

Tech report

Just be careful that you don't get lost in the cloud

Premium content from Philadelphia Business Journal by Ned Dunham, Guest columnist

Date: Friday, January 20, 2012, 6:00am EST

Related:

[Insurance](#), [Technology](#)

It's catchy. It's cool. And many businesses have bought into the idea that "cloud computing" means saving a ton of money while at the same time exponentially increasing information technology capabilities. There is considerable upside in converting to this paradigm-shifting approach, but companies also need to exercise some necessary precautions.

We begin by demystifying the term. Cloud computing is a marketing term that refers to any set of Web-hosted services, files or applications that are used over the Internet. It is a hugely scalable way to use the Internet to service multiple external customers.

There's a lot to like about it. Gartner Inc., the technology research and advisory company, thinks that the evolution of cloud computing is no less influential than the advent of e-business. Users can access applications through Web browsers for desktop and mobile apps and thereby save development costs. Shared services and infrastructure convergence make it easier to get applications up and running more quickly with lower development costs and less maintenance and are easier to manage during their operational life. These capabilities provide significant cost savings for users who now are not paying for 80 percent to 90 percent excess capacity which they will rarely, if ever, use. On-demand access, or just-in-time access with just the right amount of capacity, makes for more efficiency and less cost. The use of multiple, redundant sites improves reliability and addresses some security concerns.

The value-added proposition is significant. Small- and mid-sized businesses can scale their usage to meet demand and launch new service offerings, products and internal processes that they simply could not have afforded if they had to do it with their own individual hardware and software.

Like most other new technology, however, informed prudence is in order before letting your intellectual property, trade secrets and other information you are charged with

keeping private, out of your direct control. When engaging cloud computer vendors, you may be taking the data out of your safe and putting it in someone else's equally strong safe, or you may be putting it into someone else's shoe box. Weak systems that are easily penetrated and critical encryption issues fall into the latter category. With careful and knowledgeable planning, you can address the most important operational issues and get the most from your cloud-based system.

When switching its IT operations to cloud computing, a business trades the control of its data and processing for greater efficiencies and cost reductions. This loss of control has a number of risks. Data may be located in servers in various jurisdictions around the world, creating potential legal problems when a dispute arises between a business and its cloud vendors. With access over the Internet, the potential for successful hacking increases exponentially. There may be serious security issues if the third-party vendors do not protect a business' data like it is their own. Encryption of data, in its several forms, is a major issue that businesses need to address competently to ensure that not only is their data secure but that they have continuous access to it. Finally, the availability of insurance coverage for losses incurred when a business, or its customers, lose access to data and processes, is critical and may be complicated.

These risks can and should be controlled by careful lawyering in close cooperation with IT experts and knowledgeable insurance brokers and underwriters. Contracts with cloud providers absolutely must address the following:

- n Where your data is stored and how you can remove it and at what cost.
- n What kind of security safeguards the vendor will apply to your data.
- n What limits of liability the vendor is imposing in the event of a loss.
- n Who will control a data breach incident response and bear the cost.
- n Whether the vendor will indemnify the organization and under what circumstances.

The most significant insurance issue, beyond coverage for data breaches and the significant associated costs, is indemnification for business interruption losses. A promising coverage for these kinds of losses is contingent business interruption, or CBI coverage. The thorny issues of whether data and processing losses are physical property losses and therefore covered are being dealt with by a number of courts around the country as this is being written. The complexity of the issues demands knowledgeable insurance coverage lawyering and insurance brokering and underwriting.

Cloud computing technology is not an unmixed blessing. For sure, its advantages are so significant that it is here to stay. Managing its risks is not a job for amateurs, however, but if done well, will pay significant dividends in both positive cash flow through significant cost reductions and in avoiding entirely preventable losses.

NED DUNHAM is a litigator specializing in insurance coverage and risk management at the Philadelphia law firm of **Kleinbard Bell & Brecker** and also the co-inventor of an automated, algorithm-based cyber-risk assessment and remediation process. He can be reached at edunham@kleinbard.com and at 267-443-4109.

Cyber Security

Are you asking the right questions about your cyber risk?

Premium content from Philadelphia Business Journal by Ned Dunham

Date: Friday, December 9, 2011, 6:00am EST

Related:

[Technology](#), [Human Resources](#)

Every day we are inundated with a stream of information about the dark side of the cyber world. But while the Internet poses substantial challenges to our personal and commercial security, the very technology that underpins it also enables real-time, cost-effective and readily available cyber risk assessments that will help you protect yourself.

Selecting an assessment program that fits your needs and level of risk is critical to saving time and money. A really good assessment will be cost effective for the size of your company, assess both legal and IT risks, enable a rapid turnaround, present graphical comparisons of the risk areas addressed and will be attorney-client privileged. What follows are some risk factors to consider as you decide on the assessment process that suits you best.

First you should determine your company's overall cyber activity profile. The extent and nature of a firm's day-to-day Internet activity is a necessary base line in establishing the risk profile of an organization of any size. Companies that market and sell goods and services online have, by definition, a high cyber-risk profile. Companies that only put up informational websites with no e-commerce component have a low-risk profile.

This does not mean that companies in the low-risk category are off the hook. Many companies with passive websites pay very little attention to their cyber security because they believe their low-risk profile makes them invulnerable to attack. When hackers stole and compromised sensitive client information and protected personal information from one such local company, it paid dearly in legal fees and additional security costs in addition to suffering professional embarrassment and loss of business.

Next to consider are security policies and procedures. You may employ the most qualified technical personnel and sophisticated hardware and software, but you will not achieve the desired level of security without the appropriate policies and procedures in place. You might consider adopting an enterprise-wide policy governing regulatory compliance, including the destruction of sensitive information and departure procedures. A security

awareness program for employees, vendors and contractors who access, handle or process sensitive customer data is essential. Good contingency planning will include procedures for handling breaches of data security. If you store information in "the cloud" it's important to know precisely where your data is stored, what, if any, restrictions your cloud provider has in moving the data without informing you, and who controls the rights to the all-important encryption keys. A first-rate assessment will ask these kinds of questions and address the effectiveness of your electronic and physical security including firewalls, intrusion prevention and encryption requirements.

A privacy policy ensures that an organization does not breach its obligations to protect sensitive information it acquires, uses, processes or transmits to others. Control procedures for mobile devices are particularly important, as is employee access to personally identifiable information. An organization-wide privacy policy and established procedures to prevent the unauthorized removal of sensitive company information on mobile devices are critical in the process of securing your data against costly privacy breaches.

Then there are legal considerations. A reasonable legal risk-avoidance action plan, authored by knowledgeable attorneys, would include procedures for reviewing website content that could infringe others' intellectual property rights as well as intellectual property compliance procedures that include a document control, retention and destruction policy covering both physical and electronic data. This policy will stand you in good stead should you need to defend yourself in litigation.

Social media is a cornucopia of legal and information technology risks. Establishing a social media policy for all employees, both on-the-job and at-home, is not easy, but it's critical to your company's security. At the very least, you need to consider the legal, human resources and public relations ramifications of monitoring any social media sites used by your employees, and of using social media sites in the employment application process. The policies you put in place will depend on your company's organizational structure, its marketing philosophy, and a number of legal considerations.

At the end of the day, you can pay a lot or not so much for cyber-risk assessments. Major consulting and accounting firms will take quite a bit of your time, issue an IT-oriented report, and charge you in the tens of thousands. Also available from smaller firms are semi-automated processes which are front-end loaded, meaning the work has been done in asking the right questions and in making the right remediation recommendations based on your answers. These types of solutions will take less of your time (less than a day if you make the right people available to answer the questions), cost much less (in the several thousand dollar range), and highlight your vulnerabilities in a way you can understand and process to give you some much-needed comfort.

NED DUNHAM is a litigator specializing in insurance coverage and risk management at the Philadelphia law firm of **Kleinbard Bell & Brecker** and also the co-inventor of an automated, algorithm-based cyber-risk assessment and remediation process. He can be reached at edunham@kleinbard.com and at 267-443-4109.