Round Table
How secure is the cloud?

OpenForum Academy
Report

ROUND TABLE 1: How Secure is the Cloud?

15 May 2012, Sofitel Brussels Europe

Disclaimer

This report is prepared by the rapporteur, Dr. E. Altsitsiadis, for OpenForum Academy (OFA). The summaries of the speaker presentations and panel discussions in this report are based on the rapporteur’s notes and they are not in any way binding or necessarily complete. All effort has been given to reflect and convey objectively the essence of the speakers’ presentations and the discussion. The views expressed in the report do not necessarily reflect those of the rapporteur or OFA. Neither the rapporteur, nor OFA should be held accountable for any claimed deviation from the original speeches.
Foreword

The OpenForum Academy organized two Breakfast Round Tables on “Putting the ‘Open’ into Open Innovation” for Cloud computing on the 15th and 23rd of May.

The debates come as the European Commission is putting the final touches to its long-awaited cloud computing strategy for Europe. The EU recognises that it needs to become not only cloud-friendly, but cloud-active, if it is to take full advantage of the benefits cloud computing offers. This is especially true for Europe’s public sector. We believe this is the right moment to debate the merits of a pro-competitive cloud computing environment that is both global and open.

This report summarizes the discussion that took place during the first round table, titled ‘How Secure is the cloud?’. Our three invited speakers discussed the main security issues and challenges with respect to Cloud Computing. The speakers elaborated on the evolution of the security issues, the underlying trends that are now surfacing and how to approach cyber-security. In the discussion that followed, a number of topics were touched, from the new era of Bring-your-own-device and the resulting challenges, to cost-effective assurance and the way to promote it, to the EU perspective and the need for industry collaboration.

The cloud is an economic opportunity but in order to be able to exploit it, Europe should take a light touch approach, avoid “local emphasis”, help bring more transparency and harmonize its legislation to facilitate cloud uptake.

“In this world there is no such thing 100% security, the best we can do is try to be close to 100%”
Speakers:

Hans Graux, time.lex and K.U. Leuven

Eran Feigenbaum, Google - Director of Security for Google Enterprise.

Nick Coleman, IBM - Global Cloud Security Leader for IBM within the services organisation.

Moderator: Graham Taylor, CEO of OpenForum Europe.

Rapporteur: Dr. Efthymios Altsitsiadis, KU Leuven - Research Group Marketing
**Graham Taylor** quickly introduced the Open Forum Academy round tables theme and their overarching aim to put the linkage between open and openness into open innovation. The Cloud is one aspect of IT that has the potential to revolutionise the market, both for supplier and consumer. But there is considerable debate not just on the opportunity but potential blockers to success. In this the first of two Round tables we will be looking at the issue of security. The European Commission has understood the importance and the opportunity value and it resisted the temptation of pursuing a restricted (e.g. European) cloud. As Kroes said, it is not just about making Europe cloud-friendly but cloud-active, it is also about encouraging the use of the cloud. Referring to Jim Welsh’s presentation urging for very little intervention, Mr. Taylor stressed that we need to increase understanding of what the potential issues are around using the cloud. Those about legislation, jurisdiction and security are the ones emerging very quickly, much of which goes back to confidence and trust, both of which are touched in these round tables.

**Mr. Graux** talked about the major topics with regards to security issues and concerns in the cloud. These issues have now evolved from being a largely academic topic, to being a real life operational challenge. Mr. Graux grouped security challenges under three phases of cloud computing project setups, namely: scope, operations and termination.

There is a gradual shift with regards to the type of data and services that are entrusted to the cloud; as maturity increases, vital assets (e.g. HR data) are now increasingly placed in the cloud. US cyber-legislation is one of the barriers for cloud adoption in Europe; the trust concerns with regards to data hosted in the US that stem mostly from the Patriot Act, are commonly used either as a reason or at least as an excuse for not adopting the cloud.

The operational aspects of the cloud are quite similar to what one sees with traditional outsourcing services with the exception of increased requirements for the cloud. Auditing mechanisms are a major but difficult issue also from a policy perspective. Direct auditing possibilities by the customer itself are required by companies that want to entrust data to external service providers, but from an operations point of view this remains very challenging. Data breach notifications is another challenge that will become increasingly more common. Mr. Graux noted the increasing maturity of cloud computing also with respect to guarantees and warranties.

Termination is one of the issues explicitly raised by customers; they acknowledge that such provisions might come with a cost, but they are increasingly more concerned about data mobility and migration and having the possibility to shift cloud providers.

In conclusion Mr. Graux highlighted the overall maturity, noting that there are still barriers, but that most of these can be resolved more and more easily by building on past experience. Some policy challenges remain; notably, it should be made easier for cloud providers to be able to assess the compliance of their service with the existing rules and principles.
**Eran Feigenbaum** started off by suggesting that clouds can be as secure if not more than what most organizations are doing. Not all clouds are created equal and the fact that some providers may have some issues in the future might give a bad mark for the industry. Looking at the underlying patterns in customer needs and how they would be different in the cloud, some interesting trends become apparent: costs for companies to manage servers remain high, and offer a limited efficiency from a security point of view (e.g. delays in patch deployment).

Another consistent trend is that user expectations are different and considerably higher. Times have changed and if users are not enabled they find other ways to get their job done which can be less safe (e.g. USB sticks). When Google thinks about security, it looks at three components: people process and technology. Google is manufacturing its own servers, which allows the creation of a homogeneous environment as all servers look the same and are easier to manage (from patching to anomaly detection), and the ability to drop features that are not needed but could become a security liability. Looking at the technology perspective, Mr. Feigenbaum talked about the security benefits of using multiple redundant servers and the practice of storing multiple copies of data chunks within and between centers.

Most providers do not support customers performing their own auditing due to its impracticality with Third-party-audits being a potential alternative. The lack of transparency is an important concern. Very few companies have the resources to respond to sophisticated attacks. In conclusion it all comes down to trust; in order to win it, cloud providers need to be fully honest and apologize when they have made a mistake.

**Nick Coleman** talked about cyber-security, where security is moving to and how that applies to the cloud. Mr. Coleman referred to and introduced the definition of the four disciplines of assurance: leadership and governance, continuous risk management, policy and operations, monitoring and assurance. He showed for example every government department in the UK now has at board level an information risk owner (senior risk owner), who makes sure that information assurance is delivered in the organization. Embedding these principles in business-as-usual instead of treating security as a stand-alone, extra procedure is crucial in reducing the overall security risks. Mr. Coleman noted that overall the threat landscape is changing, demanding more immediate response and an evolution of the four principles.

In the second part of his comments Mr. Coleman talked about Cloud Computing and that there are different models of Cloud Computing. He also talked about evolving security for the cloud and also building out from the security heritages. Citing for example in IBM cloud delivered services are within existing IBM data centers thus benefiting from the existing infrastructure. IBM, he also mentioned, gives its customers flexibility and the ability to decide on which delivery center they put their data in. He summarized by saying the main questions that come to

---

1The Coleman Report, UK Government
the mind of the cloud customer are still usually: Where is my data? Who will have access to it, and how can I be assured of what is going on? Mr. Coleman talked about cost effective assurance and how important it is to bring the principles of assurance for both the process, as well as for the people and also for the technology. The four principles underpinning this, delivering security in all the different business models a continuous risk managed set of solution which can be assured.
Discussion

Disclaimer: These comments were taken from the general part of the meeting and do not necessarily represent any of the speakers’ views or those of their organisations.

- Is there something different about the cloud?

There are certainly differences; security-wise for example assurances from cloud providers are far from those of typical outsourcing. Scale offers advantages to SMEs but the way we consume cloud services is very different; for example moving to the tablet brings new challenges. Increased flexibility brings higher level of security but safeguarding the access point to the cloud is an important issue for the users.

Scalability (rapid scale up or down) is without doubt a major difference, but another interesting one is the requirement to define the clarity of who’s responsible for what.

- Cost effective assurance – the majority of cloud users will be SMEs and many of the providers of cloud services will be SMEs. How are you going to convince that these SMEs have the right assurance levels?

One has to understand the landscape he is really operating in and what the requirements and the right model for that service are. The cost-effective piece is benefited by building assurance in at the infrastructure level, and delegating assurance to the provider.

- Is there clarity in the architectural, infrastructural, security, contractual model for the different roles?

There is clarity. It is absolutely important to be very clear and that everyone understands who does what. The interesting value is the software and service aspect, going from one extreme to the other. Not everything should move to the cloud; on premise software is not going away, but the interesting innovations will happen in the cloud.

- From a European perspective; how much intervention is needed and where could Europe contribute?

A type of single global standard would be more sensible, limitations like European Cloud could be limiting the resulting benefits. The data loss after the recent natural disaster in Japan is an example of the drawbacks of the “local” emphasis and the restriction of the global aspects of the cloud. Overall a light touch approach is preferable. We need to provide mechanisms for customers to determine whether a service complies with existing rules.

Following what ENISA said, what we need to do is bring transparency. The industry came together to really talk about the issues; there was commonality on the
challenges. Europe should do more on that respect; industry should collaborate more to discuss best practice.

- What about the new era of bring your own device and how do we deal with that?

Bring your own device is indeed a rising trend, but cloud providers would expect to be able to put their corporate policy on the device. There are nevertheless challenges from both a policy-conceptual and technical implementation point of view. Extending the security approaches (scanning of devices and so on) to the mobiles and other devices is important. Not all the data will move to the cloud, information and security policies need to be managed appropriately and be made easier for the user. We need to design systems that make it easy for users to do the right thing and they will. If we don’t provide them with the necessary tools, users will need to engage in unsafe application usage in order to do their job.

Bring your own device is here to stay, but there are still risks. People losing their laptops is a very crucial security issue; password protection would not suffice, establishing consistent corporate policies is necessary together with data encryption. There’s still a long way ahead, however, in order for users to take all the necessary precautions and device makers to facilitate this process (privacy by design).

Bring your own device, however, is broader; how we use and invent technology and how we need to secure this. This effort includes the food chain, the manufacturer of drugs and so on. We’ve always looked at ICT in security but we are now starting to see pervasive computing.

As one participant suggested and the speakers agreed, “...in this world there is no such thing 100% security, the best we can do is try to be close to 100%”.

- How do we make Europe cloud active? What should the European Commission do?

Cloud is an economic opportunity, to become active Europe should help educate people on the potential of the cloud and help them consume it faster.

Regulation should change; there’s a lot of benefit that European companies are not reaping because of the existing legislation causing Europe to fall behind the rest of the world.

More harmonization of legislation is needed; Europe should understand the detrimental impact of legislation on the uptake of the cloud and let information flow more freely.

Cost-effective assurance in Europe should be approached through frameworks which really facilitate people to achieve this cost effectiveness assurance. We should promote the use of cost-effective assurance standards and principles that have been proved effective and stood the test of time.
Short Speaker Bios

Hans Graux, time.lex and K.U. Leuven - Hans is a partner at time.lex, an associate researcher at the Interdisciplinary Centre for Law and ICT at the K.U.Leuven, and an independent legal expert in the Flemish Supervisory Committee (Vlaamse Toezichtscommissie). Hans frequently acts as a legal advisor to the European Commission in several policy areas, including electronic signatures, identity management, privacy protection and e-procurement. In 2007 he co-founded time.lex. His recent assignments center mainly around data protection (privacy protection), cloud computing, open source software development and geographic information systems.

Eran Feigenbaum, Google - Director of Security for Google Enterprise. Eran defines and implements security strategy for Google's suite of solutions of Enterprise Products. Prior to joining Google in 2007, Eran was the US Chief Information Security Officer for PricewaterhouseCoopers (PwC). At PwC, he led a team responsible for all aspects of network, server, application, and desktop computer security, as well as security policies, architectures, standards and enforcement. Earlier, Eran spent several years designing and implementing high-performance cryptosystems for electronic commerce solutions for Fortune 1000 clients and government agencies. Eran holds a bachelor's degree in electrical and computer engineering from the University of California at Irvine, and an MBA from Pepperdine University. In his spare time, he enjoys performing magic and mentalism and was featured on the NBC television show Phenomenon.

Nick Coleman, IBM - Global Cloud Security Leader. Nick is responsible for leading in IBM in securing cloud computing worldwide based within the services organisation. Prior to this he was with the UK Government, where he was the UK Government Reviewer. He authored the 'Coleman Report' published in 2008 by the Cabinet Office. He is an appointed advisor to the EU Network and Information Security Agency (ENISA) serving on the Permanent Stakeholders Group. He is a fellow of the Institution of Engineering and Technology (IET) and a Fellow of the British Computer Society (BCS). He holds an MBA with distinction from Manchester Business School.