

booz&co.

Cloud Computing
*An Information
Security Perspective*



Contact Information

Beirut

Ramez Shehadi

Partner

+961-1-985-655

ramez.shehadi@booz.com

Düsseldorf

Jens Niebuhr

Partner

+49-211-3890-195

jens.niebuhr@booz.com

Canberra

David Batrouney

Principal

+61-2-6279-1235

david.batrouney@booz.com

Florham Park, NJ

Michael Mariolis

Principal

+1-973-410-7690

michael.mariolis@booz.com

Chicago

Mike Connolly

Partner

+1-312-578-4580

mike.connolly@booz.com

Frankfurt

Rainer Bernnat

Partner

+49-69-97167-414

rainer.bernat@booz.com

Delhi

Suvojoy Sengupta

Partner

+91-124-499-8700

suvojoy.sengupta@booz.com

Rome

Matthew W. Holt

Senior Associate

+39-06-6920731

matthew.holt@booz.com

EXECUTIVE SUMMARY

The popularity of cloud computing is growing fast, thanks to its ability to increase flexibility, improve access to data, and cut costs. Yet concerns about the security of the data that is moved to cloud environments remain—for good reason, given the inherent loss of control of critical data the technology demands. Only by developing a comprehensive and systematic approach to assessing the risks of moving data into the cloud—one that takes into account the concerns of both business users and IT security managers—can these risks be managed with confidence.

Our approach begins with a thorough assessment of the applications and data being considered for the cloud. How sensitive is the data, and how serious are the consequences of a potential data breach? Depending on the level of risk, the data must be assigned specific security requirements, and then matched with the cloud architecture being considered—private, public, or hybrid—and its associated security capabilities. Once this process is complete, security managers must work with business users to map out concrete, fact-based solutions regarding which specific cloud environments are appropriate for each data set and application, depending on its level of risk.

Ultimately, cloud security must be placed within the context of each company's overall information security program, including risk management, incident management, continuity planning, and governance. Doing so will require the combined efforts of everyone with a stake in ensuring the security of the data being moved into the cloud.

KEY HIGHLIGHTS

- The cloud services market is expected to grow almost four times as fast as other IT markets through 2013.
- Without an adequate means of assessing security risk in the cloud, many companies either refuse to move any data there or simply ignore the problem, leaving themselves open to real risks.
- Making sure business users and IT security managers work together is critical to maintaining security in the cloud while keeping incremental security costs down.
- Matching the risk level of particular information assets and associated security requirements with cloud security capabilities is an effective way to strike the right balance.
- Trustworthy cloud security will ultimately depend on strong governance within the overall information security program.

UNDERSTANDING RISK IN THE CLOUD

Relaxing on his couch at home in the evening, a sales manager for a large manufacturer of industrial products turns on his wife's iPad to check the latest client orders. His ability to get work done in the comfort of his own home allows him to keep up to date with the many accounts he manages, and increases his productivity substantially. But the information he receives wirelessly comes from the cloud, via application servers hosted by an external cloud service provider. Is he exposing his company to an unacceptable level of security risk?

Without question, cloud computing has the potential to be the most revolutionary trend in the information and communications technology

(ICT) industry in the next several years. Forecasts generally see revenues growing almost four times as fast for the cloud services market as for other IT markets through 2013. That's because the cloud has enormous potential not just to save IT costs, thanks to standardization and scale benefits, but also to provide the business with better service, anytime access, and faster time to market. Yet virtually every discussion of cloud computing inevitably raises the same question: Will my data be safe?

This is the question that has vexed CIOs and chief information security officers ever since the advent of cloud computing. The data called up by the sales manager no longer sits within his company's trusted networks behind a protected security perimeter, and the sales manager no longer accesses this data from a defined end-user device that follows tightly controlled access restrictions. This raises several critical issues about the security risks involved in putting this information in the cloud and giving him access to it from anywhere.

Companies that move data into the cloud often have little visibility into the cloud service providers' processes and procedures—including technical updates and hiring practices—and thus only a vague notion of the security risks the provider itself faces. The interfaces between the company and the provider may themselves be insecure, which could result in compromise, loss, or leakage of data both in storage at the provider and in transit back and forth. Since the nature of cloud services usually eliminates the contractual connection between the physical infrastructure that providers use to store data and produce services—the location of which is likely to be unknown to customers—and the actual data storage and process-

ing services that customers purchase, it becomes difficult or impossible to audit the data and to guarantee compliance with legal, regulatory, and corporate requirements. Finally, employees may themselves become less “security-conscious” and simply assume that the cloud provider will worry about such matters.

Reactions to the problem of security in the cloud range all the way from ignoring the issue completely to clinging so tightly to traditional IT security philosophies and methods as to ban cloud services entirely. Companies that have experienced governance and compliance problems, or outright data breaches, often exert additional scrutiny of the

process. And it's a justifiable concern: Significant security breaches can adversely affect a company's reputation for years, resulting in low customer confidence, lost current and future revenues, a poor public image, and legal liability.

On the flip side, in times of tight IT budgets, overpayment for security services must be avoided. What's the best way to resolve this conflict? We believe that it lies in taking a holistic, risk-based approach to security in the cloud that gives companies a consistent, structured way of deciding which kinds of data can be safely moved there.

Companies need a consistent, structured way of deciding which kinds of data can be safely moved into the cloud.

BRIDGING THE GAP

The key to both the problem and the solution to cloud security lies in the very nature of cloud computing—that critical data must be moved out beyond the corporate firewall and given over to a cloud services provider that offers storage and provides access. As such, cloud computing raises security questions that cannot be resolved with traditional IT security practices. These questions include the following:

- Which services and related data can be moved safely into the cloud, and when?
- How will sensitive data be protected in storage, in transit, and in use?
- How can access to cloud-based data and services through new hard-to-

control devices such as smartphones and iPads be managed in line with security requirements?

- What security levers built into cloud architecture components can be pulled to mitigate new risks?
- How can companies be sure that cloud service providers are compliant with their security requirements?
- Are industry-recognized security standards applicable?
- Will the incremental cost of cloud security potentially offset the commercial benefits?

Few IT security practitioners trained in the past know how to pragmatically answer these questions in a defensible, fact-based manner. As a result, the long-standing gap between IT security and the business only widens. Security managers continue to struggle to make the appropriate connection between high-level business requirements and specific security controls and requirements

in a way that business managers understand. And the classic “we need to comply with existing industry standards” defense doesn’t help, since those standards have not yet been adapted to cloud-specific challenges such as multi-tenancy in virtualized environments, problematic location control due to cloud provider load-sharing configurations, and reduced access-point control. Moreover, the issue of security in the cloud remains at a high level of conceptual abstraction, as many discussions on the topic remain primarily “model-based” rather than focusing on specific architecture components and solutions.

This ongoing disconnect only serves to sharpen the conflict between IT security requirements and business demands. Security managers erect increasingly high barriers to a smooth-running cloud environment, further encouraging business managers to view the security staff as opponents of cloud deployment and thus as impediments to business development. To bridge this gap, a new approach to security in the cloud must be found.

Cloud computing raises security questions that cannot be resolved with traditional IT security practices.

RISK LEVELS IN THE CLOUD

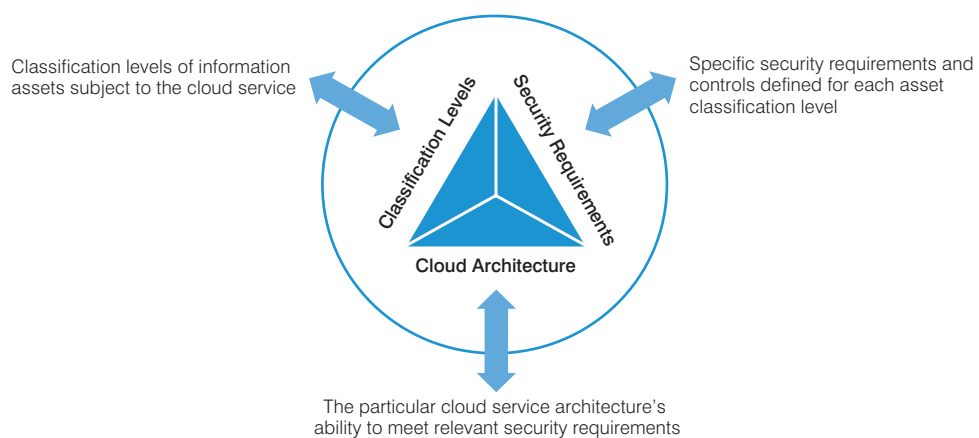
Companies considering cloud computing must first take into account which applications and accompanying data and services they might move into the cloud, how much risk they are willing to take in doing so, and which specific components of an application will be moved into

the public, private, or hybrid cloud architectures available.

The first step involves classifying all of the information assets of an application being considered for the cloud into different risk levels—such as basic, sensitive, and critical—depending on the nature of the data and the potential consequences of any security breach, such as lost revenue, legal liability, or damage to reputation. In the second step, each classification level is assigned the specific security requirements and

controls needed to reduce risk to an acceptable level. In the third, each classification level and its security requirements are matched with the appropriate cloud architecture, depending on the ability of the components of that architecture to meet those requirements. At every step, all three elements—classification levels, security requirements, and cloud architecture—must be in harmony, as any deficiency in one component will reduce the effectiveness of the others (*see Exhibit 1*).

Exhibit 1
Matching Risk Levels to Cloud Architectures



Source: Booz & Company analysis

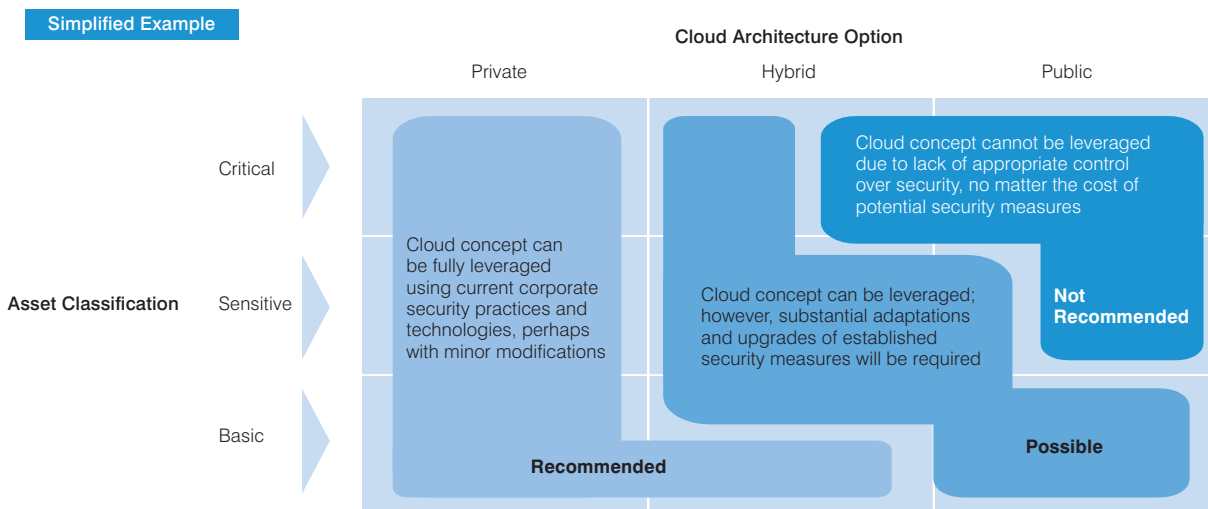
Unfortunately, there is no standard answer for how to balance these three elements that can be applied in all situations. Classification levels and security requirements vary from one company to the next, and the number of variables that make up any specific cloud architecture are too many to count. Security and business managers must work together to find the right balance on a case-by-case basis.

As an example, consider the sales manager checking new orders on his wife's iPad. His company had the option to deploy this particular application into any of the three types of cloud architecture—public, private, and hybrid. So the responsible business manager asked the security manager to define which of the three would be feasible, given the current security requirements for the various levels of data the application uses. The security manager drew up a map

showing which of the application's processes and associated data could be moved into which cloud architecture in this specific case (see *Exhibit 2*).

The light blue area on the map indicates the conditions under which the company's data can be freely moved to the cloud. In this case, the security manager was confident that the components of the specific private cloud architecture being

Exhibit 2
Options for Moving a Sales Order Application into the Cloud



Source: Booz & Company analysis

evaluated could meet the security requirements defined by his company for all data classification levels. He also felt sure that the company would have significant control over all of the security capabilities of this architecture's components. Therefore, he informed the business manager that he could move all levels of his data into this specific architecture.

The medium blue area represents a different environment. The business manager was tempted to move much of the application's data components into a hybrid cloud architecture, reducing costs and increasing flexibility. But the security manager was worried that this architecture, in which other customers of the cloud service provider might share certain components, would not meet the more stringent security requirements demanded by his company for its most sensitive and critical data. Only basic-level data would be eligible to be moved immediately to this specific hybrid environment. For the sensitive and critical data, the security manager identified a set of specific additional security measures and associated costs that would be required to comply with security requirements. In each case in this environment, the business manager had to decide either to make

the additional investment needed to meet the security requirements, not to make the investment and operate in the cloud at an elevated level of risk, or not to move the data into the cloud at all.

The outcome of this decision invariably presents the real possibility that if the cost of a security solution is too high, the business owner may intentionally lower the data's security classification level in order to reduce the needed security requirements and costs. To avoid this result, the company must put in place a formal process for determining the residual risk to a data asset even after security requirements have been agreed on and for authorizing the business owner to make the final decision on whether to accept this residual risk in the best interests of the company.

The dark blue area indicates the difficulty of moving the company's sensitive and critical data into a particular public cloud architecture, which is essentially open to all comers and thus offers the lowest level of control over the architecture's security capabilities. Here, the loss of control could effectively render deployment of sensitive or critical data into the cloud impossible, no matter what the

cost of increasing the surrounding security. So the security manager advised the business manager that the sales order application and its critical data could not be moved into this public cloud environment and still meet the necessary security requirements. Again, it is ultimately up to the business manager to make the final decision, based on the levels of residual risk the company is willing to accept.

The results of this mapping process hinge, of course, on the exact definition of the three critical dimensions: the asset classification, the security requirements, and the cloud architecture options. Any change to any of these dimensions would produce different results, even for the same company. For example, if the security manager in this case were to evaluate two different public cloud service providers, the capabilities inherent in the cloud architectures of the two would most likely differ, thereby producing slightly different medium and dark blue areas. And if this company's main competitor were to perform the same in-house evaluation involving similar applications, the results, based on that company's unique set of security requirements, would differ yet again.

CLOUD SECURITY GOVERNANCE

In addition to deciding whether to move assets into the cloud, companies must also make sure their cloud computing efforts are fully integrated into their entire information security program. That means understanding the process as it fits in our ICT Resilience Lifecycle, which takes into account not only the prevention aspects, including risk management and information security, and the reaction elements, involving incident management and continuity planning, but also the overall governance process (see Exhibit 3).

Governance: As companies decide to deploy assets in cloud environments, they must rethink their IT security governance procedures accordingly. That process should begin with the establishment of an overall vision of how the cloud fits not only into the necessary information security procedures, but also with the goals and objectives of those procedures and a road map for establishing them.

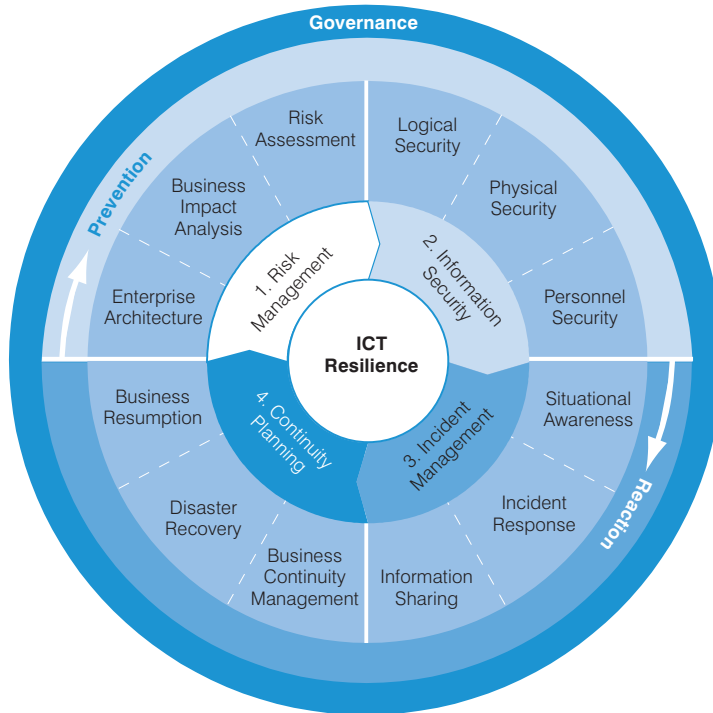
Risk management: As discussed above, security requirements must be aligned with overall corporate-level appetite for residual risk and ongoing classification of data assets.

Incident management: As assets are moved into the cloud, every cloud provider must be integrated into the company's overall centralized incident response procedures.

Continuity planning: Business continuity plans must take into account assets moved into the cloud, and be regularly updated and tested to account for new cloud architecture and provider models.

As part of this effort, security practitioners must define the scope and boundaries of all security functions that may be relevant to cloud environments, and develop an approach to improving and monitoring the performance of all of the cloud's stakeholders, including service providers, users, and technical staff. Finally, they should provide top management with the tools needed to gain visibility into cloud security—such as a security-level dashboard—and the levers needed to manage the overall cloud computing program.

Exhibit 3
The ICT Resilience Lifecycle



Source: Booz & Company analysis

About the Authors

Jens Niebuhr is a partner in Booz & Company's Düsseldorf office. He focuses on IT strategy and transformation for large enterprises and leads the firm's European IT activities in the communications and utilities sectors.

Matthew W. Holt is a senior associate in Booz & Company's Rome office. He leads the firm's ICT Resilience and Cyber Security Center of Excellence, focusing on governance, risk management, integrated security, incident management, and business continuity solutions.

Thomas Aichberger is a senior associate in Booz & Company's Vienna office. He focuses on IT security, next-generation networks, and IT strategy, processes, and operating models, with an industry emphasis on telecommunication network operators.

Angelo Rosiello is a senior consultant in Booz & Company's Milan office. He focuses on cybersecurity, IT strategy and governance, ITIL-based process design, risk management, and outsourcing.

CONCLUSION

Cloud computing represents a major opportunity for corporate IT to provide greater flexibility and value to the business while saving money at the same time. Yet security will always be a concern when important information assets are no longer under direct control. A proper cloud security program will provide business managers with concrete, fact-based solutions to support their business needs and allow them to enjoy the benefits of the cloud without putting the company at undue risk of data breaches or loss. Such a program will identify where the risks of moving information assets into the cloud are too high, which security practices management can put in place to reduce that risk to acceptable levels, and whether the costs of those practices are warranted by the benefits inherent in cloud computing.

The most recent list of our offices and affiliates, with addresses and telephone numbers, can be found on our website, booz.com.

Worldwide Offices

Asia	Bangkok	Helsinki	Middle East	Florham Park
Beijing	Brisbane	Istanbul	Abu Dhabi	Houston
Delhi	Canberra	London	Beirut	Los Angeles
Hong Kong	Jakarta	Madrid	Cairo	Mexico City
Mumbai	Kuala Lumpur	Milan	Doha	New York City
Seoul	Melbourne	Moscow	Dubai	Parsippany
Shanghai	Sydney	Munich	Riyadh	San Francisco
Taipei		Oslo		
Tokyo	Europe	Paris	North America	South America
	Amsterdam	Rome	Atlanta	Buenos Aires
Australia,	Berlin	Stockholm	Chicago	Rio de Janeiro
New Zealand &	Copenhagen	Stuttgart	Cleveland	Santiago
Southeast Asia	Dublin	Vienna	Dallas	São Paulo
Adelaide	Düsseldorf	Warsaw	DC	
Auckland	Frankfurt	Zurich	Detroit	

Booz & Company is a leading global management consulting firm, helping the world's top businesses, governments, and organizations. Our founder, Edwin Booz, defined the profession when he established the first management consulting firm in 1914.

Today, with more than 3,300 people in 61 offices around the world, we bring foresight and knowledge, deep functional expertise, and a practical approach to building capabilities and delivering real impact. We work closely with our clients to create and deliver essential advantage. The independent White Space report ranked Booz & Company #1 among consulting firms for "the best thought leadership" in 2010.

For our management magazine *strategy+business*, visit strategy-business.com.

Visit booz.com to learn more about Booz & Company.
