THE NATIONAL CYBERSECURITY SOCIETY

HOW TO SELECT A CLOUD SERVICE PROVIDER

Has your company leveraged free data storage? Who hasn't? Like Google Drive, Dropbox, SugarSync or GitHUB? Do you know where your data is being stored and how it is protected? Do you know who has access to your data? Have you reviewed the fine print – under Terms and Conditions, and even if you did, have you thought about whether you can decline certain elements of their contract?

Fundamentally, cloud computing is a delivery of computing in a service format. The term "cloud" is a term used to describe the aggregation of servers and applications into a cohesive ***service*** that provides highly scalable and distributed access to resources in a variety of formats. Utilizing the idea of economies of scale, cloud providers can provide more cost effective solutions to their customers – you basically buy only what your need, when you need it – or in some cases get it for free.

We believe that the small business owner needs to balance the convenience of the cloud storage solution with the security needs of your company. Cloud storage is definitely the preferred solution – as compared to not backing up your data or storing them on an unprotected computer or server in your office. Many cloud solutions provide security – and we are here to help guide you through the process of selecting a cloud "secure" storage provider.

DID YOU KNOW?

- ✓ Many free cloud storage services are just what they say they are – free! You use these services at your own risk, and under their terms and conditions.
- ✓ Files are seldom encrypted, data transfer is not encrypted, data is commingled with other users, and the companies who hold your data can also access your data (if legally required to do so).
- ✓ The flip side is that these services are just what a small business owner needs – economical, easy to use, and provide a quick and easy way to back up your data and collaborate among users – in the office or on the road.
- ✓ Protect your business from ransomware by having critical data backed up in a secure location.

STEP 1: DOCUMENT IDENTIFICATION

Identify what documents you need to back up. Are these sensitive files? In all likelihood they are, since you have decided that they are important enough to backed up at a remote location. If you have temporary files that remote users/employees need access to, then selecting a free service will work for that business situation.

The best way to do decide what to back up is to develop a business needs statement. What this document does is lay out the requirements for your cloud storage solution. Elements to consider are: automatic backup (you establish the periodicity), file syncing, encryption of files before backup, encrypted data transmission, ease of use (does this service work well with other applications and services you are using), authentication, collaboration (multiple users can collaborate on a document at the same time), e-signatures (different parties can

Still have questions, need help?
Contact us at our **"Ask-an-Expert"** service,
web@thencss.org or visit us at the link below.

JOIN THE NCSS

Become a member of **The National Cybersecurity Society** today and learn more about how to protect your business from a cyber attack.

Cloud Service Provider continued...

sign and return legal documents), cost (what you are willing to pay for the service, or what would you pay if these files were corrupted or stolen) number of users who need access to these files, location of the data center. (U.S. or international locations). Prioritize the requirements and/or indicate the level of importance. You will use these criteria to select the provider.

STEP 2: ESTABLISH THE BUSINESS RULES

Establish a policy, write it down, communicate and train your employees. Without a descriptive policy statement or business rule, employees either won't know what is required, not implement it, or implement based upon their own understanding of what is required. If these documents are sensitive, you might want to establish more business rules on who has access to these sensitive files.

An example would be personnel or financial files – clearly you will want to limit access to these records. Typically, a data owner is identified – who will make the decisions on the data, how long it needs to be kept, the level of sensitivity, who has access, and under what conditions. If you have limited staff, the business owner of the company can decide. Define how long these files will be kept and under what conditions – 5 years is usually the maximum required. (The "Data Protection Act" requires personal data processed for any purpose "shall not be kept for longer than necessary for the purpose." This act states the maximum period of retention is regarded as 5 years.

STEP 3: SELECT THE CLOUD SERVICE PROVIDER

Evaluate and select a cloud "secure" service provider. Using your business needs statement, start the process of selecting a provider. As a minimum, all sensitive documents should be encrypted before transit to the data center and while stored at the data center. Some types of data require encryption during transmission (meaning the routing and session information about your transmission is encrypted as well). Other items to consider in evaluating your cloud secure storage provider: business references; how long the entity has been in business; what is their reliability (meaning percentage of uptime, usually 99.8% or greater); how they select their employees, security of the facility; and facility location.

As part of the evaluation process, read the fine print of the cloud service agreement and determine if you can change the terms of service to meet your specific needs. Learn about their breach notification procedures - find out how you will be notified and how long after a breech will you be notified. Will you learn on the nightly news or after all of their other larger clients are notified? In reading the fine print, determine if

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.

Cloud Service Provider continued…

the burden of encryption prior to transfer is your responsibility and if it is stored on a commingled server with others. Evaluate the cloud service back up plan, in the event that the server your data is stored on goes down, how often do they backup their client's data. Bottom line is to make sure your sensitive data remains protected and recoverable.

Evaluate the other services the cloud storage provider offers – such as automatic backups and file syncing capabilities and determine how these services align with your security needs. You probably don't want to have an auto back feature that copies unencrypted files from your desktop to the cloud service provider, unless the cloud service provide encrypts your files prior to transfer.

Authentication – ensure your cloud storage service offers two-factor authentication, to protect your data from theft or compromise. Two-factor authentication offers a means to authenticate your users with the cloud service using two types of authentication – usually a password and a token.

Encryption – there are different types of encryption and different needs based upon the type of data. Health care information and credit card transactions require data be encrypted while stored on the servers (at the cloud) and during transmission. AES 256 is currently the strongest encryption but comes in AES 128/192/256.

Changing Providers/Data Destruction – during the evaluation period determine the method of changing providers – how will you move your data from one provider to another? How will you be assured that no data resides on the previous cloud service provider? These are important elements to consider before you transfer all of your data to one provider, and then learn, it is not so easy to move. Something that might seem low cost now, may end up a year from now costing you a bundle. Have a **back-out** plan for your data.

STEP 4: VERIFY AND VALIDATE

No business policy or process is effective without periodic review and assessment. Examples include: periodic review of company policy to determine if your goals for secure storage are being followed by your employees; assessment of the cloud service contract (are you still happy with the service, has the cost changed); review the cloud storage incident history during the year (what security incidents occurred and your assessment of their ability to respond); and lastly, test your recovery procedures – to ensure the data you stored is recoverable, and your employees know the procedures.

Storing your data in the cloud is safe and secure if you know the factors to consider. And lastly, not having a back up of your critical business data is probably the biggest risk a small business owner faces.

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.

Cloud Service Provider continued...

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.