nCrypted Cloud

470 Atlantic Avenue
Boston, MA 02210
Office: +1.617.520.4120

QUESTIONS AN ENTERPRISE SHOULD ASK TO ENSURE SECURE CLOUD STORAGE

Executive Summary

Enterprises need to maintain their privacy, security and compliance posture when using cloud-based file storage and sharing technology.

If enterprises are to gain the business benefits of cloud storing and sharing technology; they must select a solution that provides the necessary privacy and security capabilities.

This means enterprises must get satisfactory answers to questions relating to:

- Deployment capabilities to ensure successful implementation.
- Privacy mechanism to ensure information stored or shared remains confidential.
- Security safeguards to ensure information is protected at all times.
- Secure hosting by the cloud service provider to ensure reliable safekeeping of the information.

Cloud-based File Storage and Sharing – Level Setting

Cloud-based file storage and sharing is the underlying technology to access, synchronize, and share documents or files anywhere, anytime, with anyone, and from any device using a cloud-based storage providers such as Dropbox.

Cloud-based file storage and sharing is an enabling technology for enterprises to deliver better customer services, support BYOD, improve business collaboration, and more importantly, innovate business processes for competitive advantage.

Enterprises want to gain the competitive and cost advantages that cloud-based storing and sharing technologies deliver.

The challenge for enterprises is to select a solution that provides the necessary privacy and security safeguards and reliable hosting services that enterprises require.

Questions that need to be answered

Below are the vital questions that an enterprise needs to ask while evaluating and assessing a secure cloud-based storage and sharing solution.

Enterprises must assess whether the solution has the capabilities necessary to successfully deploy. That the solution provides the necessary mechanisms to preserve the confidentiality of the information and offers the safeguards to ensure the information is protected, all the time, and in all places.

Finally, an enterprise must ensure the service provider delivers reliable and secure computer processing facilities to ensure high availability and business continuity.

Questions to ask relating to deployment capabilities

Usability, deployment, and enterprise administration capabilities are critical to ensure a successful implementation and to manage the day to day operation of a secure cloud-based storage and sharing solution. Key questions to ask are:

- Does the solution provide a user experience that consumers expect? (aka as a consumer-centric design that is predominant in mobile computing.)
- Are there enterprise administrative capabilities to readily provision consumers?
- Does consumer have delegation capabilities to securely share information with clients or business partners to foster collaboration?

Questions to ask relating to privacy safeguards

Ensuring that the confidentiality of the information stored in the cloud and shared among individuals or devices is crucial for all enterprises. Privacy related questions to ask include:

- Is the information persistently encrypted especially at rest on mobile devices (i.e. smart phones, tablets) and traditional devices (i.e. personal computers, laptops)?
- Are there confidentiality features to restrict access to information at desired minimum levels? (e.g. read only, watermarking, termination date triggers, etc.)

Questions to ask relating to security safeguards

Enterprises need the administrative capabilities to securely manage cloud-based file storage and sharing activities. Enterprises need means to enforce security policies and have the monitoring capabilities to ensure compliance. Security related questions to ask include:

- Are only explicitly authorized individuals allowed access to information?
- Are all access events captured and logged for monitoring and reporting purposes? (who, what, when, and where)
- Is there an audit facility to easily monitor activity?
- Can access be terminated at the individual, folder, or document level when it is no longer needed?
- Are there forensic and data loss prevention capabilities?

.

Questions to ask cloud service provider

Enterprises need to ensure that information stored at the service provider in the cloud is secure, highly available, and recoverable in case of a disaster. Questions to ask the cloud service provider include:

- Do they adhere to generally accepted safe computing practices? (e.g. physically secure data center, system and application change controls, secure network)
- Do they have backup and restoration capabilities to ensure timely restoration of services in case of a disruption? (e.g. backups, fail over capabilities, recovery plans)
- Do they have Third Party report such as a third party report (e.g. SSAE 16 or SAS/70, ISO certification) to attest to their computing practices and controls?
- If personal health information (PHI) is involved, are they willing to sign a Business Associate Agreement (BAA) asserting they are HIPAA compliant?

Conclusion

Enterprises need to assess and select the cloud-based storage and sharing solution that will provide the necessary privacy and security safeguards.

This assessment needs to include gaining assurance that the deployment, privacy, security, and cloud hosting capabilities will be sufficient to maintain the desired compliance and security posture.