To Cloud or Not to Cloud

By Stewart C. W. Weiner
and Brian A. Nettleingham

Recent weeks have seen widespread media reports discussing “hacked” accounts and stolen data, from celebrities such as Jennifer Lawrence and Kate Upton to businesses like Home Depot, PF Changs, and Target. These reports have forced many people to consider the potential risks that accompany the advantages of cloud computing.

By “cloud computing,” we mean the practice of using programs or data storage on remote servers, rather than locally on a private computer or server. The term encompasses everything from simple data storage to complex programs run on remote systems. For example, a company may use a cloud-based service to process sale transactions, where portions of the transactions actually occur on a remote server.

Cloud computing is here to stay, of course, and its use is growing rapidly. It is likely that your company currently uses the cloud in at least some way as part of your business operations. Even if your company has not implemented an enterprise-wide cloud solution, it is almost certain that your employees are using cloud accounts – whether from desktops or mobile devices – to work efficiently.

Are you comfortable that you have mitigated the associated risks? A discussion with a legal professional might be beneficial. Below is a brief list of some of the advantages and disadvantages of cloud-based solutions and a few relatively simple steps you can take to make the cloud experience more secure.

Potential Advantages of the Cloud:

- File sharing and quick access to data across multiple platforms.
- Maintenance and security software updates can be automatically pushed out to devices.
- Cloud-based services can reduce IT costs by reducing the need to purchase and/or maintain technology infrastructure.

- No hardware or software installation.
- Centralized document control and storage.
- The flexibility to work from anywhere, internally or remotely.
- Environmentally friendly, as experts claim that cloud computing uses approximately 30% less energy consumption and carbon emissions than on-site servers.

Potential Disadvantages of the Cloud:

- Security is only as good as the service provider, and data stored in the cloud can be at greater risk of attacks from third parties, malware, etc.
- Confidentiality and privacy of data can be a concern. By definition, cloud computing involves the transfer of information to a third party for storage and access. If that information is confidential or regulated (such as non-public personal information from consumers or clients), extra precautions may need to be taken.
- Access to the cloud-based storage or services is dependent on internet connectivity, so if you lose the connection, you may lose access.
- Ownership of data stored in the cloud may be an issue, depending on the service. In some cases, even though you provide the data and consider yourself the owner, some cloud providers include provisions in their terms of use that expressly state that the service provider owns any uploaded data, not the customer.
- Control. Someone else is maintaining your data and access depends on the service provider.
- Government review given the NSA leaks and concerns about government intrusion.

Potential Steps a User and Customer Should Consider:

- For business cloud users, request a copy of the provider’s last audit report.
- Ask the provider about prior data compromises and data losses.
- Ask the provider about its policy concerning the reporting of data losses.
- Encrypt your data before you upload it.
- Although this advice is frequently provided, do not make it easier for the professional cyberattackers by using the same password on all accounts, especially those accounts that are sensitive, such as banking, brokerage accounts, credit card accounts and the like. Use different passwords for each account for which sensitive and private information is provided and

change those passwords routinely.

- Whenever it is available, take advantage of two-step authentication. With two-step authentication, once a user provides his or her password, the account will send the user either a text message or email with a separate code that is needed to access the account. Apple (for iCloud), Google (for its Gmail service) and a number of banks are making this service available.
- When all else fails, if you remain nervous or wary of risks involved in cloud computing, then the best course of action may be to obtain your own secure server, maintain it and limit connections to the server.
- For personal cloud storage, consider Amazon Cloud Drive, Apple iCloud, Dropbox, Google Play and Google Drive and Microsoft SkyDrive, but be mindful that the consumer accounts available through these providers do not typically provide the security required for storing regulated data (such as a consumer’s non-public personal information).