Mark Estberg, *Senior Director of Risk and Compliance Management, Online Services Security & Compliance, Microsoft*

Jim Reavis, *co-founder and executive director, Cloud Security Alliance*

Greg Kane, *director IT and product technology, Security Executive Council*

Jeff M. Spivey, *director, Security Risk Management Inc.*

From a risk management perspective, how is security in cloud computing different from security in outsourced services?

There are more similarities than differences from a risk management perspective. The fundamental problem remains the same, which is whether transferring risk outside of your organization is the right choice. What is different is that there are fewer accepted standards to establish a trusted transfer of risk.

Outsourcing has matured to a level where contractual terms and conditions are relatively routine and mechanisms exist to verify security claims of an outsource provider.

Cloud computing lacks these practices for efficient supplier and customer understanding.

Certifications based on industry best practices such as ISO 27001 and methods to verify whether specific security capabilities are in place and operating such as SAS 70 types I and II are a start.

The same types of capabilities to allow for a trusted transfer of risk for outsourced services need to be developed for the cloud computing environment.

While there are many similarities, the differences are profound. The economic optimization of computing as a utility puts pressure on some traditional data center practices that seek to mitigate risks.

The location of an enterprise's assets may be unknowable; commingling of your data with other enterprises may be common; and isolating and extracting your data may be more difficult.

In general, the physical segregation of computer systems and dedicated outsourced employees managing/manipulating those systems is missing, and all security controls must be logical, which may not be well understood by the customer.

In addition, the business relationship itself between the cloud customer and the cloud service provider may be extremely dynamic, brokered by a third party with transient terms of service. This puts additional pressure on the customer to accurately quantify the risks and understand evolving threat vectors.

I would posit that security in cloud computing is actually not significantly different than security in outsourced services. You are essentially expanding the scope of your organization to include a third party. If you have a robust and reliable process to assess and maintain the security of outsourcing at your organization, then you probably have a good start on securing your cloud computing initiatives.

Whether the decision is to use outsourcing or cloud computing, your organization cannot relax its risk mitigation posture. If you are not assured that your provider is maintaining the security and privacy of your information, then you can't afford to use them. Outsourcing is relatively more mature and as such its providers tend to readily acknowledge the specific security requirements of their customers.

Organizations must work to get these same assurances from their cloud computing providers. Security practitioners need to make senior management aware of the risks of moving to cloud computing, just as they did for outsourcing initiatives. Get ahead of the business on this. Having policies in place encourages your organization to include them as requirements when seeking a provider of cloud computing services.

Risk management uses a framework to evaluate risk of emerging technologies — identifying risks and then managing them in support of the enterprise goals. Understand that a cloud can be private or public. The risks that virtualization technology exercises in a cloud are a concern of bits/bytes, but when a cloud is public, there are both technical risks and all the risks of outsourcing added to the mix.

Governance, risk compliance and controlling framework moving across virtual layers while provisioning resources — these are complicated and require technical frameworks, third-party validation and transparency of operations for public cloud providers.

Outsourcing requires precise service-level agreements covering important process and security-related responsibilities. The customer company should maintain any organizational core competencies in the course of outsourcing and thoroughly understand virtualization/emerging cloud risks so that the organization's interests are being managed and are not dependent on the cloud provider.

Next Month's Question: How do you define the cost of security?

For more information about the Security Executive Council, please visit www.securityexecutivecouncil.com/?sourceCode=std.