WTA-13: Secure Clouds?

We all are the test team for a medium sized company (say 1,000 people).

Due to the desire to spread to small regional offices, but keep key documents available we are looking at cloud options to store important documents. We want to make this as easy for our users as possible, so we are exploring numerous options in the marketplace today. There are some famous names like Dropbox, Sugar Sync, etc. that we can consider. But the big concern with corporate is security. How can we make sure that what we put online is safe?

Our mission is to explore testing options, and examine various services (pick additional versions if the two I've mentioned don't float your boat). Report back on what we can do to test and confirm this approach (or not confirm it).

Wow, this is secure! ;-)

Requirement #1: more secure than typewith.me ;)

Expectation of safety and privacy

* secured with passwords or other devices (key cards, fingerprint scans, etc,)

* data is available to those who should have access when needed, and data is not available to anyone else

Security:

Does the system integrates with the, say, Kerberos authentication of our Intranet? (I know I'm repeating myself, but this redirects the user/pass questions to a different direction)

Passwords: Passwords might have requirements such as length, required to contain certain of: caps, lowercase, numbers, letters, punctuation. There may be requirement to change passwords with some regularity.

SSL Encryption

Boundary Area: there should be a demarcation and level of access for certain areas. sections that I would want to keep open, and areas I would want to keep closed to just me.

Methods of Testing:

* Try methods of intercepting communications between client and server (in both directions: upload and download).
* Check different permissions types: read only, read write, etc.
* Check different permission groupings: individuals, groups, roles, etc.
* Could server load affect performance and even functionality?
* Move files between public and private spaces (large files, many files). can we catch them in the transition state?
* Using a cloud service to spin up large amounts of file transfer to and from the service.
* Try to spoof passwords and see how many I could crack.
* See if public areas could allow for back door access to private areas (API, etc).

Additional considerations:

* credibility of service provider
** ability to grow and accommodate large organizations
** trust in the organization to service requests securely

* look at security beyond the front door. does authorized access as one user unintentionally give access to other info. e.g.: recent url hacking of bank website that gave hackers logged in as one user access to others' data

* social engineering can outweigh any considerations to actively securing hardware an software. the human element can undermind any and all security safeguards.