**HOW SECURE IS THE CLOUD?**

New York-based investment banking and financial services firm Cowen and Co. has moved its global sales systems to the cloud using Salesforce.com. So far, Cowen's CIO Daniel Flax is pleased. Using cloud services has helped the company lower upfront technology costs, decrease downtime and support additional services. But he's trying to come to grips with cloud security issues.Cloud computing is indeed cloudy, and this lack of transparency is troubling to many.

One of the biggest risks of cloud computing is that it is highly distributed. Cloud applications and application mash-ups reside in virtual libraries in large remote data centers and server farms that supply

business services and data management for multiple corporate clients. To save money and keep costs low,

cloud computing providers often distribute work to data centers around the globe where work can be

accomplished most efficiently. When you use the cloud, you may not know precisely where your data

are being hosted, and you might not even know the country where they are being stored.

The dispersed nature of cloud computing makes it difficult to track unauthorized activity. Virtually all cloud providers use encryption, such as Secure Sockets Layer, to secure the data they handle while the data are being transmitted. But if the data are stored on devices that also store other companies'

data, it's important to ensure these stored data are encrypted as well.

Indian Harvest Specialtifoods, a Bemidji, Minnesota-based company that distributes rice, grains, and legumes to restaurants worldwide, relies on cloud software provider NetSuite to ensure that its

data sent to the cloud are fully protected. Mike Mullin, Indian Harvest's IT director, feels that using SSL (Secure Sockets Layer) to encrypt the data gives him some level of confidence that the data are secure. He also points out that his company and other users of cloud services need to pay attention to

their own security practices, especially access controls. "Your side of the infrastructure is just as vulnerable, if not more vulnerable, than the provider's side," he observes.

One way to deal with these problems is to use a cloud vendor that is a public company, which is

required by law to disclose how it manages information. Salesforce.com meets this requirement, with

strict processes and guidelines for managing its data centers. "We know our data are in the U.S. and we

have *a* report on the very data centers that we're talking about, " says Flax.

Another alternative is to use a cloud provider that give subscribers the option to choose where their cloud computing work takes place. For example, Terremark Worldwide Inc. is giving its subscriber

Agora Games the option to choose where its applications run. Terremark has a Miami facility but is adding other locations. In the past, Agora had no say over where Terremark hosted its applications

and data.

Even if your data are totally secure in the cloud, you may not be able to prove it. Some cloud

providers don't meet current compliance requirements regarding security, and some of those

providers, such as Amazon, have asserted that they don't intend to meet those rules and won't allow

compliance auditors on-site.

There are laws restricting where companies can send and store some types of information—personally identifiable information in the European Union (EU), government work in the United Sates or applications that employ certain encryption algorithms. Companies required to meet these regulations involving protected data either in the United States or the EU won't be able to use public cloud providers.

Some of these regulations call for proof that systems are securely managed, which may require

confirmation from an independent audit. Large providers are unlikely to allow another company's

auditors to inspect their data centers. Microsoft found a way to deal with this problem that may be helpful.

The company reduced 26 different types of audits to a list of 200 necessary controls for meeting compliance standards that were applied to its data center environments and services. Microsoft does not give every customer or auditor access to its data centers, but its compliance framework allows auditors to order from a menu of tests and receive the results.

Companies expect their systems to be running 24/7, but cloud providers haven't always been able to provide this level of service. Millions of customers of Salesforce.com suffered a 38-minute outage in early January 2009 and others several years earlier. The January 2009 outage locked more than 900,000

subscribers out of crucial applications and data needed to transact business with customers. More

than 300,000 customers using Intuit's online network of small business aplications were unable to access these services for two days in June 2010 following a power outage.

Agreements for services such as Amazon EC2 and Microsoft Azure state that these companies are not going to be held liable for data losses or fines or other legal penalties when companies use their services. Both vendors offer guidance on how to use their cloud platforms securely, and they may still be able to protect data better than some companies' home-grown facilities.

Salesforce.com had been building up and redesigning its infrastructure to ensure better

service. The company invested $50 million in Mirrorforce technology, a mirroring system that creates a duplicate database in a separate location and synchronizes the data instantaneously. If one database is disabled, the other takes over. Salesforce.com added two data centers on the East and West coasts in addition to its Silicon Valley facility. The company distributed processing for its larger customers among these centers to balance its database load.