**Cloud Computing Home Assignment #2**

**Security issues with your SaaS Application**

Assignment by:

BE-E-21: Neha Bhagwat

BE-E-24: Sarvesh Darak

BE-E-25: Abhishek Dayama

BE-E-37: Shreya Kawtikwar

BE-E-49: Pritam Patange

BE-E-52: Aishwarya Patil

There are numerous security risks to look at before adopting software-as-a-service. Here are five problems to consider.

**1. Identity management in the cloud is immature**

Cloud providers themselves aren't always sophisticated about integrating their platforms with identity services that exist behind the enterprise firewall, says Forrester analyst Chenxi Wang.

[Google](http://code.google.com/securedataconnector/docs/1.3/overview.html) has a "Secure Data Connector" that forms an encrypted connection between a customer's data and Google's business applications, while letting the customer control which employees may access Google Apps resources. Salesforce provides a similar tool.

But this approach may become unwieldy because customers that use numerous SaaS applications could find themselves dealing with many different security tools, she notes. Third-party products at least offer the advantage of connecting to many different types of SaaS applications.

Identity and access management in the cloud has a long way to go.

"Managing identities and access control for enterprise applications remains one of the greatest challenges facing IT today," according to research from the [Cloud Security Alliance](http://www.cloudsecurityalliance.org/guidance/csaguide-dom12-v2.10.pdf). "While an enterprise may be able to leverage several cloud computing services without a good identity and access management strategy, in the long run extending an organization's identity services into the cloud is a necessary prerequisite for strategic use of on-demand computing services."

Unfortunately, the evolution of SaaS has outpaced efforts to build comprehensive industry standards, the Cloud Security Alliance says. Specifically, the group says there is "limited proprietary support for user profiles," and industry standards including Service Provisioning Markup Language (SPML) have not been significantly updated in several years.

**2. Cloud standards are weak**

There's no guarantee that your data will be safe with an ISO 27001-compliant vendor, however. One survey of IT managers commissioned by [CA](http://www.ca.com/files/supportingpieces/quocirca_priviledgd_usr_mgmt_oct_19_09_219925.pdf) found numerous companies that claim to be compliant with ISO 27001 yet "admit to bad practices with regard to privileged user management," including sharing of administrator accounts between users and granting broader privileges to users than is necessary.

The case of Google engineer [David Barksdale](http://www.networkworld.com/news/2010/091510-engineer-fired-for-privacy-violations.html) further illustrates the problem that companies may not follow their own guidelines. Google, like other vendors, have strict privacy policies for their employees. But those policies reportedly did not prevent Barksdale from accessing Google Voice call records and Gmail and Google Chat accounts of several Google users, and he was subsequently fired.

**3. Secrecy**

Cloud vendors argue that they are more able to [secure data](http://www.networkworld.com/news/2010/05251-cloud-apps-misconceptions.html) than a typical customer, and that SaaS security is actually better than most people think. But some customers find this hard to believe because SaaS vendors tend to be rather secretive about their security processes.

In particular, many cloud service providers release very few details about their data centers and operations, claiming it would compromise security. However customers and industry analysts are getting fed up with all the unanswered questions and hush-hush nondisclosure agreements.

Service-level agreements (SLA) have [sometimes proven deceptive](http://www.networkworld.com/community/node/45816) or confusing. But at least in theory, enterprises should be able to receive strong guarantees in SLAs, particularly if they have the time and expertise to negotiate with the vendors beforehand.

"The entire software-as-a-service environment is really driven by SLAs," says CTO Joe Coyle of technology consulting and outsourcing firm Capgemini. "If you really think about it, there's nothing you would do in SaaS that isn't SLA-based."

In some cases, if the vendor is willing, a customer may be able to bring in its own experts and attempt to hack the vendor's network in order to test security, Coyle says.

**4. Access everywhere increases convenience, but also risk**

One major benefit of software-as-a-service -- that business applications can be accessed wherever there is Internet connectivity -- also poses new risks. Coupled with the proliferation of laptops and [smartphones](http://www.networkworld.com/news/2010/092110-why-i-switched-to-android.html), SaaS makes it even more important for IT shops to secure endpoints.

Maintaining control over e-mails and documents is easier when those files are stored on your local servers, rather than in the cloud.

Enterprises that make use of SaaS need to implement policies to control connectivity, MacDonald says. A customer could, for example, work with the SaaS vendor to make sure a service can be accessed only from certain IP addresses, and require remote users to go through a VPN, he says.

Access can also be regulated by using secure [Web gateway appliances](http://www.gartner.com/technology/media-products/reprints/cisco/article6/article6.html) from [Cisco](http://www.networkworld.com/subnets/cisco/) or Blue Coat, which broker the connection between a customer and cloud services. In one simple example, a company could allow employees access to Facebook, but block the chat feature. The approach of blocking access to certain types of functionality can be applied to business-focused cloud services as well, MacDonald notes.

There is also the problem of employees accessing SaaS products without IT knowledge. The keys to preventing this, Wang says, are educating employees and using various network monitoring and Web filtering technologies.

**5. You don't always know where your data is**

Regulations such as the Federal Information Security Management Act (FISMA) require customers to keep sensitive data within the country. Although keeping data within U.S. borders seems like a relatively simple task on its face, cloud vendors will often not make that guarantee.

In highly virtualized systems, data and virtual machines can move dynamically from one country to another in response to load balancing needs and other factors. Google, for example, would note that if an end user in California goes on a business trip to London, it's better (or at least faster) for that user's data to be served up by a data center in Europe.

[Google Apps](http://www.networkworld.com/news/2010/042810-google-apps-microsoft-office.html) has received FISMA certification for its government cloud, but that same guarantee is not available to private industry. This isn't just a problem for U.S. customers either.

Symantec, which has data centers in 14 countries, does offer an in-country guarantee, according to Trollope.

But this is still considered a relatively rare feature. Even if data stays within a country, customers need to be able to verify the data's location in order to meet regulatory requirements. That's why EMC says it is developing [technology to track and verify](http://www.networkworld.com/news/2010/083010-emc-fisma-compliance.html) the location of virtual machines in cloud networks. But this technology will not hit the market until early next year, and it requires integration between EMC, VMware and Intel products.

"Right now, there's nothing that provides any verifiability of where a virtual machine lives," says Chad Sakac, vice president of the VMware technology alliance at EMC. "There's nothing stopping you from moving a VM from one place in the world to somewhere else, and more importantly, there's no way to audit that at any sort of scale."

