Research Journal of Applied Sciences, Engineering and Technology 6(7): 1184-1191, 2013
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: August 24, 2012 Accepted: January 11, 2013 Published: July 05, 2013

Secure NXT-the Next Level of Cloud Security

[1]N. Venkata Subramanian, [1]V. Prakash and [2]K.S. Ramanujam
[1]Department of Computer Applications, SASTRA University, India
[2]Bharathidasan University, Perambalur

Abstract: The promise of the cloud is appealing: reduced costs, greater agility, flexibility, scalability and potentially greater security. At the same time, IT organizations recognize that the cloud introduces a number of issues related to security, data integrity, compliance, service level agreements and data architecture that must be addressed. Therefore, the adoption of cloud services is being tempered by a significant level of uncertainty. Numerous surveys indicate that the top concerns for moving to the cloud are security, performance and availability. In other words, enterprises are looking for assurances that they are not adding risk to the business by leveraging the cloud. For many, moving to the cloud is still a leap of faith. Different cloud deployment models-public, private, or hybrid have different security vulnerabilities and risks. Generally, risk increases from greater degrees of multitenancy among increasingly unknown participants. The objective of this article is to insist the fact that cloud security begins with and adds to, well-defined enterprise security; it also introduces a new cloud security model called Cloud Security NXT.

Keywords: Cloud computing, cloud security, private cloud, public cloud

INTRODUCTION

Although there is ample discussion of cloud security in literature and industry media, People in top level management must focus on securing their own enterprise's use of cloud based services and not whether the cloud, in general, is secure.

Decision makers in organizations should consider the following broad steps as part of a cloud security program:

- Establish a risk-based approach
- Design (or convert) applications to run in the cloud securely
- Implement ongoing auditing and management
- Assess infrastructure (and platform) security during service sourcing

These steps will help address changes to the security landscape in a new era of cloud-based services and solutions. Cloud environments have reduced or removed traditional security perimeters, which means that enterprises need to adopt an information-centric approach to security. There will always be a need to continually assess risk and be agile in appropriately adapting new cloud solutions. When moving to cloud-based solutions and services, enterprises must first address the definitive information-related risks associated with a shared-service model. There will be many questions and concerns that can affect enterprise risk for using cloud services. Addressing cloud security requires total business involvement from the enterprise (Ronald and Russell, 2010).

NEED OF A NEW APPROACH

Security concerns are not unique to cloud; cloud is just one of many disruptive technology trends. In today's enterprise, there's an increased drive to adopt new technologies related to devices and data in particular, all of which alter the approach to enterprise security. Traditionally, the IT security environment of most organizations was seen as a hard shell with a soft center. Security was based on creating a strong perimeter to keep threats out of the organization. Once through this shell, security was typically light. In part, this reflected the model where data and applications were essentially static. The only way to access data was via an application, so a security fortress could be built around this static pairing. This has resulted in a common digital access tradeoff of richness versus reach-a few people can have access to rich, useful data, or a lot of people can reach limited and diluted data. Because traditional monolithic IT systems were complex and expensive to maintain and alter, few parts of an organization were supported by rich data and processes. The rest of the organization was and often still is, "information poor"-relying on home-brewed spreadsheets fed by limited data from the core IT systems. However, as business has become faster and more global, the need to share data has increased. The traditional models do not really address the needs of

Corresponding Author: N. Venkata Subramanian, Department of Computer Applications, SASTRA University, India

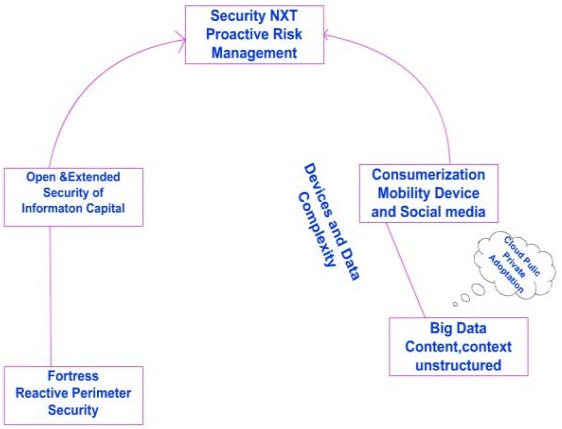

Fig. 1: Security NXT

mobile data and applications. Enterprises need richness and reach (Mell, 2012).

These trends also mean that the traditional corporate perimeter, with clearly identifiable boundaries, has diminished, making a perimeter approach nearly impossible to maintain. Compounding this situation is the rise of computer hacking and the rapid increase in security and privacy compliance legislation. This is creating a "perfect storm" of increased complexity. Complexity often results in significant blind spots within an organization, meaning that organizations have to force their security controls to be reactive to the latest threat or fire drill we believe security must move to the next level to meet these rising business opportunities and challenges. For security to be a more integral part of the business processes and data, effective security should be incorporated into processes throughout an enterprise, not just on the perimeter or in the cloud. A holistic and comprehensive approach is required. We work with our clients to help them take a proactive, risk-based approach. We call this Security NXT shown in Fig. 1.

CLOUD SECURITY-AN ENTERPRISE FOCUS

Attempting to define and achieve "cloud security" may be similar to trying to attain world peace. As we will briefly outline below, the cloud can mean many different things to many different people or organizations and can be analogous to the full spectrum of IT services. Security in this complex environment, like peace, can never be 100% achieved and guaranteed. And security, like peace, is a journey, not a destination. There are only degrees of more or less security, which ultimately must be judged in context of an enterprise (or individual). We should strive for cloud security by addressing the issues and vulnerabilities that we can control. For this reason, we stress that your focus should be on "securing your own enterprise's use and application of cloud based services" to set the appropriate context upon which sound business decisions can be made.

Table 1: The interpretations of cloud security

Security FOR the cloud	Security technologies, solutions, and services that allow you to secure your application and data in the cloud
Security FROM the cloud	Security technologies that are delivered to you in a "security-as-a-service" way
Security IN the cloud	Security technologies and methods that enable cloud platforms and applications to be intrinsically secure in their cloud environment
Security ACROSS clouds	Mechanisms for secure interoperability across cloud boundaries consisting of a cascading network of service providers

What do we mean by "cloud security?" There are many aspects to security and cloud. It is important to understand in what context you're evaluating the security of cloud services and what your own specific requirements are within that context. To begin, we outline four broad perspectives of cloud security (Table 1).

SECURITY POSTURE OF CLOUD DEPLOYMENT MODELS

Different cloud deployment models greatly influence the potential security vulnerabilities or "attack surface," as shown in Fig. 2. The increasing risks arise from an increased level of multitenancy among progressively more unknown participants

Private cloud: The cloud infrastructure is operated solely for one organization. It may be managed by the organization or a third party and may exist on premise or off premise (Goth, 2011). In the latter case, this is typically known as a managed/virtual private cloud. A private, on-premise cloud solution, deployed in an enterprise-owned/operated data center, has a similar security profile to other non-cloud systems that are operated in the same facility. Risks may increase by sharing resources among different business units or in the shared use of storage facilities for data (assets) with different security classifications (such as mixing an internal company blog storage area on storage used for data with requirements and regulations for PII).

Community cloud: The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns such as mission, security requirements, policy, or compliance considerations. It may be managed by the organizations or a third party and may exist on premise or off premise. A community cloud increases that level of shared resources by including a community of organizations with potential increases for security

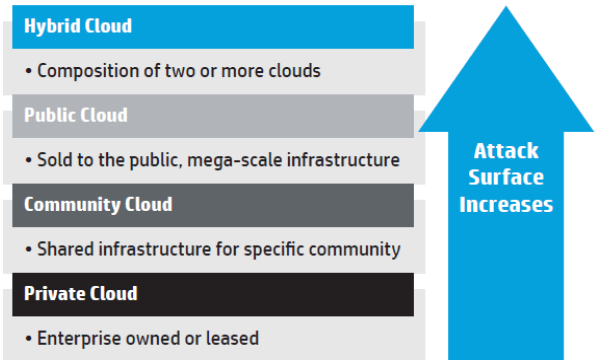

Fig. 2: Deployment models

incidents, data exposures, or breaches. The risk profile of the community cloud is bounded by the limits upon which the community is defined and we assume this size is less than that of a public cloud (Takabi *et al*., 2010)

Public cloud: The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services. A public cloud typically places no limits on the community of customers that may use and subscribe to the use of the shared resources that the public cloud service provider offers-other than an ability to pay for services consumed. A public cloud can be viewed as a community cloud with no limits on community membership or makeup (Takabi *et al*., 2010)

Hybrid cloud: The cloud infrastructure is a composition of two or more clouds (private, community, or public), each of which remains unique entities but are bound together by standardized or proprietary technology that enables data and application portability (often called "cloud bursting"). A hybrid cloud is, by definition, the combined use of two or more clouds to provide services for a common business function or application that can make dynamic use of the collection of facilities. The term hybrid cloud often refers to the use of a private cloud with an overflow or capability to scale out to a public cloud (Tim *et al*., 2009)

Security expectations of cloud service models: It is important to recognize that all clouds are not created equal in terms of service levels and security. Cloud services are often described by the type of service model that is offered. This is sometimes called the "SPI" model, referring to software –as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS).

The selection of a service model has a great effect on the distribution of roles and responsibilities of the cloud service provider and the cloud service consumer. In general, when using SaaS, the provider has more control and responsibility. By contrast, the consumer has more control and responsibility when using IaaS. So in many ways, organizations need to choose how much risk they want to retain and how much they are prepared to share with the cloud broker/provider (Tim *et al*., 2009).

WHAT IS REALLY NEW ABOUT CLOUD SECURITY?

Despite what is commonly reported in the industry press and other media, many cloud security incidents are actually previously known issues with web applications and data hosting, but at greater scale and frequency, due to early adoption of new cloud services. The underlying cause of many of the incidents was found to be phishing, downtime, data loss, weak passwords, or compromised hosts running botnets. This is not to say that these incidents are not "real" or important-they are. The point here is that there is nothing inherently cloud related that caused these incidents to occur (Tim *et al*., 2009).

It should be noted, however, that most clouds are shared, whether among programs, organizations, or communities. This means that "the needs of the one rarely outweigh the needs of the many."

Security policies and service-level agreements can be used to manage expectations, support management decisions regarding providers and govern performance-but cannot typically be imposed unilaterally on a shared service. Companies using cloud need to understand that they are consuming a shared resource and must, therefore, select the service that provides the levels of security and service that they need the following are some examples of new risks that arise from the use of cloud services, resulting from multitenancy and shared computing facilities and services.

Side channel and covert channels: Because cloud computing introduces a shared resource environment, unexpected side channels (passively observing information) and covert channels (actively sending data) can arise.

As a result, activity patterns may need to be protected in addition to the applications and data sources themselves. Previous research has exposed vulnerabilities that include ways to place an attacker virtual machine (VM) on the same physical machine as a targeted VM and then to construct a side channel between two VMs on the same physical machine. Much of this depends on the security mechanisms employed by the cloud service provider-in particular, network configuration and hypervisor security hardening. For enterprises that are highly concerned with masking activity patterns and/or side channel attacks, some cloud providers offer dedicated physical machines,

which may warrant additional consideration (Ronald and Russell, 2010).

Reputation fate sharing: Reputation fate sharing is an academic way of saying "you are known by the company you keep." This risk entails possible blacklisting or service disruption due to "bad neighbors" in which a single subverter can disrupt many users.

For example, a group of spammers subverted Amazon's EC2 and caused Spamhaus to blacklist a large fraction of EC2's IP addresses. This caused major service disruptions for legitimate EC2 customers, impeding their ability to send outbound mail. A second noteworthy fate-sharing incident occurred during an FBI raid on Texas data centers in April 2009, based on suspicions of the targeted data centers facilitating cybercrimes. The agents seized equipment and many businesses that were collocated in the same data centers faced business disruptions or even complete business closures.

Longer trust chains: The issue of trust is a significant concern in cloud security. Cloud services may introduce longer supply chains and, in turn, longer trust chains. This results from the ability to create composite services using two or more discrete cloud services in a cascading chain of services. It is important for enterprises to review and understand the supply chain and trust chains of cloud services that they are seeking to use. Enterprises should assess the cloud provider's supply chain for vulnerabilities and other business implications, in the same manner that it assesses other suppliers of goods and services. Key considerations include the following questions:

Are my security policies enforced throughout the network of service providers?

- Who is responsible and accountable?
- How is compliance measured, documented and reported?
- What is the reporting process regarding low-level breaches that may affect my enterprise's use of your services?

Trust chains are not only longer; they are also increasingly complex and rising in number. In this setting, the security aspects of the service contract are crucial mechanisms by which the trust relationship between customer and supplier is established and maintained.

Elimination or reduction of security perimeters The "safe harbor" of on-premise mainframes, servers, storage and data networks does not exist in most cloud deployment models (with the possible exception of an isolated on-premise private cloud).

Gone are the database and operating system models, replaced by platform as a service and the mobile application infrastructure (Kui *et al*., 2012).The security perimeters that were established to protect critical information assets in the traditional data center do not exist in the environment of cloud services. Because of this, enterprises should pay close attention to moving existing applications and data to a third-party cloud service. The architecture used for existing applications and database designs was most likely predicated on the assumption of a "safe and secure operating environment." The development team probably did not consider additional measures that would be necessary to protect the application, transactions and data in a hostile environment (Qian and Cong, 2011). The typical assumption only a few years ago was something like "… security is Operations' responsibility."

WHAT SHOULD A DECISION MAKER DO NOW?

As with most security challenges today, technical solutions are only part of the puzzle. What is needed is a well-rounded approach to the problem. We recommend the following broad steps as part of a cloud security program:

- Establish a risk-based approach
- Design (or convert) applications to securely run in the cloud
- Implement ongoing auditing and management
- Assess infrastructure (and platform) security during service sourcing

First, a risk-based approach is necessary to fully understand the risk impact of moving chosen applications and data (assets) to a particular cloud deployment model and service model. This assessment must be undertaken from a viewpoint of how it affects the entire enterprise. Second, many existing applications were not designed to run in a potentially hostile environment-thus the need to build in security at the application and data level for new systems. Existing applications should be thoroughly reviewed, inspected, amended and tested before deploying on a cloud platform; this exercise should be guided by the output of the risk-based assessment. Third, a thorough program for continual and ongoing audit and compliance management is needed in a dynamic, cloud-based services environment. A traditional regime of annual or monthly audits becomes meaningless in an environment that changes completely on a daily or hourly basis (Goth, 2011).

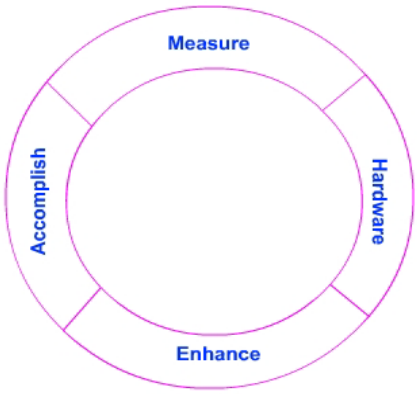

Fig. 3: MHEA life cycle

Establish a risk-based approach: Establishing a risk-based approach is a critical undertaking of managers in an era of cloud services. In fact they are responsible for selecting the services that are necessary to meet the needs of the business. This means they will need to analyze the business needs, using a risk-based approach to identify the service model and security levels necessary to support them. Essentially, this is because cloud is a consumption model for IT services and key to this model is an understanding of the service levels that must be met (Goth, 2011)

The primary objective of the risk-based approach is to help an enterprise move from a reactive to a proactive stance for enterprise security, with the end goal of measurably reducing business risk.

We have developed a risk-based methodology-Measure, Handover, Enhance, Accomplish or "MHEA"-that helps enable enterprises to achieve these goals. However, we find that enterprises benefit most by completing all four stages to achieve a more rigorous and effective risk-management strategy. The MHEA lifecycle methodology improves an enterprise's security posture while reducing risk and investment and finds the correct balance between securing and enabling the enterprise as shown in Fig. 3.

First, we should assess our client's risk tolerance profile, compliance requirements, operational requirements, organizational capabilities and resources. We then look to transform our client's environments. We structure and prioritize the client's security issues and undertake remediation projects.

Next, we optimize the environment and also broaden our client's level of security awareness. We can help the client continually monitor its environment and proactively recommend operational and process improvements that can deliver an optimized security and risk posture. Finally, we manage the associated security transformation programs required to deliver security in the most effective way for the enterprise, adopting proven security technologies and flexible sourcing models. We recommend the use of our comprehensive, end-to-end Enterprise Security Framework, as shown in Fig. 4.

This framework is guided by a Security Governance layer, shown at the top. This layer addresses comprehensive governance services that integrate and maintain your security policies and processes in alignment with your business drivers, legal and regulatory requirements and threat profile.

The Security Operations layer is responsible for managing and delivering security functions and processes, guiding by the policies and requirements noted in the security governance layer above.

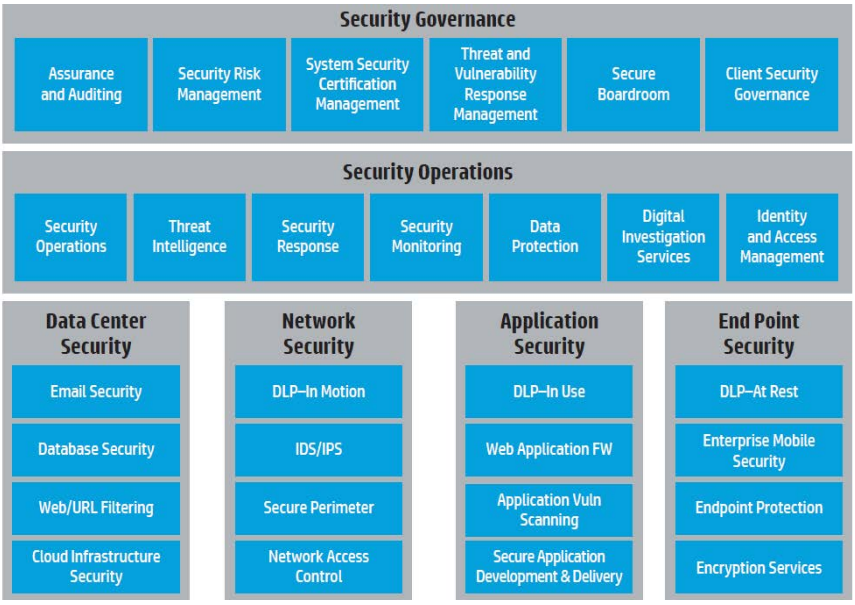

Fig. 4: Enterprise security framework

The technology layers provide technologies, tools and processes to provide secure operation and monitoring of critical areas for service delivery, including data center, network, application and end point.

Design applications to run in the cloud securely: It should be noted that the cloud is a new environment and, as such, it is not yet clear what the best ways are for companies to gain the most business advantage from its use. The evolution of corporate use of the Internet, for example, has evolved from the tentative first steps of publishing corporate advertising to a website to real-time commerce and collaboration with customers. The cloud will go through a similar evolution, so it is vitally important to implement good application design and deployment practices now to allow safe use of this new and growing opportunity.

Over the past decade, enterprises and traditional IT service providers have become increasingly adept at hardening network and infrastructure through advances in perimeter security, intrusion prevention, vulnerability and threat management. From an adversarial point of view, when the network and infrastructure are increasingly secured, attackers will move to the next weakest link-applications and data. Additionally, in a public cloud setting, the traditional "fortress" of the enterprise data center goes away-potentially leaving assets like applications, data and intellectual property vulnerable to theft, manipulation, exposure and/or destruction. We must also consider the significant changes that have occurred in the threat landscape over the past several years. A full treatment of these shifts is outside the scope of this study, but several trends are worth examining. A significant shift has occurred in the typical threat actors, as well as their targets and motivations. A decade ago, the typical threat agent was the stereotyped "lone hacker" who was motivated to break into enterprise and/or government networks and deface or disrupt websites and services with the primary goal and reward of fame and notoriety. A generalized profile could be assumed to be that of a mischievous adolescent (Tim *et al*., 2009).

Adopt an information-centric approach to security: New cloud applications should be developed with security built in. Developing applications with security already designed in dramatically reduces the risk of vulnerabilities and produces solutions that have greater security assurance at lower cost. By addressing new attack surfaces early in the design cycle with a security requirements analysis, security maintenance and remediation needs are reduced during the testing and operational phases. New cloud-based applications and data structures should be designed and built with the following considerations in mind:

- New attack surfaces addressed early in design
- Policy and compliance management
- Anomaly detection, pattern recognition for self-auditing and self-protecting systems
- Identity management and access control Adoption of a new mindset to privacy-encrypt everything by default, end-to-end
- Content-aware encryption to aid data loss prevention by selective data encryption based on policy
- Encryption alternatives-tokenization, data anonymization, fine-grained access controls

Since 80% of security breaches happen at the application layer, enterprises should employ third-party testing services for vulnerability analyses and penetration testing.

Implement ongoing auditing and management: Continuous compliance monitoring is essential to securely delivering cloud services and, of course, ensuring compliance. Cloud services are inherently dynamic. The dynamic provisioning and deprovisioning of resources is a key part of the cloud value proposition and business model. This makes automation of operational monitoring, continuous audit and compliance reporting essential in this dynamic environment. To comply with policy and legislation-such as the EU Data Protection Directive, GLBA, HIPAA and export compliance controls like ITAR-enterprises require continuously running audit and compliance monitoring.

Enterprises often lack an overall view of their security operations, risk, compliance and budget, creating difficulties in making informed risk and security decisions. This typically results from many years of implementing specific point solutions and tools that were needed on a reactive basis. As a result, many organizations do not have the means to produce a comprehensive integrated view of the security posture, risk level and compliance status.

Continuous monitoring and maintenance of security incident records and log files are crucial to enabling forensic examination and analysis in the event that a security breach or disclosure occurs.

This information must be available in real time to facilitate rapid response, notification and containment measures.

Communicating the value of security and addressing risk is one of the single biggest challenges for enterprise leaders because of the difficulties in reporting on actual metrics and Return on Investment (ROI).

CONSIDERATIONS FOR SERVICE SOURCING AND INFRASTRUCTURE SECURITY

Cloud-based services typically are designed to implement a single unifying architecture, which enables the rapid scaling and reusability features that characterize cloud-based services. While this architecture enables the benefits that make cloud

services attractive, it also generally precludes the ability to customize these services to an individual client's requirements. When using a cloud-based service, the service consumer has much less direct control over infrastructure and network security, including operational policies and procedures, network configuration, intrusion prevention and traffic control. This is not to say that these issues are not important and critical factors for the security of a cloud-based solution. In fact, they are all highly critical areas in cloud-based services; however, because enterprises have little or no influence on a provider's implementation of mechanisms and controls in these areas, a thorough review of the service provider's policies should be completed as part of the due diligence process during contract negotiation and service sourcing (Tim *et al*., 2009).Should you find that a particular cloud service does not meet, or cannot meet, your requirements for certain infrastructure related security measures, you will then need to seek an alternate provider that can meet your particular requirements, or move your application back in-house.

MANAGING CLOUD COMMUNITIES WITH TRUSTED CLOUD-CLIENT MANAGEMENT SOLUTIONS

The challenges to enterprises in moving to cloud computing include the inability to enforce security requirements relevant for data classification (s). By containerizing our data, we gain not only the ability to separate corporate from personal data, but can selectively introduce functionality such as remote wiping, advanced threat monitoring, or intrusion prevention. Research promises to take containerization-based security management models to mobile devices more generally, with the appropriate cloud integration for manageability.

We have been researching systems security architectures for the next-generation cloud-based enterprise and identified some innovative technologies which are the needs of the day such as:

- **Trusted computing:** System architecture for remotely verifying a device's properties to establish trust
- **Trusted virtualization:** A device architecture that can provide container-based security policies for multiple operating systems on a single device while supporting multiple independent IT domains to be managed securely on a single client device. We are also researching how to use such "state-of-the-art" developments to facilitate cost-effective cloud-based security management enterprise in a consumerized world.

From an IT department perspective, cloud communities could be defined and securely managed throughout, from the end-user cloud client devices to the data center. Importantly, our suggested approach is to allow end-user devices to be registered with multiple communities, rather than being limited to just one personal and one business persona. By supporting multiple personas, next-generation devices and services will allow multiple IT departments to have advanced security management control over their communities of mobile users and business applications, while end users will be able to maintain privacy and choice for their own device, within other cloud communities, or within personal applications (Tim *et al*., 2009).

Trust economics-business-aligned decision support: Decision-making and risk assessment for cloud and data loss is very difficult because:

- There is a challenging trade-off between enablement and risk mitigation
- Stakeholders have different views/incentives/ knowledge/responsibilities
- It is not just about technology-there are human factors, too

CONCLUSION

As enterprises adopt cloud-based solutions and services, they must first address the definitive information-related risks associated with a shared-service model. There are many questions and concerns that affect enterprise risk for using cloud services. Just a few of these questions are:

- Who can use our services?
- How is our data protected?
- What is the availability of our services?
- How would we be harmed if our data were lost, altered, or exposed to unauthorized parties?
- Who is liable for breaches?
- How can we measure compliance?
- Are we locked in now?

Addressing cloud security requires total business involvement from the enterprise. The security landscape has changed considerably in a new era of cloud-based services and solutions. There will always be a need to continually assess risk and be agile in appropriately adapting new cloud solutions. Enterprises that are adopting these services should keep the following points and recommendations in mind:

- Adjust for a changed and more industrialized threat landscape. Employ comprehensive and integrated approach to enterprise security and risk management
- Conduct security threat analyses for all critical applications

- Design in security from the beginning, especially when implementing public cloud usage
- Be vigilant with continual compliance monitoring and audits, intrusion testing and verifiable backups
- In summary we recommend that organizations should
- Establish a risk-based approach for assessing viability of cloud services
- Design applications to run in the cloud
- Implement ongoing auditing and management
- Thoroughly assess infrastructure security mechanisms of cloud service providers during service sourcing
- Innovate, as the cloud is fast-moving

REFERENCES

Goth, G., 2011. Public sector clouds beginning to blossom: Efficiency, new culture trumping security fears. IEEE Internet Comput., 15(6): 7-9.

Kui, R., W. Cong and W. Qian, 2012. Security challenges for the public cloud. IEEE Internet Comput., 16(1): 69-73.

Mell, P., 2012. What's special about cloud security? IT Prof., 14(4) 6-8.

Qian, W. and W. Cong, 2011. Enabling public audit-ability and data dynamics for storage security in cloud computing. IEEE T. Parall. Distr., 22(5): 847-859.

Ronald, L.K. and D.V. Russell, 2010. Cloud Security: A Comprehensive Guide to Secure Cloud Computing. Wiley Publicatoin, Indianapolis, Indiana.

Takabi, H., J.B.D. Joshi and G. Ahn, 2010. Security and privacy challenges in cloud computing environments. IEEE Secur. Priv., 8(6): 24-31.

Tim, M., K. Subra and L. Shahed, 2009. Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance (Theory in Practice). O'Reilly Media Inc., Sebastopol.