Mitigating Security Risk in the Cloud

Interest in cloud computing is on the rise, but security concerns linger. This paper discusses how best to protect your data in the cloud.

EXECUTIVE SUMMARY

Cloud computing isn’t for start-ups anymore. Recent surveys reveal that the biggest growth in cloud computing deployments is among companies with higher revenues. They’re discovering the financial value—lower costs, economies of scale, and easier budgeting—of employing cloud-computing solutions for a variety of applications and situations.

But with that value come security concerns: Who’s responsible for security, compliance and governance? What kind of effect does cloud computing, which is virtual rather than physical, have on these aspects? Companies must figure out how to create holistic policies while accommodating both virtual and physical infrastructures to avoid overwhelming their IT departments with specialized solutions.

THE LURE OF CLOUD COMPUTING

Cloud computing is not a new concept. Two decades ago, the Internet was represented on flow charts as a cloud, simply because its decentralized architecture took information in and routed it somewhat invisibly to its final destination. Ten years ago, vendors touted themselves as application service providers, companies that would let customers access infrequently used applications online for a fee, so that the latter could avoid the cost of deployment and management.

More recently, consumers have begun to take advantage of cloud computing through hosted systems that store photographs (Flickr), files (Google Docs), and even information...
How Symantec Helps Mitigate Cloud Computing Risk

Symantec is already helping companies manage their cloud computing challenges. Symantec solutions for cloud computing are optimized to address a variety of information security, availability and management challenges.

Symantec focuses on five key areas to ensure its customers have confidence in the cloud:

Security and compliance. The cloud model requires secure interfaces between users and endpoints (the outermost devices on a network); between endpoints and backend infrastructure; and between services. Each of these interfaces presents a technical, operational and contractual challenge, but Symantec security, access control and compliance solutions are designed to manage the information on both sides of these interfaces.

Availability. Public and private cloud providers depend on system availability and uptime. Symantec has developed clustering, replication, high availability and disaster recovery solutions to achieve the necessary reliability.

Storage management. Virtual environments require an optimized storage management capability for the most appropriate allocation and utilization. Symantec solutions in this area leverage low-cost data and storage servers to make scalability possible. Symantec FileStore platform also helps customers build and manage internal cloud storage capabilities.

Data protection. Symantec solutions provide multiple virtualization technologies and offer advanced management and reporting that help cloud administrators handle their backup requirements. These include deduplication and archiving solutions for offline data management, disk-based replication, tiered storage, and retention.

Endpoint virtualization. Endpoint virtualization helps users benefit from applications delivered through portable devices that create secure client environments, insulated from underlying client OS and patch considerations. The devices allow applications to be centrally managed and streamed to users on demand if necessary.

Interest in cloud computing is on the rise, as evidenced by a recent survey of more than 7,000 C-suite executives, conducted by PricewaterhouseCoopers in conjunction with CIO and CSO magazines. Some 43 percent of respondents said they were using some form of cloud computing, whether in terms of software, platform or infrastructure. Interestingly, the larger a company’s annual sales, the more likely it was to have a cloud computing strategy.

There are several reasons for this. One is cost, even beyond the capital vs. operational expense argument. In the past,
companies have been burned by enterprise software deployment projects that dragged on far beyond their original schedule, sucking up resources without providing the business with the features it needs to compete. A prebuilt application run by a third-party provider within a SaaS environment eliminates that uncertainty.

And though enterprises are not turning over their infrastructures to service providers on a wholesale basis, they can do so in targeted, specific ways by using IaaS (infrastructure-as-a-service). For instance, some companies are moving older, less critical systems to cloud computing providers. Others are relying on third-party providers for storage and archiving or, given the increased flexibility that virtualization technology brings, for high-availability disaster recovery.

Cloud computing platforms are also being used for pilot projects. PaaS (platform-as-a-service) eliminates the need for IT to procure, set up, and machine new servers and gives business units the opportunity to investigate new possibilities. Salesforce.com and Microsoft offer PaaS capabilities. They provide preconfigured applications, servers for companies to test applications, and are making concerted efforts to groom add-on applications.

By accommodating the needs of projects in this way, IT still maintains knowledge of systems and can work with the cloud-computing vendors to maintain appropriate governance (more about governance later).

CONCERNS ABOUT THE CLOUD

Despite the growth in use and popularity of cloud computing systems, CSOs maintain significant concerns about them. Not surprisingly, IT executives worry about keeping company data safe and accessible, 24/7—it is, after all, their responsibility. According to the PricewaterhouseCoopers survey, they fear a loss of control, influence, or audit capability within the third-party provider's environment (see chart, "Perceived Risks In Cloud Computing").

There are ways to mitigate the concerns around cloud computing. One relates to the first rule of outsourcing: maintain strong ties with your service provider. If there’s a high level of concern about QOS, CSOs must ensure that the level of access they want is built into the service-level agreement (SLA); uptime must be audited regularly to ensure that it conforms to the SLA.

The same concepts apply to security and privacy. If executives ensure that service providers are well-educated about their company’s specific regulatory needs, and those needs are addressed accordingly, there’s less chance of a problem. Similarly, CSOs and service providers must exchange information about where the latter places its servers physically to ensure conformance with specific regional privacy and security regulations.

Meanwhile, technology is advancing significantly enough to lessen some concerns. Though virtualization technology is making multi-tenancy (the hosting of multiple companies’ data on a single server or rack) easier, companies can still ask service providers to keep their servers separate. Virtualization technology is also making availability and backup systems less expensive to maintain, while broadband and other high-speed networking technology is becoming more reliable and less expensive.

Admittedly, cloud computing represents a new cultural mindset for IT. The inability to physically touch servers brings uncertainty, and working with third-party providers may require a different set of skills and training for IT staff. But by offloading a large proportion of maintenance and monitoring activities, IT has the opportunity to work more closely with business units on strategic technology issues, rather than tactical ones.

Companies must be aware that the financial and business benefits of cloud computing will ultimately overtake IT’s reluctance and reticence. Similarly, C-suite executives should be aware that bypassing IT’s security expertise can be a

<table>
<thead>
<tr>
<th>PERCEIVED RISKS IN CLOUD COMPUTING</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uncertain ability to enforce security policies at a provider</td>
</tr>
<tr>
<td>Inadequate training and IT auditing</td>
</tr>
<tr>
<td>Questionable privileged access control at provider site</td>
</tr>
<tr>
<td>Uncertain ability to recover data</td>
</tr>
<tr>
<td>Proximity of data to another customer’s</td>
</tr>
<tr>
<td>Uncertain ability to audit provider</td>
</tr>
<tr>
<td>Uncertain continued existence of provider</td>
</tr>
<tr>
<td>Uncertain provider regulatory compliance</td>
</tr>
</tbody>
</table>
recipe for disaster. Lobel tells the story of a business unit that went to its IT department to develop and deploy an application, one with clear revenue-generating potential. The IT department estimated a 10-month schedule and a $130,000 cost.

Frustrated, the executives went to a third-party infrastructure provider, getting the same application at a quarter of the cost and in less than a month. Because the deployment was so successful, the CEO gave the business unit an award. However, Lobel cautions, “The CEO never asked where the data was, whether it was secure, and if anyone was applying consistent and effective controls to confirm its security.”

So what can CSOs do to ensure that they avoid situations like this?

**CREATING THE SECURE INFRASTRUCTURE**

The answer to mitigating cloud risks is to develop a secure, holistic infrastructure—one that encompasses both physical and virtual computing systems no matter where they reside, and no matter where data resides. Call it a hybrid model. In a way, accommodating security for cloud computing is simply an extension of dealing with security for mobile devices. As the boundaries of where data resides have been expanding to laptops and smartphones, they must expand to virtual systems, including those run by third parties.

This means thinking about data security based on content instead of location so security regulations become consistent no matter where data resides. For IT, it’s a three-step process:

- Establishing high-level information security policies for protecting data
- Establishing more granular compliance-related policies for specific departments, such as finance and human resources
- Establishing processes for auditing and improving policy effectiveness

Once a consistent internal policy has been developed, it’s time to start looking at what third-party service providers can contribute. This process doesn’t differ from most other outsourcing procurement plans. It involves:

- conducting a cost/benefit analysis
- ensuring the third-party service aligns with business objectives
- identifying regulatory and privacy requirements
- developing a contingency plan and exit strategy

It is crucial that third-party providers understand your unique privacy and security requirements, so look for providers with industry experience and a background in handling your specific needs. Contingency plans are important because you need to have a way to handle your data should the relationship not work out. As Lobel puts it, “Ask yourself if you can get information security in the cloud. Is your data protected and used appropriately while it’s in the cloud? And can you get the data out again?”

Once you’ve established that your traditional security and governance activities map to a cloud computing scenario, you’ll be well on your way to creating a holistic structure that accommodates both on-premise and off-premise infrastructures.

---

**FURTHER RESOURCES**

- Symantec in the cloud: [www.symantec.com/cloud](http://www.symantec.com/cloud)
- Symantec Hosted Services: [www.symantec.com/hostedservices](http://www.symantec.com/hostedservices)

Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries.