

A Brief Security Overview of Cloud Computing

What Is The Cloud?

The term 'cloud' in 'cloud computing' actually originates from network diagrams which depict the Internet as a cloud. A large number of services and applications can be considered a part of the 'cloud'. Cloud computing can be roughly summarized as a virtual computing and storage environment that is managed and hosted by third parties. These third parties present a vast amount of computing power, storage, and accessibility at much lower financial and administrative cost than most companies can provide on their own.

Cloud computing services may vary, but the one defining component they all share is that all of the data, services, and applications they provide are stored outside of the customer's physical location. Use of any cloud computing services puts part of your infrastructure, and therefore your security, in another company's hands. Your administrators and managers must carefully evaluate the technical, legal, and security implications of any arrangement with a cloud computing provider prior to any setup.

Who Are The Major Providers?

The biggest providers of cloud computing services are Amazon Elastic Compute Cloud (EC2) with Amazon Simple Storage Service (S3), Google App Engine, and Microsoft Live Mesh. Many more companies, like IBM and Dell, also offer a variety of personal and commercial cloud computing services as well. These services include hosting packages, word processing software, spreadsheets, and telecommunication offerings.

What Are You Putting In The Cloud?

It's important to identify *what* you will actually be putting in the cloud and make the distinction between applications and data. The degree of risk associated with cloud computing is directly related to the sensitivity of the data that will be stored, processed, or transmitted using a cloud computing service. It is critical to determine the level of sensitivity of the information that your company and employees will be trusting the third party provider to secure from both internal and external threats.

Where Exactly Is Your Data In The Cloud?

Most of the major providers of cloud computing services do a good job of physically protecting the machines used to host and process applications and data. These providers house the physical servers in world-class datacenters; however data may be spread across several different servers in geographically separate locations. This setup increases the reliability of the cloud service but makes it difficult to establish and evaluate the security controls *all* of your data is under. Ideally, it is expected that the third parties internal standards would ensure that the controls for each physical location are uniform, although you won't know unless you read the customer agreement and talk to the vendor.

Read The Customer Agreement

Many of the technical and security questions your managers and administrators will want answered can be found in the customer agreements posted by the third party providers. While it should be obvious, don't use the cloud computing services of any third party vendor that doesn't display or provide a customer agreement with sufficient detail to make your security and risk decisions. Members of your legal team and technical staff should review all customer agreements to discern the limitations, protections, and potential regulatory conflicts.

Your Responsibilities

Your internal information security policies and practices should govern whether a cloud computing arrangement is acceptable in your organization. If you do not have formal information security policies in place, focus your efforts there to start. Involve legal, technical, operations, and management individuals to ensure you create acceptable policies, and create training materials to educate your organization about information security.

Once your information security policies are in place, use the customer agreement and contact the provider to get additional information. Ensure you know how your data will be handled if there are any grey areas and ask to review as many of the technical details they are willing to disclose. Clarify and ask for amendments to any part of the customer agreement which may not meet your policies. Have a security analysis conducted on the access points to the cloud servers, machines, and applications anywhere they are or have access to your internal network. And remember, endpoint security is often the weakest link; be sure that the systems at each end are protected from malware and patched frequently.

For More Information

If you have any questions about the contents of this document, or are interested in learning more about risk analysis, risk assessment, or risk management, please contact:

Peter Hesse (pmhesse@geminisecurity.com) or Laura Raderman (lraderman@geminisecurity.com)
Gemini Security Solutions, Inc. 4451 Brookfield Corporate Dr. Suite 200 Chantilly, VA 20151
703-378-5808 <http://geminisecurity.com>

About Gemini Security Solutions

Gemini Security Solutions, Inc. provides impartial information security consulting services that ensure the confidentiality, integrity, and availability of critical business information and resources. Our value is centered on our ability to deliver the right expertise and the right experience, at the right time.

Founded in 2001, and with decades of experience, our certified team of experts assists organizations to assess and deliver security solutions in compliance with business strategy, policy and regulatory requirements. Our services include risk analysis and management, regulatory compliance, identity access and management, operations security, and security software development.

Gemini Security Solutions is focused on providing big business experience with a small business approach. Working with you every step of the way, Gemini Security Solutions enables secure business operations with vigor, agility and a commitment to excellence.