Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Online Backup: Worth the Risk?

For most organizations, data is the lifeblood of the enterprise. Yet while much time is spent creating and using data, too often little thought is given to protecting that data from loss. While backups have been the time-tested method for loss protection, they too often get shoved down the priority list and not paid enough attention to in the organization. The proliferation of online backup services seems to be the easy and obvious answer to maintaining an effective organizational backup plan. Yet there are a numbe...

Copyright SANS Institute
Author Retains Full Rights

AD

Online Backup: Worth the Risk?

GIAC (GSEC) Gold Certification

Author: Steve Strom, steve@stevestrom.com
Advisor: Tim Proffitt

Accepted: 5/3/2010

Abstract

For most organizations, data is the lifeblood of the enterprise. Yet while much time is spent creating and using data, too often little thought is given to protecting that data from loss. While backups have been the time-tested method for loss protection, they too often get shoved down the priority list and not paid enough attention to in the organization. The proliferation of online backup services seems to be the easy and obvious answer to maintaining an effective organizational backup plan. Yet there are a number of questions that should be addressed before committing enterprise data to an online backup environment. The goal of this paper is to surface the issues that need to be addressed when considering an online backup platform.

© 2010 SANS Institute, Author retains full rights.

1. Introduction

1.1. Data: Key to the Enterprise

1.1.1. Growth of Data

The sheer quantity of digital data, and the rate at which that data is growing, is almost beyond comprehension. This explosion of all things digital – recordings, graphics, documents, video, and other forms – has led to a staggering need to manage and account for that data. According to a report issued by EMC, the digital universe in 2007 was an overwhelming 281 exabytes in size (Gantz, et al.). Yet according to that same report, the digital universe is growing at such a phenomenal pace that by the year 2011, it will be 10 times the size it was in 2006 (Gantz, et al.)!

1.1.2. Consequences of Lost Data

All of this data has value, the loss of which will incur a cost. Some has an obvious immediate economic impact (like loss of the accounts receivable database), while other types of data has a more nuanced result (like the loss of trend data). While the cost of lost data will vary due to the type of data and circumstances surrounding the loss, it will always have some type of a cost. An analysis commissioned by DeepSpar Data Recovery Systems and written by David Smith of Pepperdine University concluded that, on average, a single data loss incident will cost an organization $2,900 (Smith).

While the average incident cost may be rather low, it should be noted that data loss can also have much more severe financial consequences. Notification and monitoring costs after a data breach can easily multiply and rapidly become a drain on corporate finances.

1.2. Impact of Select Trends on Data Management

The problem of managing this gigantic amount of data has, in some instances, been compounded by current trends in information technology.

1.2.1. Cloud computing

Cloud computing is a term that is currently used by many IT professionals, yet it is one for which everyone seems to have a different definition. While the Internet itself is

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

often referred to as the "cloud", when coupled with the phrase "computing", the term is fairly fuzzy in definition.

Perhaps the best definition of "cloud computing" is that which is provided by InfoWorld:

> Cloud computing comes into focus only when you think about what IT always needs: a way to increase capacity or add capabilities on the fly without investing in new infrastructure, training new personnel, or licensing new software. Cloud computing encompasses any subscription-based or pay-per-use service that, in real time over the Internet, extends IT's existing capabilities (Knorr & Gruman).

A slightly different view of the cloud is provided by another author:

> The cloud itself is a set of hardware, networks, storage, services, and interfaces that enable the delivery of computing as a service. Cloud services include the delivery of software, infrastructure, and storage over the Internet (either as separate components or a complete platform) based on user demand (Hurwitz, Bloor, Kaufman, & Halper, 2009).

Using these definitions, Cloud Computing encompasses everything from SaaS offerings (like Salesforce.com) to utility computing infrastructures (such as Amazon Web Services). The problem with Cloud Computing, from the perspective of this paper, is that enterprise data now resides in a distributed environment. Some of it may reside on the corporate desktops and on-site servers, some on the cloud servers, and even more in a cloud application and database. Yet while this data is distributed across various vendors and platforms, the enterprise IT team is still responsible for managing and caring for that data. This responsibility is particularly troublesome with reference to the data stored in the cloud, as the IT team has responsibility but no real authority over controls implemented on that cloud data.

1.2.2. Mobile computing

Closely linked to the growth of Cloud Computing is the absolutely explosive growth in Mobile Computing. A recent IEEE Spectrum article noted that

> By 2014, cell phones and other mobile devices will send and receive more data each month than they did in all of 2008. Three-fourths of the total will come from internet access and nearly all the rest from audio and video streaming.

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

> A big part of the increase in mobile data will come from cloud computing applications. Utility software (such as maps), will lead the way, followed closely by productivity tools (especially for sales, data sharing, and collaboration), then social networking and search (Cherry, 2009).

From the perspective of data backup, mobile devices now become an additional device upon which data resides and must be managed.

1.2.3. Digital footprint

The term "Digital Footprint" is sometimes used to indicate the total digital information created by a single event or transaction. Most people severely underestimate the size of the digital footprint created by a transaction. To help explain that footprint, EMC created a little vignette titled "A Day in the Life of An Email" which examines the total amount of digital data created in the transmission of a single email.

> The email itself is small, but with it is a 1MB attachment. If the email is sent to four people, wouldn't that mean that there are 5 x 1.1MB involved? The original and four copies?
>
> No, unfortunately. To begin with, there is the document itself stored on the local machine, then the email that contains the document. In this infrastructure, copies of all emails are kept on the central email server, which, in order to keep the email system up and running, includes a redundant server. Desktop files, where the original document sits, are backed up daily to a server. The servers are then periodically backed up to tape and taken offsite. Our original 1.1MB email has a footprint eight times bigger than itself.
>
> Now add up the local and backed-up copies of the email sent to the four colleagues, and that footprint is 30 times larger than the original email.
>
> Then there is all the temporary data created as the emails and backup systems send data back and forth across the local and wide area networks. In transmission, all manner of communications overhead is introduced: signaling data, packet addresses and headers, security codes, router caches, and management and tracking information. The estimate here is admittedly fuzzy, but it is within the order of magnitude. (Gantz, et al.).

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

The problem from a backup perspective is that this large digital footprint presents the need for serious evaluation. Which pieces of the digital shadow, if any, need to be backed up? What are the consequences during a restore if pieces of this digital shadow are missing? And how do we ensure that all the shadow pieces are appropriately managed so that data loss can be mitigated?

1.2.4. Online Backup: Panacea?

Such quantities of data present vast problems for enterprise management. As the same EMC report noted, "While 70% or more of the digital universe is created, captured, or replicated by individuals --- consumers and desk and information workers toiling far away from the datacenter – enterprises, at some point in time, have responsibility or liability for 85%" (Gantz, et al.).

From a backup perspective, it would seem that the easiest way to manage this data would be to:

- Backup everything
- Backup automatically
- Backup to an offsite location

This is the promise of online backup services – to automatically backup everything (or everything that is selected) to a secure offsite location. But is that really a good idea? Are there any issues that should be considered when evaluating whether or not to use automatic online backup? What regulatory frameworks need to be considered if an organization chooses to use an online backup provider? And how does this impact the responsibility to manage corporate data?

1.3. Three Providers for Consideration

For the purposes of this paper, three different online backup services will be used as examples of this industry segment. Nothing in this paper is to be construed as an endorsement or caution against any of these individual providers. Rather these three have been chosen as representative services from which we can draw conclusions about the use of such services in a business environment.

1.3.1. Carbonite

Carbonite (www.carbonite.com) is one of the most well-known services in this

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

industry segment. An extensive advertising campaign coupled with a catchy name has provided this service with a memorable offering.

Carbonite promotes service for Windows and Mac by noting that "Every year, 43% of computer users lose their music, photos, documents, and more" (Carbonite). They advertise their service as online backup for small businesses with multiple PCs, with these major selling points:

- Unlimited backup capacity
- Completely automatic
- Secure and encrypted
- Easy file recovery (Carbonite)

1.3.2. BackBlaze

BackBlaze (www.backblaze.com) offers their online backup service for personal and business computers. This service does not backup servers or Linux based machines, but does backup Windows and Mac computers..

One of the unique things about BackBlaze is their storage pod design. Using readily available components, they have designed a cheap storage pod and released the design to the world (Nufire).

1.3.3. Jungle Disk

Jungle Disk (www.jungledisk.com) is an online backup service for Mac, Linux, and Windows based computers. The differentiator for this service is that they use Amazon Web Services as their storage platform. Clients who backup to Jungle Disk end up with their data transferred into the Amazon S3 cloud for storage (Jungle Disk).

2. Understanding Online Backup

2.1. How Online Backup Works

Online backup services follow a common pattern in their design and deployment. While the details may vary somewhat among various providers, the general process tends to be very similar.

2.1.1. Client install

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

Every online backup service has some type of software client on the subject computer. Some services have that client run continuously in the background so that changed files are backed up immediately. Other services start their client as a scheduled task or cron job on a regular basis to handle the backup tasks.

The client software gives you the option of what files to backup. Usually the My Documents or equivalent folder is included by default, with the ability to include other folders and files for backup as needed.

2.1.2. Backup process

Once the software client fires, it then evaluates files to see if they need to be backed up. Some services backup the file and only keep the current version of that file on the backup server. Other services backup the current version while also keeping older versions in the cloud, so that is it possible to restore a file to an earlier point in time.

2.1.3. Data Transfer

Online backup services require that the client computer be online to the internet in order for the backup service to work. However the amount of bandwidth required will vary depending on a number of factors. Some of these factors include:

- How many files need backed up and the file size
- The level of compression used for the transfer
- The level of deduplication to prepare the backup

Available bandwidth can be an important factor when evaluating online backup providers. It should also be noted that the required bandwidth will increase as the number of protected clients grows.

2.1.4. Encryption

Encryption is "the process of converting an original message into a form that is unreadable to unauthorized individuals – that is, to anyone without the tools to convert the encrypted message back to its original format" (Whitman & Mattford, 2009, p. 350). It is "a technique through which source information is converted into a form that cannot be read by anyone other than the intended recipient" (CompTIA, 2008, pp. 2-2).

Online backup systems generally employ encryption both to transmit data to the cloud as well as to store the data on the cloud server.

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

2.1.5. De-duplication

Traditional backup systems often duplicate the information that is copied to the backup. This may be intentional as different versions of one file are copied, or it may happen because only a small piece of a particular file has changed while the majority of the file remained unchanged. Copying the same data multiple times results in excessive time spent on creating the backup.

De-duplication tries to solve this problem. It can be explained this way:

> De-duplication is a rather intensive process that examines each block of data as it comes into the device and attempts to determine if it's seen the block before. If it hasn't, it stores it. If it has seen the block before, it throws the block away and stores only a reference to it (Preston, 2007, p. 290).

While this might not seem like a very important feature, the above author goes on to claim that "the average de-duplication system can reduce the amount of storage needed to store its backups by 20 to 1 or more" (Preston, 2007, p. 290).

2.1.6. Restore process

The restore process is pretty similar across services. Some services let you restore from a pane in the software client, while other services use a web interface from which to launch the restore. The selected file can then be overwritten to the same place on the initial computer, restored to a different place on the initial computer, or even restored to a different computer entirely.

All of the backup services use a password for access to the restore process. Security of that password is of paramount importance in order to protect the offsite backed up information.

2.2. Regulatory Frameworks

One of the big questions surrounding online backup services is the question of regulatory compliance for data that is backed up to the cloud. One author framed the issue this way:

> The ability of cloud computing to adequately address privacy regulations has been called into question. Organizations today face numerous different requirements attempting to protect the privacy of individuals' information, and it is not clear

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

> (i.e., not yet established) whether the cloud computing model provides adequate protection of such information, or whether organizations will be found in violation of regulations because of this new model (Mather, Kumaraswamy, & Latif, 2009, p. 31).

There are many different regulatory frameworks – both legislative and industry specific – that can impact whether or not online backup is an appropriate solution for a particular company. It is wise for an entity considering such a service to evaluate the data that is proposed to be protected by online backup as well as the regulatory requirements incumbent upon the organization in managing that data.

Following is a summary of representative legislative frameworks that may be pertinent to an online backup evaluation. This list is not meant to be exhaustive in scope nor detailed in analysis. It is simply presented as an example of the types of regulations and the questions that may need to be considered.

2.2.1. Computer Security Act

One of the first attempts to protect federal computer systems was the Computer Security Act of 1987. This act established minimum acceptable security practices while giving the National Bureau of Standards responsibility for developing these security standards (Whitman & Mattford, 2009, p. 91).

2.2.2. Electronic Communications Privacy Act of 1986

The Electronic Communications Privacy Act of 1986 is "a collection of statutes that regulate the interception of wire, electronic, and oral communications" (Whitman & Mattford, 2009, p. 92). While it could be assumed that this act affords privacy to data stored in the cloud, the reality is that this is not necessarily the case. One author notes that:

> SLAs, contractual clauses, and a high-level understanding of applicable legislation can giver user organizations, as well as data subjects, a false sense of security with regard to their rights to privacy. Users may assume that they are protected under the Electronic Communications Privacy Act (ECPA); however, a legitimate court order exempts electronic communications and remote computing service providers from adhering to the law (Mather, Kumaraswamy, & Latif,

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

2009, p. 158).

The author of the above quote goes on to provide several legal examples to prove his point.

This is a key question to understand when considering an online backup service. Storing backed up data in the cloud effectively changes the jurisdictional issues under which that data can be challenged. The prospective user needs to be aware of this issue.

2.2.3. Family Educational Rights and Privacy Act (FERPA)

The Family Education Rights and Privacy Act of 1974 is a federal law designed to protect the rights of student records. It recognizes two types of student record information, and the fact that the "non-directory" information "must not be released to anyone, including parents of the student, without the prior written consent of the student" (Van Dusen).

It appears from this law that any use of an online backup service to secure student record information potentially places that service within the realm of FERPA accountability. It may also create liability for the originating organization if student record information is considered "released" when it is stored in the cloud, or if that cloud provider suffers a breach which then releases student record information.

2.2.4. Health Insurance Portability and Accountability Act (HIPPA)

This act establishes national standards for electronic healthcare transactions. For the purposes of this paper, two specific rules affect data that is considered for online backup.

The Privacy Rule states that "organizations affected by the law must take reasonable steps to ensure the confidentiality of communications with individuals" (Bunker & Fraser-King, 2009, p. 51). This would include ensuring the confidentiality of data stored in a cloud service provider as an online backup.

The Security Standards Rule addresses various security standards and required implementations. This rule requires administrative procedures that "must identify employees or classes of employees who will have access to Electronic Protected Health information; access is restricted to only those who need it. Contingency plans – including those for backup, disaster recovery, or business continuity, are also required" (Bunker & Fraser-King, 2009, p. 51).

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

The Security Standards Rule also mandates control of physical access to data. This would include physical access to the hardware upon which an online backup may be stored (Bunker & Fraser-King, 2009, p. 51).

The final area in which the Security Standards Rule mandates control relates to technical specifications. This area deals with protection of the computer systems, databases, networks, and data. While encryption is a part of this area, it is not the only item within this realm (Bunker & Fraser-King, 2009, p. 51).

Any organization with HIPPA regulated environment must consider how an online backup service (or any other Cloud Service Provider) meets the mandates of these regulations.

2.2.5. HITECH Act

The Health Information Technology for Economic and Clinical Health (HITECH) Act was implemented as a section of the American Recovery and Reinvestment Act of 2009. HITECH amended and expanded HIPPA, with the immediate impact being a significant expansion in the number of entities covered under HIPPA (Mather, Kumaraswamy, & Latif, 2009, p. 161).

Mather explains the effect upon Cloud Service Providers (CSPs) this way:

> This HITECH law has a significant impact on CSPs; under this law many of them are now business associates, and as such they are subject to privacy and safeguarding requirements. They are also now subject to the expanded rule on PHI breaches. These new requirements have a significant impact on the privacy and security safeguards that a CSP should implement. A key area is protection so that patient information does not fall under the definition of *unsecured PHI* (PHI that is unsecured by a technology standard that renders the PHI unusable, unreadable, or indecipherable to unauthorized individuals) and is developed or endorsed by a standard developing organization that is accredited by the American National Standards Institute (ANSI) (Mather, Kumaraswamy, & Latif, 2009, p. 161).

The provisions of HITECH certainly expand the issues that must be considered when evaluating the suitability of online backup for regulated data.

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

2.2.6. Computer Fraud and Abuse Act (CFAA)

The Computer Fraud and Abuse Act, written in 1984, initially only covered federal computers. The CFAA was amended in 1986 to expand the scope of coverage so that all "federal interest" computers were covered. With this amendment, the act coverage was broadened to include the following:

- Any computer used exclusively by the U.S. government
- Any computer used exclusively by a financial institution
- Any computer used by the government or a financial institution when the offense impedes the ability of the government or institution to use that system
- Any combination of computers used to commit an offense when they are not all located in the same state (Stewart, Tittel, & Chapple, 2008, p. 634)

Further amendment of the CFAA in 1994 modified coverage to include any computer used in interstate commerce (Stewart, Tittel, & Chapple, 2008, p. 634).

Once again the question of jurisdiction is raised by the CFAA. If multiple companies backup their data to a particular online backup service, and one entity is charged under the CFAA, does the cloud server that hosted their backups suddenly become a covered computer? And if it does, what is the legal status of the backed up data from the other business entities?

2.2.7. USA PATRIOT Act

The USA PATRIOT Act "modified a wide range of existing laws to provide law enforcement agencies with broader latitude in order to combat terrorism-related activities" (Whitman & Mattford, 2009, p. 91). This act, while aimed at terrorism-related activities, has implications for cloud computing in general and for those considering online backup services in particular. One author framed the issue like this:

> At a high level, the challenge with the Patriot Act can be viewed as location, location, location. Exactly where is your data physically, and therefore whose government policies will your data be subject to? What law enforcement (including intelligence) practices, or perhaps conversely, privacy regulations, is the location of your data and your CSP [Cloud Service Provider] required to abide by (Mather, Kumaraswamy, & Latif, 2009, p. 156)?

Many times an online backup service does not provide the customer with control over

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

the location in which the online backup data is stored. This then raises the question as to jurisdictional control of that backup, and if a government order can access that backed up data simply based on the storage location.

2.2.8. Gramm Leach Bliley Act (GLBA)

The Gramm-Leach-Bliley Act of 1999 focuses on facilitating "affiliation among banks, securities firms, and insurance companies. Specifically, this act requires all financial institutions to disclose their privacy policies on the sharing of nonpublic personal information" (Whitman & Mattford, 2009, p. 93).

The GLBA Privacy Rule has a great implication for online backup services that store that data in the cloud. The many difficult privacy issues raised by GLBA have been examined by Mather:

> The privacy notice must explain information collection, sharing, use, and protection. As previously described, the privacy implications of these activities within the cloud have many thorny issues and unanswered questions. GLBA also requires that the notice give a financial institution's customer the right to opt out of the information being shared with unaffiliated parties. It has yet to be determined legally whether CSPs are unaffiliated parties, because the law is frequently behind technology. But the implications of a financial institution using an open cloud model are that there is the distinct possibility that (in the future) CSPs would be deemed unaffiliated parties. The issue remains of how a CSP customer could opt out of the sharing while still using the service if the cloud is the platform employed. In addition, financial institutions are required to update their privacy policies when they change, and offer an opt-out at that time as well. How can a financial institution truly state the nature of the use and protection of such data, when it does not have full control over the data, may not have complete ownership of the data depending on the SLA, and may not be able to anticipate the dynamic use of the data in cloud applications (Mather, Kumaraswamy, & Latif, 2009, p. 160).

For a business considering an online backup service, the issue of guaranteeing data privacy remains a difficult consideration.

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

2.2.9. EU Directive

Directive 95/46/EC is a European Union regulation "designed to protect the privacy and protection of all personal data collected about citizens of the EU, with regard to the collection, storage, use, modification, and transmission of that data" (Photopoulos, 2008, p. 282).

The intent of this law was to prevent the transfer of personal data outside the European Union or countries that have been designated as having adequate safeguards already in place (Mather, Kumaraswamy, & Latif, 2009, p. 163).

The implications of someone considering an online backup service are apparent -- any backup containing EU citizen personal data must be done such that it complies with this directive. While not automatically eliminating online backup and other CSP applications, it does make one stop and evaluate whether that EU citizen data will be adequately protected.

2.2.10. State and Local Regulations

Anyone considering online backup would be wise to investigate any pertinent state and location regulations. While broader than the scope of this paper, a number of states have enacted privacy regulations that may be pertinent to anyone considering online backup services.

2.3. Industry and Standards Frameworks

Various industry and standards organizations also have frameworks that may apply to the question of whether or not to use an online backup service. Following are three representative examples of industry and standards frameworks that may be applicable to the question of using online backup. This review is not meant to be exhaustive, but rather to illustrate the types of questions that need to be raised.

2.3.1. NERC

The North American Electric Reliability Corporation (NERC) is charged with providing sound guidance and a strong standards enforcement program to ensure the reliability of the bulk power system in North America. Since June 18, 2007, NERC has had "the legal authority to enforce reliability standards with all users, owners, and

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

operators of the bulk power system in the United States, and made compliance with those standards mandatory and enforceable" (NERC).

A number of Cyber Security standards have been developed by NERC which will affect decisions relating to use of online backup services. In particular, the CIP-007 series deals with the methods, process, and procedures necessary to secure various Cyber Assets (NERC). Backup is an important component of any data security plan, and questions on whether or not online backup is appropriate would need to be evaluated by anyone covered by the NERC guidelines.

2.3.2. SAS 70

Statement on Auditing Standards No 70 (SAS 70) is a widely recognized set of standards developed by the American Institute of Certified Public Accountants. The goal of SAS 70 is to represent "that a service organization has been through an in-depth audit of their control objectives and control activities, which often include control over information technology and related processes" (SAS 70).

Any organization considering online backup should evaluate how the Cloud Service Provider meets this audit framework, as well as how using a CSP for online backup allows the organization to meet this framework. A SAS 70 audit of a CSP will generally cover these areas:

- Audit of controls based on control objectives and control activities (defined by the service provider).
- Auditor opinion on the design, operational status, and operating effectiveness of controls.
- Intended to cover services that are relevant for purposes of customers' financial statement audits (Mather, Kumaraswamy, & Latif, 2009, p. 196).

2.3.3. ISO 27000

ISO 27000 is the common name for a group of standards beginning with ISO 27001. These standards deal specifically with information security matters.

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

ISO 27001 is the specification for an Information Security Management System (An Introduction to ISO 27001). It might be important to evaluate any potential CSP for online backup to see if they meet the requirements of this audit framework. It could also be important for a business to consider how online backup will affect their desire to meet this framework.

3. Considerations When Evaluating Online Backup

From the above discussion, it becomes apparent that deciding whether or not to use an online backup service is a more complicated decision than it initially appears. So what are some of the questions that need to be answered before determining to use an online backup service?

For the purposes of this section, it will be noted from the published web documentation of the three backup providers mentioned earlier how they meet the various issues. Be aware that, as web information frequently changes, the example providers may very well have different published information available now than was available when this paper was written.

3.1. Is Regulated Data Involved?

Any organization considering online backup would do well to carefully evaluate whether the data being considered for backup is indeed regulated. The brief survey of various legal and industry frameworks has shown that maintaining the standards of these frameworks is of utmost importance.

It may be possible for the organization to separate regulated and non-regulated data. In that case, only using the online backup provider for non-regulated data may be the better choice. However, if the organization chooses to send regulated data into the backup cloud, it is wise to know how the provider meets applicable frameworks.

3.2. Which Regulatory Frameworks Apply?

It is quite possible that multiple frameworks will cover particular datasets, and therefore will have different requirements on how to manage that data. Knowing exactly

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

which data is covered by which frameworks will help the organization evaluate whether or not to use online backup.

3.3. Where does the online backup provider store data?

Each of the three example backup providers deals with this question differently. Jungle Disk backs up data into the Amazon S3 cloud. Users have a choice of backing up into either the US or the European cloud, but that's as detailed as the information is given.

Carbonite simply states that the data is backed up to their secure data centers, but nothing is specified as to where those data centers reside.

Back Blaze is the only provider that gives an actual address where the data will be ultimately stored. A brief description of the data center and security measures at the site accompanies this location statement.

In many instances, it may not be important to know the exact physical location of backed up data. However, there may also be times when the physical storage location is a relevant item. This may especially be significant when considering issues relating to privacy and legal jurisdiction.

3.4. Which Jurisdiction Controls Stored Data at the CSP?

Jungle Disk gives the user control by letting them choose to store data in either the American or EU versions of the Amazon S3 cloud. However, a user cannot go any further and know exactly where their data is stored or the physical access controls behind that data.

Carbonite doesn't give specific information on where their data is stored, so it's difficult to evaluation jurisdictional issues.

Back Blaze gives the most specific information relevant to jurisdictional control. Since the backed up data is stored at a specific address in California, there is more clarity as to the legal jurisdiction that controls the data in question.

3.5. What security controls are in place at the online backup provider?

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

Back Blaze is the only provider that offers any statement regarding physical security at their backup data location. The statement is concise, but doesn't specify how the backup location fares when evaluated against various audit frameworks.

The issue of security controls in CSPs was recently highlighted in an InformationWeek article. Author Greg Shipley provided this comment:

> When looking at cloud providers, the more relevant question is: Has this company successfully implemented the security controls necessary to manage the risks associated with our data (Shipley, 2010)?

Before committing important or regulated data to the cloud, it would be wise to consider the security controls used by the CSP and whether these controls are sufficient for the data in question.

3.6. What Encryption is used?

Carbonite simply states that they "use the same encryption techniques that banks use" and that "files remain encrypted at our secure data center" (How Carbonite Online Backup Works). Nothing is stated about the type of encryption employed, the length of applicable keys, or how the encrypted data is stored.

Jungle Disk states that they use AES-256 encryption for their backup services (JungleDisk Features).

Back Blaze provides a pretty detailed explanation of their encryption processes. Claiming that they have "military grade encryption made easy", the company further explains that they use a mix of public/private key encryption, as well as symmetric key algorithms (How to Make Strong Encryption Easy to Use).

3.7. Who Has Access to the Recovery Key?

In the three example providers being considered, recovery is controlled by a password. Some online providers allow their technical support staff the ability to access data unless the client chooses a particular type of backup key.

Carbonite allows the user to recover files with just a few clicks of the mouse from the desktop. This means that any individual with access to that desktop has the potential to recover files. The business edition of Carbonite allows a company administrator to

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

control access to everyone's files for that company (How Carbonite Online Backup Works).

Jungle Disk likewise allows recovery from the desktop client. They also allow access to the backed up files from the web, so any individual who had control of the logon credentials could potentially access the stored data (JungleDisk Features).

Back Blaze likewise allows restore directly to the desktop. This company will also provide a DVD or USB drive that can be sent to you with the stored data (Internet Backup Made Easy).

3.8. Is Everything Needed for Recovery Available?

A common problem is that an organization will implement a backup plan without testing that plan. Then when recovery is needed, it is found that not all the files necessary for recovery were included in that backup plan.

Online backup will have similar issues. Any organization that chooses to implement online backup should test and verify that all the files needed for recovery are indeed available. Meeting this requirement might involve implementing a combination of online and local backup.

3.9. Is There Sufficient Bandwidth?

By definition, any online backup service will require bandwidth. The amount required will vary, and be based on a number of considerations:

- Frequency of backup
- De-duplication efficiency
- Quantity of file changes

Before implementing an online backup program, it would be wise to estimate the bandwidth usage and see if this is appropriate for the organization.

3.10. How is Recovery Access Controlled?

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

Each of our example online service providers controls recovery access with a logon and password combination. Protecting that credential combination is a critical piece of maintaining the security of the backed up data.

3.11. Is CSP Compliant with Regulatory Frameworks?

While some online backup providers will provide statements of HIPPA, SOX, or EU Safe Harbor compliance, none of the three example providers have those provisions stated.

3.12. Does the Provider have a Liability Agreement?

Each of the three example providers have detailed terms of service. As an example, Carbonite offers this comment in the Limitation of Liability section of their Terms of Service (original in all caps):

> IN NO EVENT WILL CARBONITE, THE CARBONITE CONTRACTORS, CARBONITE DISTRIBUTORS OR CARBONITE SUPPLIERS BE LIABLE TO YOU OR TO ANY THIRD PARTY FOR ANY LOST PROFITS, LOST DATA, INTERRUPTION OF BUSINESS, OR OTHER SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY KIND ARISING OUT OF THE USE OR INABILITY TO USE THE CARBONITE PRODUCTS OR SERVICES OR TO USE OR RETRIEVE ANY BACKUP DATA, WHETHER FOR BREACH OF WARRANTY OR OTHER CONTRACT BREACH, NEGLIGENCE OR OTHER TORT, OR ON ANY STRICT LIABILITY THEORY, EVEN IF CARBONITE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGES OR A REMEDY SET FORTH IN THESE TERMS OF USE IS FOUND TO HAVE FAILED OF ITS ESSENTIAL PURPOSE, AND WHETHER OR NOT SUCH LOSS OR DAMAGES ARE FORESEEABLE (Carbonite Products and Services Terms and Conditions of Use).

An organization considering online backup should carefully examine these service terms to decide if the provider meets their regulatory and security liability requirements.

Steve Strom, steve@stevestrom.com

© 2010 SANS Institute, Author retains full rights.

3.13. Does the CSP have a Service Level Agreement?

None of the example providers offer a Service Level Agreement on their website. In fact, Carbonite offers this interesting note in the Warranties section of their Terms of Services:

> Carbonite and the Carbonite Affiliates do not warrant that the functions contained in the Carbonite Products or Services will meet your requirements, that the operation of the Carbonite Products or Services will be uninterrupted or error-free, or that defects in the Carbonite Products or Services will be corrected. Carbonite and Carbonite Affiliates do not warrant or make any representations regarding the use or the results of the use of the Carbonite Products or Services in terms of their correctness, accuracy, reliability or otherwise. Carbonite and Carbonite Affiliates do not represent or warrant that users will be able to access or use the Carbonite Products or Services at times or locations of their choosing, or that Carbonite and Carbonite Affiliates will have adequate capacity for any user's requirements (Carbonite Products and Services Terms and Conditions of Use).

Given that no guarantee of recovery availability is made, an organization may want to evaluate the suitability of these terms for their particular organization.

4. Conclusion

The decision on whether or not to implement online backup in an organization is not a simple question. While it may initially appear that such a service is the easiest answer to the need for backup, in many cases it is not the best or most appropriate choice.

Online backup providers do have a place. It appears from this study that they would work best for small organizations dealing with non-regulated data. Other organizations with regulated data could indeed use such a service provider, but only after carefully considering the consequences of using such a service in their environment.

Steve Strom, steve@stevestrom.com

© 2010 SANS Institute, Author retains full rights.

5. References

An Introduction to ISO 27001. (n.d.). Retrieved March 21, 2010, from The ISO 27000 Directory: http://www.27000.org/iso-27001.htm

Bunker, D. G., & Fraser-King, G. (2009). Data Leaks for Dummies. Indianapolis: Wiley Publishing, Inc.

Carbonite. (n.d.). Retrieved March 19, 2010, from Carbonite: http://www.carbonite.com

Carbonite Products and Services Terms and Conditions of Use. (n.d.). Retrieved April 18, 2010, from Carbonite: http://www.carbonite.com/terms/

Cherry, S. (2009, October). Cloud Computing Drives Mobile Data Growth. Retrieved March 19, 2010, from IEEE Spectrum: http://spectrum.ieee.org/telecom/wireless/cloud-computing-drives-mobile-data-growth

CompTIA. (2008). CompTIA Security+ Certification, 2008 Edition. Axzo Press.

Gantz, J. F., Chute, C., Manfrediz, A., Minton, S., Reinsel, D., Schlichting, W., et al. (n.d.). The Diverse and Exploding Digital Universe. Retrieved March 17, 2010, from EMC Corporation Web Site: http://www.emc.com/collateral/analyst-reports/diverse-exploding-digital-universe.pdf

How Carbonite Online Backup Works. (n.d.). Retrieved April 18, 2010, from Carbonite: http://www.carbonite.com/how_it_works/

How to Make Strong Encryption Easy to Use. (n.d.). Retrieved April 18, 2010, from Backblaze Blog: http://blog.backblaze.com/2008/11/12/how-to-make-strong-encryption-easy-to-use/

Hurwitz, J., Bloor, R., Kaufman, M., & Halper, F. (2009). Cloud Computing for Dummies. Hoboken: Wiley Publishing, Inc.

Internet Backup Made Easy. (n.d.). Retrieved April 18, 2010, from BackBlaze: http://www.backblaze.com/internet-backup.html

Steve Strom, steve@stevestrom.com

© 2010 SANS Institute, Author retains full rights.

Jungle Disk. (n.d.). Unlimited storage for workgroup, team & employee files. Retrieved March 20, 2010, from Jungle Disk: http://www.jungledisk.com/business/workgroup/pricing/

JungleDisk Features. (n.d.). Retrieved April 18, 2010, from JungleDisk: http://www.jungledisk.com/business/workgroup/features/

Knorr, E., & Gruman, G. (n.d.). What Cloud Computing Really Means. Retrieved March 17, 2010, from InfoWorld: http://www.infoworld.com/d/cloud-computing/what-cloud-computing-really-means-031

Mather, T., Kumaraswamy, S., & Latif, S. (2009). Cloud Security and Privacy, 1st Edition. O'Reilly Media, Inc.

NERC. (n.d.). About NERC. Retrieved March 21, 2010, from North American Electric Reliability Corporation: http://www.nerc.com/page.php?cid=1

NERC. (n.d.). Reliability Standards. Retrieved March 21, 2010, from North American Electric Reliability Corporation: http://www.nerc.com/page.php?cid=2|20

Nufire, T. (n.d.). Petabytes on a budget: How to build cheap cloud storage. Retrieved March 20, 2010, from Backblaze Blog: http://blog.backblaze.com/2009/09/01/petabytes-on-a-budget-how-to-build-cheap-cloud-storage/

Photopoulos, C. (2008). Managing Catastrophic Loss of Sensitive Data. Burlington: Syngress Publishing, Inc.

Preston, W. C. (2007). Backup & Recovery, 1st Edition. O'Reilly Media, Inc.

SAS 70. (n.d.). About SAS 70. Retrieved March 21, 2010, from SAS 70: http://www.sas70.com/about.htm

Shipley, G. (2010, April 12). Cloud Computing Risks. InformationWeek , pp. 20-24.

Smith, D. M. (n.d.). Data Loss and Hard Drive Failure. Retrieved March 19, 2010, from DeepSpar Data Recovery Systems: http://www.deepspar.com/wp-data-loss.html

Steve Strom, steve@stevestrom.com

© 2010 SANS Institute, Author retains full rights.

Stewart, J. M., Tittel, E., & Chapple, M. (2008). CISSP: Certified Information Systems Security Professional: Study Guide, Fourth Edition. Indianapolis: John Wiley & Sons.

Van Dusen, W. R. (n.d.). FERPA: Basic Guidelines for Faculty and Staff. Retrieved March 21, 2010, from NACADA Clearinghouse of Academic Advising Resources: http://www.nacada.ksu.edu/Resources/FERPA-Overview.htm

Whitman, D. M., & Mattford, H. J. (2009). Principles of Information Security, Third Edition. Boston: Cengage Learning.

© 2010 SANS Institute, Author retains full rights.

Steve Strom, steve@stevestrom.com

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

Last Updated: May 22nd, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**