Understanding Cloud Security Issues

In the middle of the first decade of the new millennium, Amazon faced business and technology issues: Business was very seasonal, as was demand for computing resources. For example, the powerful computer systems needed to cope with the Christmas shopping frenzy lay idle for the rest of the year.

They say that was the scenario that gave birth to the new concept – after all, Amazon is the retail giant, so instead of just books and toys, somebody was clever enough to ask: why not market computing resources to our consumers? In 2006, this idea evolved into Amazon Web Services, which generate an estimated, annual income for Amazon of around one and a half billion dollars (Amazon does not publish the direct results of AWS).

This move turned Amazon into the leading market provider of infrastructure as a service (IaaS) and compute services to hundreds of thousands of customers.

This was the beginning of cloud computing in its current form as we know it today. Of course, cloud computing already existed before Amazon entered the scene, and would no doubt have also developed without it, but why ruin a good story even if it was never officially confirmed by the executive leadership at Amazon?

My objective in this article is to examine innovation in the field of cloud computing from various legal, administrative and regulatory angles, in addition, of course, to looking at the technological challenges, and all this without "killing a good story" – meaning, without detracting from cloud technology's ability to alter the way we use our computerized services.

The Initial Challenge – Contract Management

The first issue we shall touch upon is of a legal nature. Cloud computing is perhaps one of the few interfaces in an organization that requires the cooperation of the computing department with the legal department in order to pinpoint risks and obstacles. Sometimes, the only way an organization can manage the risks involved in the transition to cloud computing is to employ contractual controls and SLAs. This is particularly true in a SaaS environment.

As you read, please remember that beyond understanding the legal implications, the customer usually has little power to introduce any significant changes into the contract with the cloud provider. The cloud provider's competitive advantage lies in the uniformity of service provision to customers. Unfortunately, many contracts with cloud providers are vaguely and ambiguously phrased regarding their responsibilities and commitments towards customers. Despite considerable invested effort to change this situation (for HP and CSA, projects are under way to define areas of responsibility within a cloud), we are still far from our goal concerning procurement of cloud services as a consumer product anchored in clearly-defined contractual terms.

The legal issues customers encounter when switching to cloud computing can be variously grouped as follows:

Functional Issues

Who is responsible for what? Organizations must remember that the transition to cloud does not absolve them of responsibility for information. On a global level, most legal interpretations assign information ownership to the cloud customer even if the information is stored in the cloud. But beyond the general question of accountability, the division of responsibilities must be clearly defined in the context of transition to cloud. For example: Who owns the metadata generated by information processing? And who is in charge of certain processes, such as eDiscovery, that are triggered in response to court orders (for example, for information disclosure), for retention of information or, on the other hand, information purging?

Contractual Issues

During the contract period, it is important to ensure that the validity period of the contract is clear and understood, and that it includes clauses detailing the unanticipated termination terms. A well-known risk associated with cloud computing is rooted in the close links with the supplier. Known as *'vendor lock-in'*, this may result from either technical or contractual issues. The purpose of the contract is to reduce exposure by means of a clear definition of the data export resources available to the customer to ensure continuity of business. Beyond this, existing contractual issues relating to supply from third-party sources are also applicable here, with certain adjustments for cloud computing.

Matters of Jurisdiction

When migrating to cloud, geography becomes a very significant matter, and not only when discussing where a contractual dispute should be investigated. When corporate information is transmitted internationally, it is essential to verify, first of all, whether the information is allowed to *'leave the country'* (for example, the European Union prohibits the export of personal data to non-European countries with more lenient privacy legislation), and whether it is subject to local regulations and legal provisions in the new location. Different US laws (such as the FISA and the Patriot Act) are liable to force your (US) cloud provider to disclose your information to the American authorities without your knowledge.

Here are a few examples of legal issues that are unique to the United States and the European Union:

USA

In the United States, the right to privacy is determined by various Federal laws and State regulations, but it is based on the definition of the right to privacy in the Fourth Amendment to the Federal Constitution. Thus, for example, an American citizen can be protected from illegal search of his home computer thanks to the Fourth Amendment. However, according to its currently accepted interpretation, the Fourth Amendment does not apply to documents stored in the cloud, for example. It is important to understand this point as it is fundamental to any legal interpretation of privacy in general, and in cloud computing specifically, in the United States.

Another issue that is relevant in the US is the mandatory provision of documents in legal procedures. Both civil and criminal law in the United States rely heavily on the principle that each side in a legal process is obliged to submit to the other side all documents pertaining to the subject of the trial. Cloud customers must remember that the transfer of information to the cloud provider (even within a different geographic zone) does not absolve the customer from mandatory disclosure of information and, during the legal process, he will still be required to produce all the documents relevant to the subject. Cloud customers should be prepared in advance for such a possibility both from the technical standpoint (for example, this kind of retrieval process in the cloud mail server is much more complex than in locally hosted mail server) and in terms of the agreement with the supplier and of the tools he offers to enable such a procedure. It is important to understand that a situation could arise, especially in the world of software as a service, where despite the issuing of a subpoena to the supplier as part of a legal process against a particular customer, the same legal process could also lead either to service blocking or to mandatory deposition of documents of other customers, even if they are not involved in the court proceedings. This is the true meaning of multi-tenancy in a cloud environment.

The final important point to understand when examining cloud computing legal issues in the US is the fact that post-9/11 legislation allows the Federal Administration to freely monitor information, particularly when owned by a non-citizen of the United States, with virtually no need for legal order or special affidavit. Companies wishing to transfer information to cloud servers owned by American companies should consider the fact that the cloud provider is obliged to grant Federal Government access to their servers without notice to customers.

European Union

The European Union is a global leader in the regulation of privacy protection, investing heavily in the protection of information owned by its local and foreign residents (unlike the US). Rules in the EU are so strict that they prohibit all export of private information outside the borders of the EU (or to be precise, outside the European Economic Area – EEA), unless its security is assured by an equivalent level of protection.

As a means to enable European companies to transfer information to US companies without fear of breach of the privacy laws, the Europe-US Chamber of Commerce has formulated an agreement, known as Safe Harbor, which states that American companies will receive approval to store European information upon declaration of their compliance with 7 information security criteria (notice, choice, onward transfer, security, integrity, enforcement).

This agreement, already much criticized in the past, underwent a further shakeup a few months ago, when the EU Advisory Committee on Privacy and Computing (Article 29 Working Party) came out in opposition to the application of Safe Harbor principles to cloud computing (WP 196). The bottom line is that the Committee declared the Safe Harbor agreements unsuitable for cloud computing, and recommended a set of mandatory steps to be taken by cloud customers before forwarding information to American cloud service providers. Their recommendations include contractual provisions and comprehensive risk analysis. Although the Committee's recommendations are not currently binding, they clearly outline the direction the EU is taking towards increased privacy enforcement. This, of course, constitutes a real obstacle to American (and Israeli) cloud providers, and without a doubt will delay the adoption of cloud technology at the enterprise level in Europe.

The Responsibility Matrix

In the previous chapter, we discussed the legal issues that the implementation of cloud services is liable to trigger. We shall now examine the division of responsibilities between cloud providers and customers.

To better understand this issue, let us clarify the three main types of cloud service available:

Software as a Service (SaaS)

Software as a service is the most popular type of cloud service, and the easiest to understand. Software as a service provider is responsible for most aspects of information security and the customer can generally rely on information management controls being integrated into the contract, except for tools such as user management and performance test and scanning systems.

Platform as a Service (PaaS)

With this type of cloud, in addition to computing resources, the customer also receives a development environment in which he can create applications. The customer usually receives a development framework, database and web servers (for example, Amazon BeansTalk, database.com, Google Apps). In such an environment, the provid-

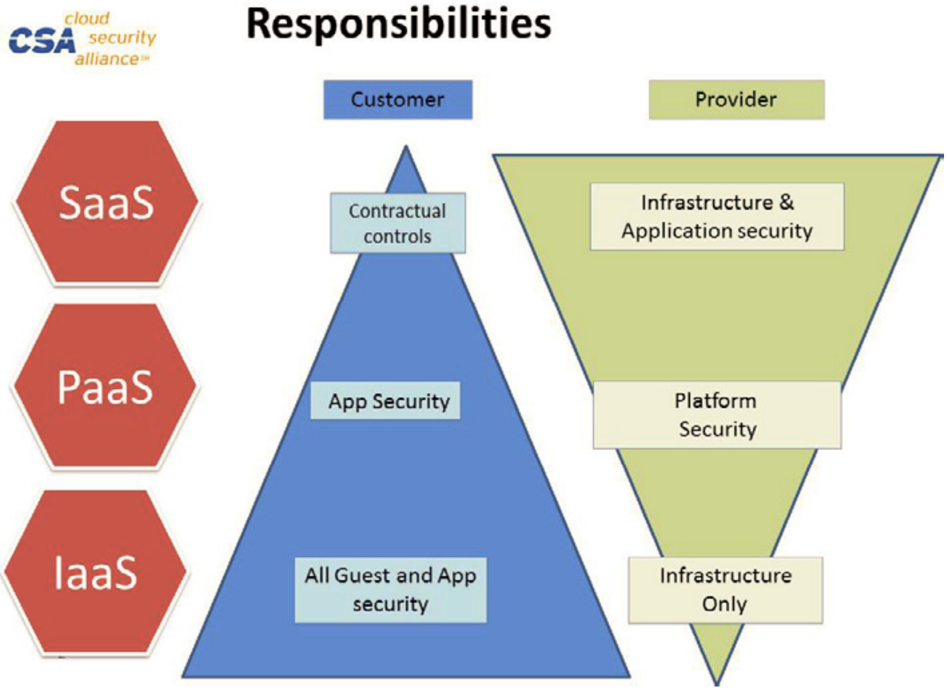


Figure 1. *Cloud – Responsibilities*

er owns the platform components, while the customer is responsible for the application itself.

Infrastructure as a Service (IaaS)

Infrastructure as a Service is a the most basic form of cloud service that provides customer with computing resources (such as the CPU, memory, archive and network) upon which infrastructure (covered by supplier warranty) the customer can install his virtual machines to consume the resources (for example, Amazon EC2, Rackspace, and Google Compute) (Figure 1).

In general, you can say that the higher the service level, the fewer the areas of customer responsibility and the greater the responsibility of the supplier. The above drawing highlights this graduated change in allocation of responsibility according to the type of service.

A few words on responsibility – It should be understood that responsibility can be transferred to a third party, as opposed to liability or accountability – and yes, an organization can transfer some of its security functions to an external organization, but it cannot transfer its general liability or accountability for protection of the information.

Understanding the critical areas of responsibility involved in migration to the cloud planning phase: We see SaaS cloud customers, who fail to realize the necessity to progress from technical operation of an information security system to risk management using contractual tools and evaluation rather than actual implementation. On the other hand, we see IaaS cloud customers, who are unaware of their need to deploy the usual tools (such as, OS hardening, encryption, antivirus, firewall, and so on) to protect their servers.

The following diagram describes some security tools, and the division of responsibilities between provider and customer: Figure 2.

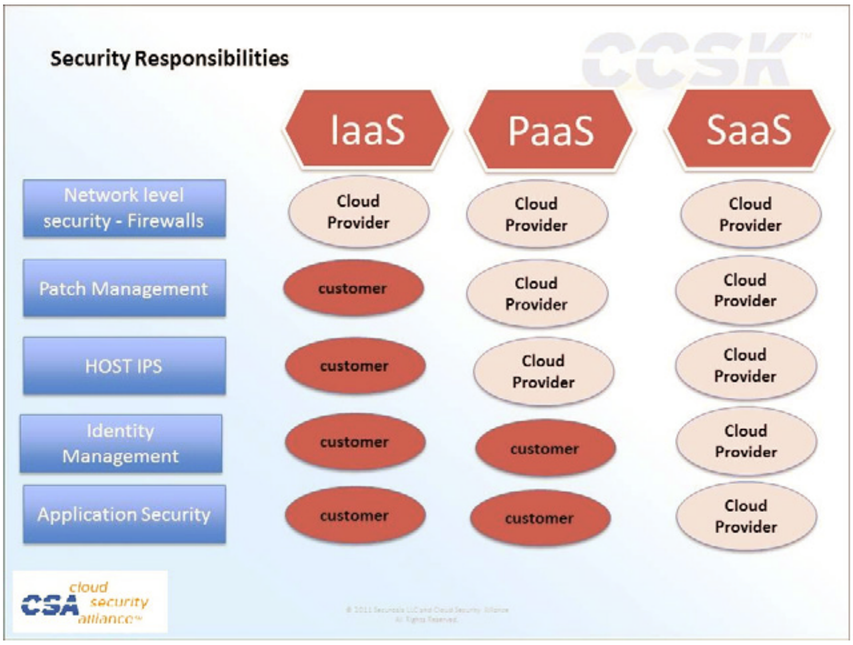
The following points merit special attention when planning the division of responsibilities between provider and customer:

Penetration Tests & Vulnerability Scan

The vast majority of Cloud Providers will request any such scan to be prescheduled. A good indicator of the maturity of a provider's information security posture is his preparedness for this process (at Amazon, for example, there is a well-defined process for these matters) and his ability also to provide previous audits on his own platform. It is worthwhile pointing out here that most major service providers will provide you with recognized and relevant certification (such as, ISO27001, PCI-PA\DSS, and so on); thereby significantly reducing the extent of audit you need to perform. For any type of cloud service (IaaS, SaaS, PaaS) there should be separate review and analysis processes. It should be noted that in the case of PaaS, for example, where the relevant application is developed by the customer, consideration should be given to the implementation of a secure development process (SDLC) as for any other enterprise application.

Identity & Access Management

Remember that in an IaaS environment, the entire responsibility for user management is the customer's, and therefore the customers need to consid-



Security Responsibilities

	IaaS	PaaS	SaaS
Network level security - Firewalls	Cloud Provider	Cloud Provider	Cloud Provider
Patch Management	customer	Cloud Provider	Cloud Provider
HOST IPS	customer	Cloud Provider	Cloud Provider
Identity Management	customer	customer	Cloud Provider
Application Security	customer	customer	Cloud Provider

Figure 2. *Tools and responsibilities*

er how to conduct management of those environments. The ruling concept is to make use of the tools existing within the organization and to extend their implementation to the cloud environment without the need to reinvent the wheel. In SaaS environments, it is necessary to determine which set of tools enables the supplier to validate identity (SAML is an excellent standard for the use of an existing corporate identity) and also to check which other tools are supported for management, monitoring and provisioning. Standards such as OAuth and SCIM are also evolving into accepted standards in the field.

Encryption and Other Controls

This section examines the challenges of encryption, which is critical for cloud computing. Cloud encryption solutions are growing in number and expanding in range with varied deployment and operation options. We cannot review them all here, but we will examine the main choices that are currently available. It should always be born in mind that planning to implement encryption raises some important questions:

- Where are the encryption keys stored and how are they accessed? There are many possible answers to the question of encryption key storage, the main determining factor being the type of threat against which protection is sought.
  For example, most cloud providers are currently able to offer encryption at block storage level. This type of encryption is symmetric and the key is saved by the storage provider. This is clearly a highly effective form of encryption for protection against possible loss of media, disks or backup tapes. However, it cannot provide us with protection in a cloud environment when we do not trust the service provider or we fear application hacking – it is transparent to the application server.
- At what stage in the data lifecycle should we consider encryption? Usually we talk about the following 3 statuses:
  - Data in Motion: When the information is being moved to the user or to other application areas
  - Data at Rest: When the information is located in a fixed storage facility (usually a database or storage server).
  - Data in Use: When the information is used by the application or user.

  For each of the above statuses, a different type of encryption is needed. For example, when data is in motion, it must be encrypted for the duration of its use by means of software, such as SSL or a VPN. In the current article, our main focus will be on Data at Rest within its application, because it is differently implemented in the cloud from in traditional environments.
- What type of cloud technology are we talking about? In an IaaS context, at best we can expect the service supplier to implement block-level encryption, and any other solutions are the responsibility of the customer. In a SaaS context, the customer usually depends on the vendor's support of the necessary solutions.

As a rule, we try to divide the types of encryption into categories, as follows:

- Storage-level Encryption: Encryption is performed at the level of the storage server. This encryption is transparent to the infrastructure and applications. However, the encryption key is usually kept by the service provider.
- Volume-level Encryption: This encryption is at the level of the virtual server. It is easy to implement in IaaS environments, as it is supported at the level of the operating system or of the various applications. This is not relevant, however, for SaaS environments. The main challenge of this encryption is to determine the encryption key storage location and access method.
- Database-level Encryption: Most databases come with encryption capabilities at different levels (field, table, and so on), sometimes built-in and sometimes using third-party software. This encryption is very effective in IaaS environments, but for SaaS or PaaS environments it depends on the service provider.
- Proxy-based Encryption: This method is based on the use of a third-party service or product with the capacity to support all the traffic between the customer and the cloud environment, to encrypt some or all of the data. This method enables, for example, encryption of customer names, credit card numbers and documents before they reach the cloud. In this encryption mode, the keys are generated and stored by the customer without exposure to the cloud provider. This area is the fastest growing encryption solution for Cloud Computing and implementation are available for IaaS environments, SaaS and PaaS.
- DRM Encryption Solutions: These types of solution involve encryption and digital rights management (DRM) at the file level. They are very helpful for organizations that keep MS Office and PDF format documents in cloud environ-

ments, and are particularly useful for applications such as Google docs, Dropbox and other ECM solutions. The DRM mechanisms enable configuration of file-level user access rights and hierarchical permissions. Although such solutions now support configuration at the levels of work groups or specific processes, it is difficult to fully implement them at organizational level.

In Summary

Encryption technology is a critical element in the migration to cloud computing, both because the implementation of such technology is a standard and regulatory requirement and because proper application of these technologies can significantly reduce the risks in the cloud. As for any technology, it is important to understand the nature of the risks we face, the regulatory provisions relating to them and the type of cloud service model we are working with, in order to select the appropriate encryption architecture.

MOSHE FARBER

Moshe Farber is one of Israel's leading information security experts. He possesses a wealth of experience in information security, and specialist expertise in identity management, information security event management and related innovative technologies. For over a decade, he served in various capacities in that field, and was involved in major projects in leading organizations worldwide. He has in-depth knowledge of both the technical and the business aspect of the latest, cutting-edge technologies.

Among his achievements, Moshe was in charge of product group security management at Ness Technologies, where he worked in sales and assimilation of information security technologies, such as IDM, SIM, DLP and the ERP security system. Previously, he developed a number of college courses in data security, risk management and regulation.

In the past two years, Moshe has focused on various aspects of cloud technology. He established the Cloud7 information security service provider that offers unique information security technologies in the form of a service in Israel and abroad. He is also a partner in the FortyCloud and Clarisite start-ups. Moshe is a certified Cloud Security Alliance instructor and provides CCSK certification training to cloud environment information security experts in Israel and internationally.

Some of the information in this article is taken from the Cloud Security Alliance Guide for Securing Cloud Computing.