Don’t be Caught in the Perfect Cyber-Storm

Leigh Ann Fulkerson
Nov. 6, 2015

Using the cloud for data storage is increasingly risky. Here are some of the factors why data-critical companies should consider a move out of the cloud to a ***hardened, not hosted*** data storage environment. After all, when you're dealing with a storm, the safest place is in a hardened storm shelter.

Data is Co-mingled in a Constantly Changing Environment

For the end user, cloud computing services appear to be structured very simply. However, the structure *inside* the cloud is inherently complex. In a typical cloud environment, multiple customers share physical databases, file servers, web servers and disk spaces. Customers' data are rarely physically separated. Moreover, organizations’ business requirements and cloud needs are constantly changing. As a result, regular restructuring of security controls becomes essential. It’s a daunting task for a third party to maintain security controls in such a dynamic and complex environment, not to mention the fact that there are multiple customers, multiple systems, and massive quantities of data.

Shifting Responsibilities Can Create Gaps

The cloud is generally an off-premise, distributed system in which users outsource their data management needs to a third party provider. The provider may do everything from performing software updates, hardware maintenance and managing security protocols. In the typical cloud environment, users trust their data into the care of employees they likely have never met. Organizations can often overlook their own responsibilities when they rely on the cloud to store their business information in cloud-based applications. While the service provider may do its best (or not), it cannot ensure absolute safety at the subscriber’s end. Organizations must ensure that their own systems are constantly updated with security patches; that all users with access to the cloud have been authorized; and that encryption keys are safeguarded. Sometimes there are communication or personnel gaps which can lead to security gaps.

Increasing Sophistication of Cyber-attacks

The hacker community is increasingly more organized and better funded. This support comes from interested parties including myriad criminal organizations and even governments. The change in the level of sophistication is evident in the speed at which vulnerabilities are exploited, the damaging capabilities of attacks and the hyper-functionality of sophisticated malware. It is increasingly difficult to completely ward off such powerful attacks. *Any data* on the Internet is at risk for theft, loss or corruption, but it is particularly problematic in a cloud environment, where volumes of data are stored by all types of users on the same system. Data on the cloud is concentrated and vulnerable to Distributed Denial of Service (DDoS) attacks, as it is easier to steal and disrupt data en masse. Most cloud providers have stringent security measures, but as technology evolves, unfortunately, so do the efforts of cyber-criminals.

Threats from the Inside

Just as the number of cyber-attacks is on the rise, so are security breaches from the inside. From the thousands of reports of accidental loss or theft of a connected mobile device such as a smartphone, tablet or laptop, to the unintentional negligence of staff, or perhaps the desire for personal gain -- insider threats are real. Once an employee gains, or gives others, access to the cloud, confidential information is potentially up for grabs. Any amount of security is not enough if there are vulnerable users in the system. Despite all the training and awareness programs, people make mistakes and thus unintentionally expose the whole system to security risks. People continue to use easy or predictable passwords, share accounts, and fall prey to phishing / vishing attacks. In the end, the hackers need just a small crack to penetrate.

Government Intrusion & Surveillance

With the recent NSA leaks and the myriad government surveillance programs, we see that competitors aren't the only ones who may want to take make use of private data. Government entities and technology companies in the U.S. and elsewhere may be inspecting data as it is transmitted or where it resides in the Internet, including within clouds. Privacy has always been a concern with the cloud, but instead of worrying about corporate competitors, unhappy customers, terrorists, or simply employees breaching cloud security protocols, businesses now have to worry about government intrusion as well. Major cloud services providers are feeling increasing pressure to allow Government snooping, and they can be *required* to hand over data in certain cases.

Legal Jurisdiction of Distributed Data

Risks associated with the cloud are not limited to security breaches. They also include the after-effects, such as lawsuits. The latest risks to using cloud for business are compliance, legal liability and business continuity. Data breach incidences are on the rise, and as a result, so are lawsuits. Owing to the distributed nature of cloud computing, it is not easy (at times it is impossible) for a subscriber to know exactly where their data is located. It may be in a different data center in a different city, state or even another country. Unless jurisdiction is certain, it is difficult to get the assistance of law enforcement, and thus for exposed clients to recover from breaches. This situation works to the advantage of the hacker community and many times cyber-criminals continue to remain at large, all the while getting better at hacking.

Lack of Cloud Standardization

What makes a cloud computing environment "safe"? A provider could have installed the latest security features, but due to the general lack of cloud standardization, there are no clear-cut guidelines for all cloud providers. Given the plethora of cloud services in different sectors, as well as how different types of businesses utilize the cloud, it especially difficult to determine exactly how "safe" a cloud provider really is. The safety depends on several variables including protocols of the provider; the type of industry and entities that are using the cloud-based services; the type of information on the cloud; and the accompanying regulations concerning the type data stored in the cloud (such as HIPPA, FTC, ITAR, etc.). Since not all cloud providers are built to achieve the same goals, one provider's definition of "safe" may not be the same as another's.

Data Retrieval Issues & Down-Time

Imagine being unable to access your data before an important meeting or, worse, dealing with a cyberattack that has taken down your entire website. What if an entire segment of critical files, such as clients' financial records or patients' health information, were completely lost or corrupted? Now imagine trying to download a massive amount of backed-up data in order to restore your files and get back to normal business operations. Anyone who has ever downloaded a large file from the web knows that the connection speed, the amount of internet traffic, and the size of the file all have a direct impact on the download speed. If your data or online presence is critical for the smooth operation of your business (and therefore the bottom line), even with specifically designed solutions, clients must be prepared to wait many hours before getting all data restored from a cloud environment, which likely means lost revenue.

The Cloud can Never be 100% Risk-Free

As technology advances, so do the risks that come with its adoption. Given these current and future dangers, it is important to weigh the benefits of cloud computing against these serious risks. Though there are many benefits to using the cloud for some daily operations, collaboration, and the utilization of some cloud-based applications, the cloud is certainly not a one-size-fits-all solution. Using a typical cloud environment as a storage, back-up and/or recovery solution for critical, sensitive or regulated data remains especially risky. If the data, the hardware, and the encryption keys are not completely under control, there is always some degree of uncertainty and risk.

Powerful Protection is Hardened, not Hosted

Companies like VaultedData, LLC are providing a niche solution which virtually eliminates the risks of the cloud by storing your mission-critical data on your own co-located hardware inside a hardened facility in a known physical location. Only the client's authorized staff have escorted, in-person (or virtual) access to the hardware, software and encryption keys that remain in 100% ownership of the client. Physical security is multi-layered, and even in the unlikely event of a physical breach, or if the hardware were confiscated, it would be difficult to impossible to access the encrypted data without the encryption keys. No data is co-mingled and only data back-up clients are allowed in the facility, which virtually eliminates the attack surface for would-be hackers. If a disastrous event requires a complete recovery of data, it is available *immediately and in totality* by picking up the hardware in person or having it couriered to you in specialized, locking cases. Down-time is significantly reduced with what is, essentially, a 100% scaleable, plug and play solution. This kind of data storage is ***hardened, not hosted*** and could help you get the best of both worlds. Often, these services are more affordable than the same amount of data storage on the cloud.