not represent an independent assessment of the ability to execute perfectly on that advertised capability. Some scores are U, which is different from the 0 (absent) score, insofar as it denotes that we were unable to confirm the existence of the capability or not; a 0 would indicate a confirmed absence of the capability.

By assessing the advertised capabilities we scored each provider in each category:

- **COST** - Providers are scored according to the price relative to the rest of the marketplace. Note cost does not denote value for money.
- **CAPACITY** - Providers are scored for the capacity offered per user. 3 denotes "unlimited."

- **Access Management** - Scored on the available integration to an existing infrastructure in the scenarios. A fully Active Directory integrated solution would score 3.
- **Reliability, redundancy, and resilience** - In many ways these three areas are intertwined. These scores are based on features such as geographic distribution of multiple copies of data, ease, and automation with which failover to another host or region occurs and likelihood of doing so.
- **Backup capability** - Is scored independently of reliability, redundancy, and resilience as this refers not to backup in case of equipment failure, but the retention and restoration of data in case of user error.
- **Operations Staffing** - Refers to the number of employees dedicated to operations, if they are 24x7 or business hours only and geographic distribution.
- **Mean time to fix** - Is scored based on data surrounding the mean (average) time to recover from failure.

The comparison is shown in Table 4.

In the event of a real organization moving forward with a cloud solution, there would of course be a more in-depth due diligence process, where risks which are pertinent to a specific organization would be assessed with prior knowledge of their risk appetite. This would include a legal review of the terms of the contract.

Costs

Costs can be broken down in to three different categories:

- hardware/software,
- implementation, and
- management/maintenance.

Cost estimates and averages for the locally based solutions were based on pricing data from publicly available sources such as: Costs can be broken down in to three different categories:

- Hewlett Packard - www.hp.com
- CDW - www.cdw.com
- IBM - www.ibm.com
- Dell - www.dell.com
- Other Manufacturer and solution provider web sites and data sheets

Across all three scenarios the following items will remain a constant:

- **COST OF LABOR** - when calculating implementation costs, a rate of $125 / hour will be used.
- **IMPLEMENTATION TIME** - when calculating time to implement the solution, the number of users will be considered in time estimates.
- **BUSINESS PROCESS ENGINEERING** - an average cost of $175 / hour will be used for any time estimated developing or documenting business processes.
- **COST OF PATCHING** - As all three scenarios will leverage Microsoft Windows Server 2012 R2, the cost of patching is estimated to be $149.00[5] per patch event per system.
- **FREQUENCY OF PATCHING** - It will be expected that there will be a minimum of 12 patch events a year.
- **CLOUD COSTS** - The cost of cloud subscriptions has been calculated by assessing the cost models of ten major providers of cloud storage solutions. For each provider, we selected the most cost-effective product which would fulfill the requirements of the scenarios, including total storage, data transfer and number of users. By applying the selected product for each provider to each of the three scenarios, we were able to understand the range of costs available in the cloud storage market. We selected the median (most central) quote from the ten providers in order to provide a comparison against using local storage. For more details regarding suppliers and product lines assessed see Table 15.

Table 1: Local Feature Comparison

	Scenario 1	Scenario 2	Scenario 3
Cost In each case, we have determined that these systems are priced in the mid-range. A more expensive solution would have received a lower score.	2	2	2
Capacity We specified systems that are at or near their theoretical maximum storage. It would be possible to specify systems which would have an expected lifespan of double the three year period.	2	2	2
Access Management We selected systems that provided Microsoft Active Directory integration functionality to handle authorization and authentication.	3	3	3
Reliability Reliability varies between the solutions as they (intentionally) offer differing capabilities in dealing with, and recovering from, failure. It is not surprising that as more money is spent on a solution, the level of reliability increases.	1	2	3
Redundancy As with reliability, there is an intentional correlation between cost and the redundancy capabilities of the solutions. With money spent on RAID, geographic distribution and synchronization, redundancy will naturally improve.	1	2	3
Resilience Unsurprisingly resilience, as with reliability and redundancy, improved as the scale of the deployments grew. Larger, distributed systems are more resilient than smaller standalone solutions.	1	2	3
Backup capability Backup capabilities are largely similar for all the products with the notable exception of capacity. All have timed backup to other media with manual restore procedures. If a file is both created and deleted before the backup schedule is run, that file is lost.	2	2	2
Operations staffing All companies scored a 1, which is tolerable within their organizations. However they do not have a 24x7 network operations center or geographically distributed staff, which would be needed to attain a higher score.	1	1	1
Mean time to fix None have a truly transparent resolution process, however Scenario 3 scored higher as the replicated and distributed system permits failover to a full-capacity system, with no outages. Scenarios 1 & 2 could potentially suffer downtime in the event of a chassis failure, for example.	1	1	2
TOTAL	13	16	20

Table 2: Cloud Feature Comparison

	Amazon	Box	Copy	Cubby	Dropbox	Google	HP	OneDrive	Rackspace	SpiderOak
Cost Cost varies considerably between various providers. This was however due, at least in part, to differing features, capabilities and billing models. Cost will therefore also vary depending on any particular given scenario.	3	2	2	3	1	2	1	1	1	U[4]
Capacity Capacity offered was typically large; providers scoring a 3 listed their capacity as "unlimited". It is possible that providers not listing an unlimited option could offer such a service, but this was not listed in the pricing materials at the point at which we assessed them.	2	3	2	1	3	3	3	2	2	3
Access management There are 3 levels of access management offered: web based dashboard, API & Active Directory integration. Typically those offering Active Directory, and scoring 3, will also offer API access.	3	3	U	3	1	2	2	3	2	3
Reliability Overall, marketing material offered surprisingly little in terms of specific details on reliability beyond stating a "reliable service".	2	U	U	U	U	3	3	U	U	U
Redundancy As with reliability, marketing material offered surprisingly little in terms of specific details with regards to redundancy.	2	U	U	U	U	3	3	U	3	U
Resilience As with reliability & redundancy, marketing material offered surprisingly little in terms of specific details with regards to redundancy.	2	U	U	U	U	3	3	U	3	U
Backup Capability Backups followed the trend of reliability, redundancy and resilience by offering very little detail regarding specific functionality. This of course does not mean that the feature does not exist, merely that the information is not as readily available as that of other features.	U	U	U	U	2	U	U	U	U	U
Operations staffing Operations staffing is not featured within price lists or product comparisons pages of any of the providers. However some details were gleaned via other materials available on the providers sites.	3	U	U	U	U	3	U	U	3	U
Mean time to fix This is not mentioned in any of the cloud provider materials in any depth.	U	U	U	U	U	U	U	U	U	U
TOTAL	17	8	4	7	7	19	15	6	14	6

Table 3: Small Consultancy LLC - Hardware and Software Costs

Item	Price ($)	Local Quantity	Local Cost ($)	Cloud Quantity	Cloud Cost ($)
Dell PowerVault NX400,[6] including: 2 x 500G mirrored disks (Operating System) 8 x 3TB disk (storage) RAID5 Card Gigabit NIC 8G RAM 1.8GHz Xeon Processor	6,680	1	6,680	0	0
Backup Hardware (locally attached)[7]	1,649	1	1,649	0	0
Windows 2012 R2 Server[8]	882	2	1,764	1	882
Backup Server Software (Symantec Backup Exec Small Business)	728	1	728	0	0
Anti-Virus Software - Server Hardware (PowerEdge R320)	2,529	1	2,529	1	2,529
Anti-Virus Software - Client Licenses (including year 2 and 3 maintenance)[9]	2,205	1	2,205	1	2,205
Total Hardware and Software			15,555		5,616

Table 4: Small Consultancy LLC - Implementation Costs

Item	Price ($)	Local Quantity	Local Cost ($)	Cloud Quantity	Cloud Cost ($)
Installation Costs (per server / per hour)	125	16	2,000	8	1,000
Workstation Configuration (per server / per hour)	125	100	12,500	100	12,500
Total Implementation Costs			14,500		13,500

Table 5: Small Consultancy LLC - Operations Costs

Item	Price ($)	Local Quantity	Local Cost ($)	Cloud Quantity	Cloud Cost ($)
Power & Cooling - NAS[10][11]	241	1	241	0	0
Power & Cooling - AV Server	153	1	153	1	153
Patching (per event / per server)	149	24	3,576	12	1,788
Maintenance Agreement (15% of hardware/software cost)	2,334	1	2,334	1	2,334
Yearly Cloud Subscription - see Table 15	9,299	0	0	1	9,299
Total Operations Costs			6,304		13,574

Table 6: Small Consultancy LLC - Total Three-Year Cost

	Local ($)	Cloud ($)
Hardware and Software Costs	15,555	5,616
Implementation Costs	13,500	13,550
Operations Costs (3 years)	6,304	13,574
	6,304	13,574
	6,304	13,574
Total Costs Over 3 Years	47,967	59,888

Table 7: Mid-Sized Regional Inc. - Hardware and Software Costs

Item	Price ($)	Local Quantity	Local Cost ($)	Cloud Quantity	Cloud Cost ($)
45 Drive NAS[12] Intel Dual-core i3-3240 8GB RAM Gigabit Network Card	7,437	2	14,875	0	0
Disks - Seagate 4TB STBD4000400[13]	180	90	16,200	0	0
Backup Hardware - Server Hardware (PowerEdge R520)	4,037	1	4,037	0	0
Backup Hardware - Tandberg Data T160 Tape Library[14]	21,420	2	42,840	0	0
Backup Media (Tapes LTO-6)	47	83	3,943	0	0
Anti-Virus Software - Server Hardware (PowerEdge R520)	4,037	1	4,037	1	4,037
Anti-Virus Software - Client Licenses (including year 2 & 3 maintenance)	29,106	1	29,106	1	29,106
Windows 2012 R2 Server (backup and AV Servers)	882	2	1,764	1	882
Total Hardware & Software			116,802		34,025

Table 8: Mid-Sized Regional Inc. - Implementation Costs

Item	Price ($)	Local Quantity	Local Cost ($)	Cloud Quantity	Cloud Cost ($)
Installation Costs (per server / per hour)	125	32	4,000	8	1,000
Workstation Configuration (per system / per hour)	125	500	62,500	500	62,500
Total Implementation Costs			66,500		63,500

Table 9: Mid-Sized Regional Inc. - Operations Costs

Item	Price ($)	Local		Cloud	
		Quantity	Cost ($)	Quantity	Cost ($)
Power & Cooling - 45 Drive NAS[15]	415	2	830	0	0
Power & Cooling - PowerEdge R520	329	2	658	1	329
Power & Cooling - Backup Hardware	110	2	220	0	0
Patching (per event / per server)	149	48	7,152	12	1,788
Maintenance Agreement - NAS Hardware	3,213	2	6,426	0	0
Maintenance Agreement - Servers	7,864	2	15,730	1	7,864
Yearly Cloud Subscription - see Table 15	83,390	0	0	1	83,390
Total Operations Costs			31,016		93,371

Table 10: Mid-Sized Regional Inc. - Total Cost

	Local ($)	Cloud ($)
Hardware and Software Costs	116,802	34,025
Implementation Costs	66,500	63,500
Operations Costs (3 years)	31,016	93,371
	31,016	93,371
	31,016	93,371
Total Costs Over 3 Years	276,350	377,638

Table 11: Big Corporation Inc. - Hardware and Software Costs

Item	Price ($)	Local		Cloud	
		Quantity	Cost ($)	Quantity	Cost ($)
Storage Area Network - Petarack Hardware[16] 2 - Intel Xeon E5 Sandy-Bridge Processors 512GB of memory Dual head units Dual network cards Dual network cards	375,000	2	750,000	0	0
Disks - Western Digital WD4001FYYG 4TB[17]	360	252	90,881	0	0
Backup Server Hardware (PowerEdge R720xd)	8,712	1	8,712	0	0
Backup Hardware (Tandberg Data T160 Tape Library)	21,420	5	107,100	0	0
Backup Media (Tapes LTO-6)	47	203	9,643		0
Anti-Virus Software - Server Hardware (PowerEdge R720xd)	8,712	2	17,424	2	17,424
Anti-Virus Software - Client Licenses (including year 2 & 3 maintenance)	145,530	1	145,530	1	145,530
Windows 2012 R2 Server	882	3	2,646	2	1,764
Total Hardware & Software			1,131,936		164,718

Table 12: Big Corporation Inc. - Implementation Costs

Item	Price ($)	Local		Cloud	
		Quantity	Cost ($)	Quantity	Cost ($)
Installation Costs (per server / per hour)	125	40	5,000	16	2,000
Workstation Configuration (per system / per hour)	125	2500	312,500	2500	312,500
Total Implementation Costs			317,500		314,500

Table 13: Big Corporation Inc. - Operations Costs

Item	Price ($)	Local Quantity	Local Cost ($)	Cloud Quantity	Cloud Cost ($)
Power & Cooling - SAN[18]	701	2	1,402	0	0
Power & Cooling - Backup Library	110	5	550	0	0
Power & Cooling - AV/Backup Servers	329	3	987	3	987
Patching (per event / per server)	149	60	8,940	24	3,576
Maintenance Agreement - NAS Hardware	71,716	1	71,716	0	0
Maintenance Agreement - Backup Hardware	3,213	5	16,065	2	6,426
Yearly Cloud Subscription - see Table 15	449,750	0	0	1	449,750
Total Operations Costs			99,660		460,739

Table 14: Big Corporation Inc. - Total Cost

	Local ($)	Cloud ($)
Hardware and Software Costs	1,131,936	164,718
Implementation Costs	317,500	314,500
Operations Costs (3 years)	99,660	460,739
	99,660	460,739
	99,660	460,739
Total Costs Over 3 Years	1,748,416	1,861,435

Table 15: Cloud Provider Pricing

Provider (annual costs)	Scenario 1 500 users 15 TB ($)	Scenario 2 500 users 150TB ($)	Scenario 3 2500 users 750TB ($)
Amazon - Zocalo[19]	4,776	47,706	237,306
box.com - Business[20]	9,000	90,000	450,000
copy.com - Pro[21]	4,495	44,950	449,500*
Cubby - Enterprise[22]	9,598	76,780	335,916*
DropBox - Business[23]	10,200	102,000	1,020,000
Google - Cloud Storage[24]	4,792	47,923	479,232
HP - Cloud Object Storage[25]	16,588	165,888	1,658,880
OneDrive - OneDrive For Business[26]	35,906	366,557	1,846,992
Rackspace - Cloudfiles[27]	18,432	184,320	1,843,200
SpiderOak - Blue Enterprise[28]	3,300	30,300	150,300
Mean (average cost)[29]	11,963	117,826	791,651
Median (the 'central' quote)	9,299	83,390	449,750
Range (difference between highest and lowest quotes)	32,606	336,257	1,696,692.40

Notes

1. http://en.wikipedia.org/wiki/Capability_Maturity_Model#Levels

2. https://blog.onedrive.com/new-onedrive-storage-plans/

3. https://www.google.com/work/apps/business/pricing.html

4. Unknown setup fee. See Table 15.

5. http://download.microsoft.com/download/1/7/b/17b54d06-1550-4011-9253-9484f769fe9f/TCO_SPM_Wipro.pdf

6. http://www.dell.com/us/business/p/powervault-nx/pd

7. http://www.drobostore.com/products/drobo-5d

8. http://www.microsoft.com/licensing/about-licensing/windowsserver2012-R2.aspx#tab=3

9. https://roianalyst.alinean.com/symantec/

10. http://www.manualslib.com/manual/390696/Dell-Powervault-Nx400.html?page=7

11. http://www.webmath.com/kwh.html

12. http://www.45drives.com/products/order/dw-redundant.php

13. http://www.seagate.com/ca/en/internal-hard-drives/desktop-hard-drives/desktop-hdd/

14. http://www.tandbergdata.com/us/index.cfm/products/tape-automation/storagelibrary/storagelibrary-t160/

15. http://www.45drives.com/products/direct-wired-redundant.php

16. http://www.aberdeeninc.com/abcatg/petarack.htm

17. http://www.wdc.com/global/products/wtb/?sfamily=wdsfRESAS&family=WD%20Re&region=ca&language=en

18. http://www.aberdeeninc.com/abcatg/powersupplies.htm

19. http://aws.amazon.com/zocalo/pricing/

20. https://www.box.com/pricing/

21. https://www.copy.com/price

22. https://www.cubby.com/pricing/

23. https://www.dropbox.com/business/pricing

24. This table represents raw storage costs; additional costs for this provider will be accrued as bandwidth and other file accesses are not included. https://cloud.google.com/products/cloud-storage/

25. This table represents raw storage costs; additional costs for this provider will be accrued as bandwidth and other file accesses are not included. http://www.hpcloud.com/products-services/object-storage?t=pricing

26. https://onedrive.live.com/about/en-us/plans/

27. Costs are extracted linearly from list-price, due to going beyond list prices based on number of users or amount of storage in a scenario. This was assumed reasonable as not every organization will have identical negotiating powers in this scenario. http://www.rackspace.com/cloud/files/

28. Costs are extracted linearly from list-price, due to going beyond list prices based on number of users or amount of storage in a scenario. This was assumed reasonable as not every organization will have identical negotiating powers in this scenario. https://spideroak.com/business_pricing/

29. Mean, Median and Range have been calculated using additional consideration for file access charges which will be accrued for providers that charge separately for access. Charges are in line with the Scenarios outlined in the body of this document.

Project Team

- **James Arlen** - Director of Risk and Advisory Services - james.arlen@leviathansecurity.com

- **Lee Brotherston** - Security Advisor - lee.brotherston@leviathansecurity.com

- **Steve Manzuik** - Security Advisor - steve.manzuik@leviathansecurity.com

- **Brendan O'Connor** - Senior Security Consultant - brendan@leviathansecurity.com

- **Chad Thunberg** - Chief Operating Officer - chad.thunberg@leviathansecurity.com

Leviathan Security Group, Inc.
3220 1st Ave S, Suite 100
Seattle, WA 98134

p: 866.452.6997
f: 206.225.2004
e: contact@leviathansecurity.com

www.leviathansecurity.com

This work was commissioned by Google Inc., and created by Leviathan Security Group, Inc.
Google had no editorial control over this document.