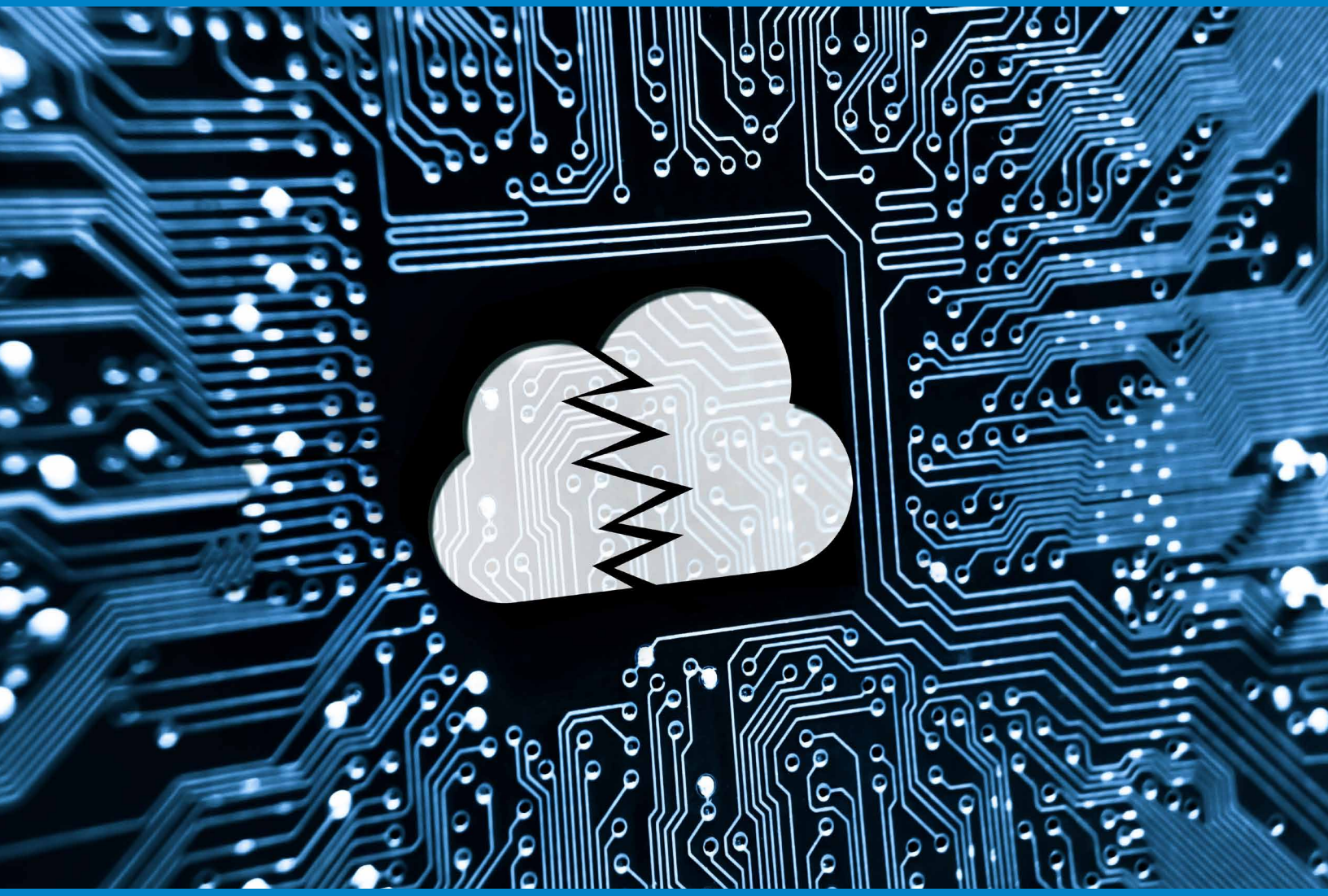
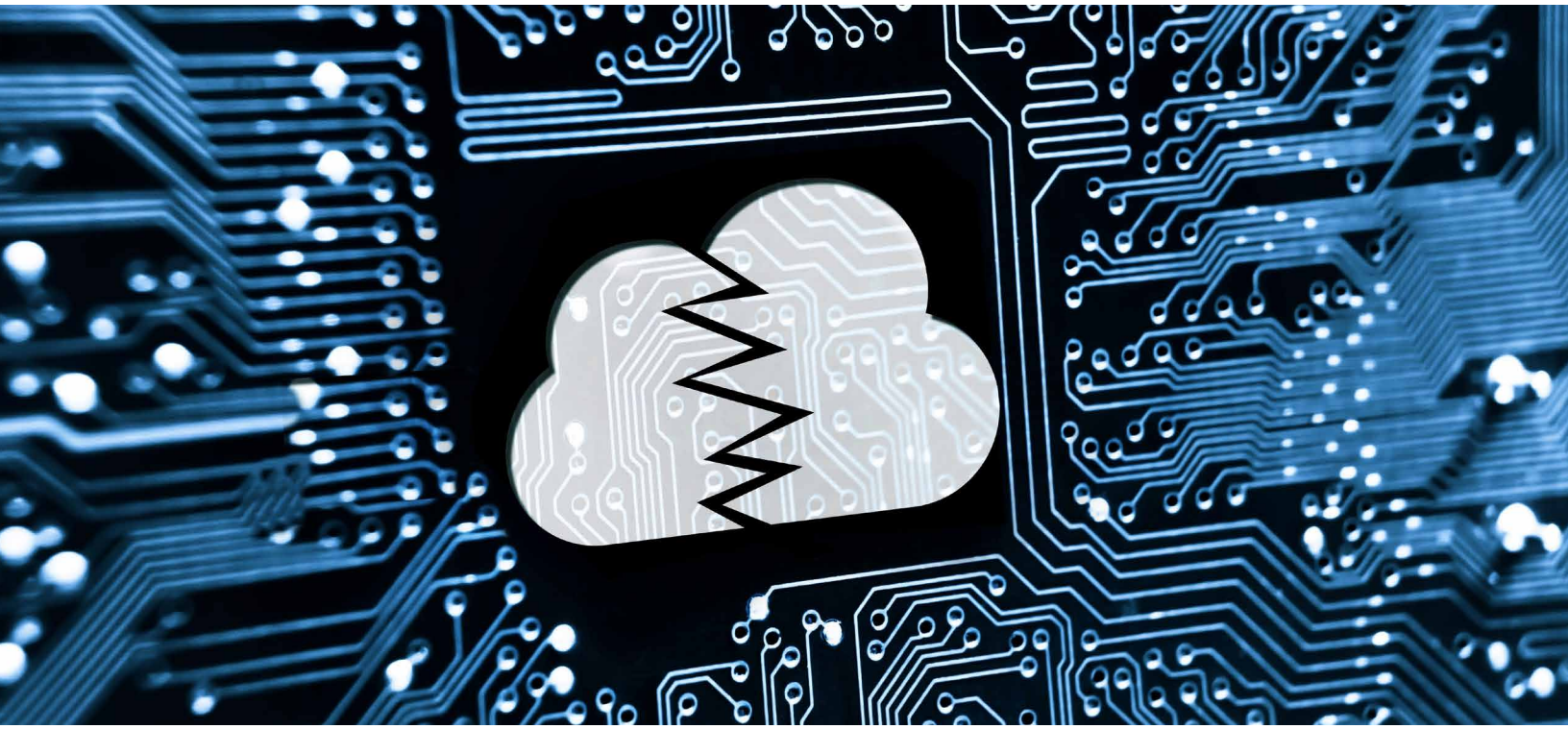
MyWorkDrive

The Risks of Cloud Storage



MyWorkDrive.com



The Risks of Cloud Storage

For all of the benefits cloud storage options provides, we cannot ignore the potential risks of public cloud computing. Even though every public cloud storage provider will tell you that your data is safe and secure, we know from reports of cloud hacks on celebrities and companies that there is no such thing as guaranteed safety when storing information in the cloud.

Take law firms, for example. Law firms may be another weak link when it comes to

protecting confidential data, which you didn't even consider. According to an article in The Recorder, lawyers lack the IT infrastructure and security we come to expect with banks, retailers, and our medical records – yet they are handling confidential information and sending it over unsecured networks and personal devices. If a lawyer puts confidential data on a flash drive and then loses the flash drive, or stores data in an insecure public cloud– it puts the client at risk. When choosing a lawyer, you might want to consider their data security systems before going with a particular firm.

Here is a list of four risks every business should consider before storing your critical data with a public cloud service:

Public Cloud = Shared Access

When you're talking about the public cloud, and storing your business data in a place that has shared access, you are exposed to some risks. Sure, the cloud provider is going to ensure security to the best of their ability. But a small flaw in how information is secured and stored could result in one cloud storage customer assuming the identity of another cloud storage customer of the same public cloud. Or, as some researchers into the security of cloud storage have discovered, when a new company signs up for cloud storage and takes over recently vacated storage space – sometimes they were able to

recover the memory and IP address of whoever was using that “space” before they moved in.

Authentication and Access Control Risks of the Public Cloud

When you store your business files in the public cloud, your cloud vendor chooses authentication, authorization, and access control mechanisms. It’s possible that many people who work for the cloud provider have access to your data. It’s also possible that you may share a common namespace with the cloud provider and even other clients of the cloud provider. With single-sign-on authentication options that make it easy to get into your data, it can increase your risks if there are shared namespaces. These are questions all companies should ask their public cloud provider, but you may not get overly detailed answers about how it all works. There is a potential for unknown security risks when you give up control of your data to the cloud provider.

Risk of Losing Your Data

When you store your information with a public cloud provider, one of the benefits of that storage is that it provides an off-site backup of your data. When reading the benefits of each provider’s service offering, no doubt they tell

you your data is completely backed up and accessible – but it seems every month a new major cloud provider is down for hours or days while companies are unable to access the data they stored with that provider.
In some cases, customers have lost data permanently when the cloud provider lost information that wasn't as backed up as they thought; or from malicious hackers. Storing data with a public cloud provider puts your backup and continuity planning in their control. If you do decide to use a public cloud provider, make sure you also back up that data on your own, somewhere else, just in case the company fails to provide an adequate backup and disaster recovery plan.

Some Public Cloud Providers Take Over Ownership of Your Data

The most surprising risk for most companies is realizing that when you upload your company data to a public cloud provider, you may not own it anymore. If you take a close look at the fine print in the contract of many cloud providers, you will find that the cloud provider, not you, owns the data you save with their cloud service. The reason cloud providers want to own the data they're storing is because it gives them better legal protections in the event something goes wrong. It also opens the door for new revenue

opportunities for them – for example, if a cloud provider goes out of business they may sell the data they've stored for their customers to the next owner of the business.

Do you really want to give up ownership of your business data? This is a risk that opens the door to many new risks should the ownership of the cloud company change hands.

MyWorkDrive: All of the Benefits of the Public Cloud Without the Risks

Sometimes the benefits of storing your data in the cloud outweigh the risks, at least until you realize there are other options that offer the benefits without the risks! MyWorkDrive from Intivix provides remote access to your files without physically storing them in the cloud or sharing space with other companies.

MyWorkDrive is a hosted service that ties into your existing file servers to provide users simple and secure remote access to files and folders from anywhere, using any browser or mobile device while you maintain corporate control. This set up allows you to enjoy all the benefits of the cloud with local file access and control, while reducing the security exposure associated with using the public cloud.


MyWorkDrive