From Chaos to Security:

Keeping Information Security a Step Ahead of Game-Changing Technologies

By Chuck Adams, Cisco Internet Business Solutions Group (IBSG)

Gone are the days when security professionals had to worry only about protecting data centers and information assets within their own organizations. New technologies such as virtualization, cloud computing, and Software as a Service (SaaS) have blurred the borders of enterprise computing, permanently changing the ways businesses use and protect their information resources. These new, game-changing technologies hold the promise of greater agility, operational efficiency, and reduced capital expenses for enterprise information systems—and bigger headaches for those responsible for keeping those systems secure.

While a highly distributed computing environment presents new challenges, it also provides an opportunity to look at the enterprise security strategy in a new way, and to change the ways we protect our information assets—with or without these new technologies. This paper will take a brief look at the special challenges security professionals face as a result of the new, distributed computing paradigm, and will suggest a unified risk-management strategy to stay ahead of the game.

Virtualization: Portable Security Policies Required

Virtualization is the ability to store data and run applications where they are most beneficial. The good news, from a security standpoint, is that virtualization requires standardization throughout an organization in order to spread computing and storage functions among many different physical computers. By running all its computer operations on standardized platforms, an organization can have more consistent security measures, applied in more uniform ways. This keeps vital information resources under the direct control of the security organization.

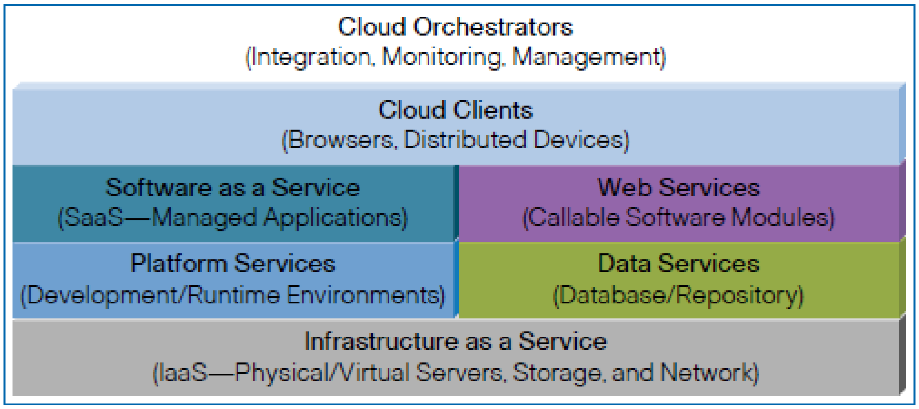
Virtualization creates its own security challenges, however, because it requires increased focus on information flows within the architecture. In a virtualized environment, security professionals need to define policies to protect those information flows and the data contained within them.

Traditionally, data centers have been built around physical machines, with policies applied at the physical server. Since virtual machines are just that—virtual—security policies must be created in a manner that enables them to remain with virtual servers and to be applied at the information level. Likewise, because applications and virtual servers share physical boxes, performance-management policies also need to be administered with control at the application and virtual server level. Another challenge is the increased importance of isolating security threats, since they could spread from one application or virtual server to another on the same machine.

Cloud Computing: Blurring the Enterprise's Borders

Few technologies have more potential to permanently change the way businesses use information technology than cloud computing. In a paper that first introduced the term, Professor Ramnath Chellappa, now of Emory University, defined cloud computing as "a computing paradigm where the boundaries of computing will be determined by economic rationale rather than technical limits."[1] The Cisco Internet Business Solutions Group (IBSG) views cloud computing as a subset of a broader paradigm we call "cloud services." Cloud services include Infrastructure as a Service (IaaS), SaaS, and platform, web, and data services—all offered via cloud clients and managed by an orchestration layer (see Figure 1).

Figure 1. Cloud Services Stack


Cloud Orchestrators
(Integration, Monitoring, Management)
Cloud Clients
(Browsers, Distributed Devices)
Software as a Service
(SaaS—Managed Applications)
Web Services
(Callable Software Modules)
Platform Services
(Development/Runtime Environments)
Data Services
(Database/Repository)
Infrastructure as a Service
(IaaS—Physical/Virtual Servers, Storage, and Network)

Source: Cisco IBSG, 2008

The benefits are many. With cloud computing, enterprises can (1) respond quickly to unusual spikes in demand without making additional capital investments; (2) subscribe to special application services delivered over the network, without having to manage and maintain those applications; and (3) use the "cloud" as a development platform for additional applications that run on the cloud infrastructure. They can access virtually unlimited computing power, on demand, and pay only for what they need.

With the benefits, however, come risks. Now, instead of having all enterprise information under their direct control and protection, security professionals must find ways to protect sensitive data that may be distributed throughout an infrastructure owned and managed by multiple vendors and service providers.

Develop a Unified Risk-Management Strategy

Each of these new IT infrastructure models offers pros and cons from a security perspective, but what is important is that as the fabrics converge and become standardized, we have an ideal opportunity to fundamentally strengthen our overall approach to security, and to embed more resiliency into the core of our operations.

[1] "Intermediaries in Cloud Computing: A New Computing Paradigm," Ramnath Chellappa, 1997, quoted by Wikipedia, 2009.

Regardless of where computing takes place—in the enterprise or in the cloud—the essential task of security professionals remains the same: keeping information assets secure, wherever they exist. Enterprise leaders need to step back and take a broad look at their overall security strategy, not just react to specific challenges raised by new technologies. They should develop an all-encompassing, unified risk-management vision that is aligned with all functional areas to accomplish core organizational objectives and to preserve the confidentiality, integrity, and availability of critical resources.

Consolidate, Integrate, and Align

In many organizations, security is built around a patchwork of "protect and defend" products and tools. Critical functions such as continuity, disaster recovery, compliance, and other physical and cyber security programs remain largely independent of each other and, in worst-case scenarios, isolated from the rest of the organization.

If this fragmented approach to security does not work in an enterprise computing environment, it certainly will not provide a secure cloud computing environment. To create a unified risk-management environment, begin by consolidating and integrating all security functions, both physical and digital. These integrated security capabilities must then be aligned with the organization's overall business objectives and designed to preserve the assets critical to fulfilling those objectives.

Reallocate Budgets To Fund the Unified Strategy

Bringing together fragmented security operations creates room to eliminate waste, reduce overlap, and think creatively about the best ways to manage risks effectively across the organization. Every dollar spent must be scrutinized and maximized, with a focus on interoperability and analysis methods that turn data streams into accurate, actionable information. Look for places where budget currently spent on either physical or cyber security *services* can be reallocated to fund integrated, interoperable security *technologies* that deliver broader protection and value. For example, new capabilities in digital video surveillance and analytics offer the opportunity to replace traditional surveillance service budgets with more comprehensive solutions, assuring a more resilient risk posture without increasing overall security spending.

As organizations begin to move computing operations outside their own physical infrastructure, they should apply the same principles. By reallocating some of the services budget, they can fund a more comprehensive risk-management strategy that should influence whether the organization chooses virtualization, cloud computing, SaaS, or other methods to assure flexibility and reliability while controlling costs.

Securing Information in the Cloud

The biggest task will be to define service-level strategies and expectations that assure the confidentiality, integrity, and availability of critical information in the cloud environment. Companies that use cloud computing services such as SaaS enterprise management suites send highly sensitive information outside the borders of the enterprise—and outside the realm of their control. Because these companies rely on third parties to protect this information, they must be clear about their expectations. They can accomplish this through carefully implemented protection-level agreements and addendums within their cloud computing service contracts.

When defining service-level agreements, consider expanding traditional service availability objectives and metrics to include security events. Design service levels that reflect the security expectations for confidentiality and integrity, and ensure that the service provider complies with recognized global standards for encryption technologies and infrastructure-management processes.

Conclusion

Cloud computing offers fundamentally new options for implementing information systems. While the vision for cloud services is still in its infancy, many organizations find the potential for flexibility, scalability, and agility a compelling reason to consider shifting at least some of their computing functions to a cloud service provider.

A comprehensive risk-management strategy will evaluate whether the benefits of a cloud approach outweigh the associated risks, and will consider alternatives for achieving these benefits. It will also define security policies that must be part of any cloud services protection-level agreement.

A unified risk-management approach will ensure that the IT and security strategies are consistent with the organization's overall vision and goals— whether or not the organization chooses a cloud services strategy.

For more information, please contact:

Chuck Adams
Business Resiliency Solutions Manager
Cisco Internet Business Solutions Group
cjadams@cisco.com
+1-512-340-3430