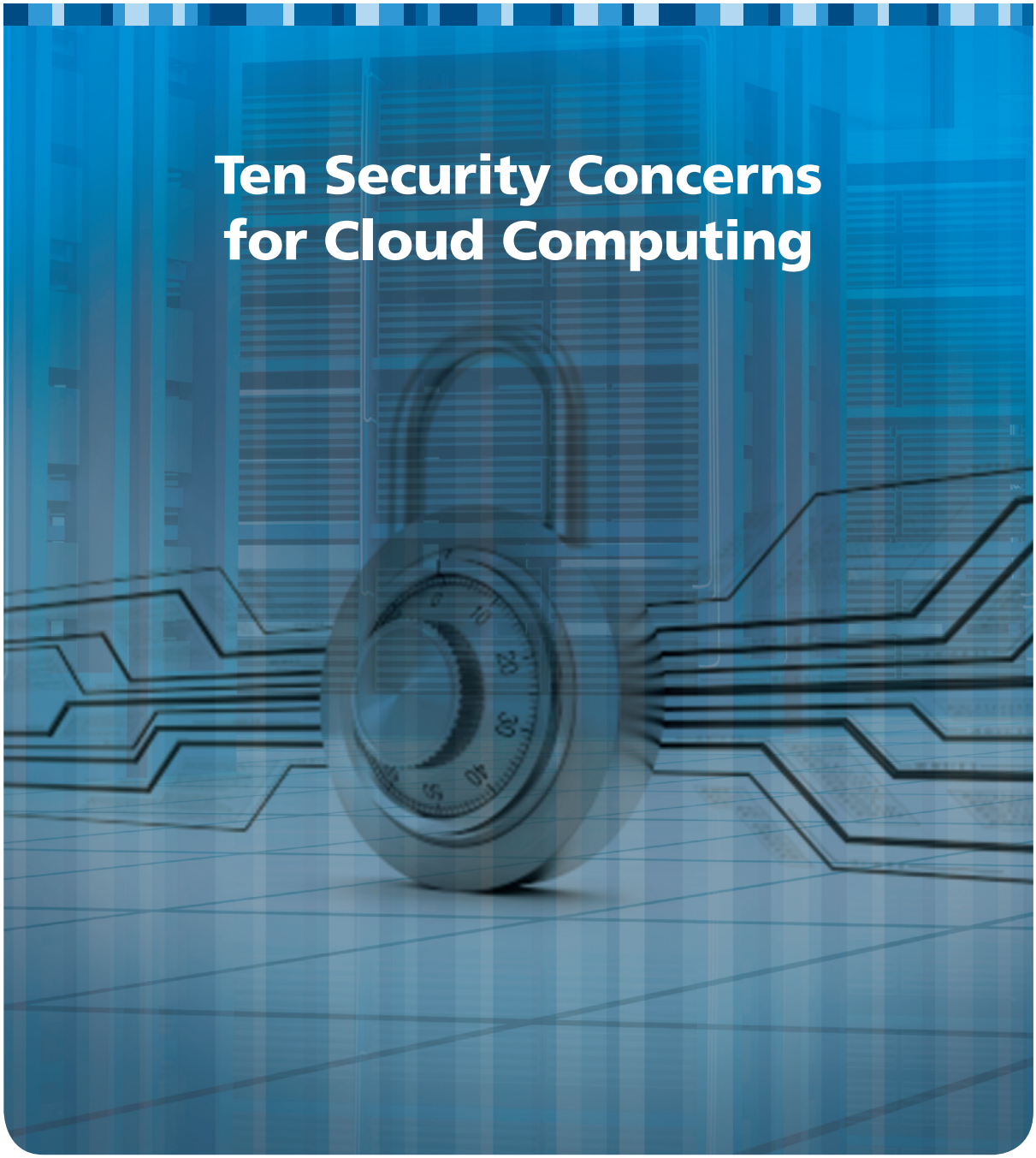
Global Knowledge®

Expert Reference Series of White Papers

Ten Security Concerns for Cloud Computing



info@globalknowledge.net www.globalknowledge.net

Ten Security Concerns for Cloud Computing

Michael Gregg, Global Knowledge Instructor, CISA, CISSP, CISM, MCSE, CTT+, CGEIT, A+, N+, Security+, CNA, CCNA, CIW Security Analyst, CEH, CHFI, CEI, DCNP, ES Dragon IDS, ES Advanced Dragon IDS, and SSCP

Introduction

Cloud computing gets its name from the drawings typically used to describe the Internet. Cloud computing is a new consumption and delivery model for IT services. The concept of cloud computing represents a shift in thought, in that end users need not know the details of a specific technology. The service is fully managed by the provider. Users can consume services at a rate that is set by their particular needs. This on-demand service can be provided at any time.

The Evolution of the Cloud Services

Infrastructure as a Service (IaaS) → Platform as a Service (PaaS) → Software as a Service (SaaS)

Cloud Computing Models

Cloud computing models can be broken into three basic designs, which are shown here and described below.

- Infrastructure-as-a-Service (IaaS) – As the name implies, you are buying infrastructure. You own the software and are purchasing virtual power to execute

as needed. This is much like running a virtual server on your own equipment, except you are now running a virtual server on a virtual disk. This model is similar to a utility company model, as you pay for what you use. An example is Amazon Web Services at http://aws.amazon.com/.

- Platform-as-a-Service (PaaS) – In this model of cloud computing, the provider provides a platform for your use. Services provided by this model include all phases of the system development life cycle (SDLC) and can use application program interfaces (APIs), website portals, or gateway software. Buyers do need to look closely at specific solutions, because some providers do not allow software created by their customers to be moved off the provider's platform. An example of PaaS is GoogleApps.
- Software-as-a-Service (SaaS) – This model is designed to provide everything and simply rent out the software to the user. The service is usually provided through some type of front end or web portal. While the end user is free to use the service from anywhere, the company pays a per use fee. Salesforce.com offers this type of service.

Cloud Computing Providers

Gartner predicts that cloud computing will surge to 150 billion dollars by 2013. Below is a partial list of companies that provide cloud computing services:

- Amazon
- Citrix
- cohensiveFT
- Flexscale
- Google
- IBM
- Icloud
- Joyent
- Microsoft
- Mozyhome
- Nivanix
- Rackspace
- Salesforce.com
- Sun
- VMware
- 3tera

Benefits of Cloud Computing

According to International Data Corporation (IDC), "The proliferation of devices, compliance, improved systems performance, online commerce and increased replication to secondary or backup sites is contributing to an annual doubling of the amount of information transmitted over the Internet." The cost of dealing with this amount of data is something that companies must address. In today's economy, companies are looking at any cost-saving measures, and the bottom line is that cloud computing provides much greater flexibility than previous computing models.

The benefits of cloud computing are many. One is reduced cost, since you pay as you go. Other benefits are the portability of the application is that users can work from home, work, or at client locations. This increased mobility means employees can access information anywhere they are. There is also the ability of cloud computing to free-up IT workers who may have been occupied performing updates, installing patches, or providing application support.

Security Concerns of Cloud Computing

While cost and ease of use are two great benefits of cloud computing, there are

significant security concerns that need to be addressed when considering moving critical applications and sensitive data to public and shared cloud environments. To address these concerns, the cloud provider must develop sufficient controls to provide the same or a greater level of security than the organisation would have if the cloud were not used. Listed here are ten items to review when considering cloud computing.

1. **Where's the data?** Different countries have different requirements and controls placed on access. Because your data is in the cloud, you may not realise that the data must reside in a physical location. Your cloud provider should agree in writing to provide the level of security required for your customers.

2. **Who has access?** Access control is a key concern, because insider attacks are a huge risk. A potential hacker is someone who has been entrusted with approved access to the cloud. If anyone doubts this, consider that in early 2009 an insider was accused of planting a logic bomb on Fanny Mae servers that, if launched, would have caused massive damage. Anyone considering using the cloud needs to look at who is managing their data and what types of controls are applied to these individuals.

3. **What are your regulatory requirements?** Organisations operating in the US, Canada, or the European Union have many regulatory requirements that they must abide by (e.g., ISO 27002, Safe Harbor, ITIL, and COBIT). You must ensure that your cloud provider is able to meet these requirements and is willing to undergo certification, accreditation, and review.

4. **Do you have the right to audit?** This particular item is no small matter; the cloud provider should agree in writing to the terms of audit.

5. **What type of training does the provider offer their employees?** This is actually a rather important item, because people will always be the weakest link in security. Knowing how your provider trains their employees is an important item to review.

6. **What type of data classification system does the provider use?** Questions you should be concerned with here include: Is the data classified? How is your data separated from other users? Encryption should also be discussed. Is it being used while the data is at rest and in transit? You will also want to know\ what type of encryption is being used. As an example, there is a big difference between WEP and WPA2.

7. **What are the service level agreement (SLA) terms?** The SLA serves as a contracted level of guaranteed service between the cloud provider and the customer that specifies what level of services will be provided.

8. **What is the long-term viability of the provider?** How long has the cloud

provider been in business and what is their track record. If they go out of business, what happens to your data? Will your data be returned, and if so, in what format? As an example, in 2007, online storage service MediaMax went out of business following a system administration error that deleted active customer data. The failed company left behind unhappy users and focused concerns on the reliability of cloud computing.

9. **What happens if there is a security breach?** If a security incident occurs, what support will you receive from the cloud provider? While many providers promote their services as being unhackable, cloud-based services are an attractive target to hackers.

10. **What is the disaster recovery/business continuity plan (DR/BCP)?** While you may not know the physical location of your services, it is physically located somewhere. All physical locations face threats such as fire, storms, natural disasters, and loss of power. In case of any of these events, how will the cloud provider respond, and what guarantee of continued services are they promising? As an example, in February 2009, Nokia's Contacts On Ovi servers crashed. The last reliable backup that Nokia could recover was dated January 23rd, meaning anything synced and stored by users between January 23rd and February 9th was lost completely.

Even basic services such as e-mail require a thorough review before moving the service to the cloud. While some organisations are starting to move their e-mail to cloud services hosted by Gmail, Yahoo e-mail, and others, there are issues to consider. In February 2009, Gmail reported an outage that affected its EU users. In January 2010, it was reported that Gmail had been targeted by attackers seeking to gain access to Chinese human rights activists. It was further reported by MSNBC that foreign correspondents may have been targeted. Although these services have many controls built in, it is not impossible for them to be compromised.

Questions that companies need to ask before outsourcing even something as basic as e-mail include:

- Can you function with no e-mail?
- How easy would it be to migrate to another e-mail provider?
- What is your email retention policy, and do you have a legal requirement to keep your email for a specific amount of time?
- Would your clients be concerned that you store email with sensitive information on a third-party server?

Cloud Computing Attacks

As more companies move to cloud computing, look for hackers to follow. Some of the potential attack vectors/criminals may attempt include:

- **Denial of Service (DoS) attacks –** Some security professionals have argued that the cloud is more vulnerable to DoS attacks, because it is shared by many users, which makes DoS attacks much more damaging. Twitter suffered a devastating DoS attack during 2009.

- **Side Channel attacks –** An attacker could attempt to compromise the cloud by placing a malicious virtual machine in close proximity to a target cloud server and then launching a side channel attack.

- **Authentication attacks –** Authentication is a weak point in hosted and virtual services and is frequently targeted. There are many different ways to authenticate users; for example, based on what a person knows, has, or is. The mechanisms used to secure the authentication process and the methods used are a frequent target of attackers.

- **Man-in-the-middle cryptographic attacks –** This attack is carried out when an attacker places himself between two users. Anytime attackers can place themselves in the communication's path, there is the possibility that they can intercept and modify communications.

Conclusion

Cloud computing offers real benefits to companies seeking a competitive edge in today's economy. Many more providers are moving into this area, and the competition is driving prices even lower. Attractive pricing, the ability to free up staff for other duties, and the ability to pay for "as needed" services will continue to drive more businesses to consider cloud computing. The decision to move to cloud-based services should fit into the organisation's overall corporate objectives. Before any services are moved to the cloud, the organisation's senior management should ensure such actions are consistent with their strategic plans and meet acceptance criteria that address the ten items discussed in this article.

Just as there are advantages to cloud computing, there are also several key security issues to keep in mind. One such concern is that cloud computing blurs the natural perimeter between the protected inside the hostile outside. Security of any cloud-based services must be closely reviewed to understand what protections your information has. There is also the issue of availability. This availability could be jeopardised by a denial of service or by the service provider suffering a failure or going out of business.

Learn More

To learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge, check out the following Global Knowledge courses:

Foundstone Ultimate Hacking: Web

Understanding Networking Fundamentals

VMware vSphere: Fast Track [V4]
VMware vSphere: Install, Configure, Manage [V4]

Visit **www.globalknowledge.net**

About the Author

Michael Gregg has 20 years of information security experience. He is the CTO of Superior Solutions, Inc., a Houston-based IT security consulting and auditing firm. He has led security risk assessments and established security programs within top corporations and government agencies. Michael is an expert in security risk assessment, security risk management, security criteria, and building corporate security programs.

He holds two associate degrees, a bachelor degree, and a masters degree Some of the certifications he holds include CISA, CISSP, CISM, MCSE, CIT+, CGEIT, A+, N+, Security +, CNA, CCNA, CIW Security Analyst, CEH, CHFI, CEI, DCNP, ES Dragon IDS, ES Advanced Dragon, and SSCP. In addition to his experience performing security assessments, he has authored or coauthored more than 10 books including *Certified Ethical Hacker Exam Prep* (Que), *CISSP Exam Cram 2* (Que), *Build Your Own Network Security Lab* (Wiley), and *Hack the Stack* (Syngress). Michael has created more than 15 security-related courses and training classes for various companies and universities.