CLOUD IN FINANCIAL SERVICES

WEBINAR 5

CLOUD SECURITY

Q&As

The 5th Cloud in Financial Services Webinar in our 10-part series has been designed to provide the C-Suite, Board Members, CIOs/Heads of Infrastructure and Architecture in financial institutions an overview of strategic and policy considerations regarding Cloud security.

Those who attended will be aware that due to the number and nature of the engaging questions asked by our attendees, our panellists were unable to answer them all sufficiently within the hour. As such, we would like to share a list of Q&As from our first webinar that we hope provide a more thorough explanation of the topics explored.

#	Question	Answer
1	Based on your experience, what is the customers' reaction to cloud security and secure cloud adoption? Do they simply try to apply already available security controls, tools and processes in the cloud, or do they work towards understanding the new concepts and possibilities offered by the cloud and then revise their security strategy to include the Cloud itself?	The decision really depends on the customer, but we tend to discriminate between two main cases: 1) Cloud security provision is included from the start of the strategy definition phase 2) Cloud security provision simply reacts to urgent business requests In the first instance, security departments are better able to grasp the chosen cloud model as well as their company's vision for the cloud evolution, with the option to re-design the security approach from a strategic point of view. Security departments have time to review their security controls, tools and processes and to assign priorities that are in line with the cloud evolution set out by IT and the business. Customers are also more likely to accept the security services offered by the CSP and to better integrate those services into the monitoring and governance tools and processes that are already in use. In the second instance, where security departments simply react to urgent requests coming from IT or the business, the most probable choice is to apply existing security controls, tools and processes and force the CSP or the implementation project to adapt accordingly. In this case, security can became a show stopper for any cloud adoption initiative or be the driver for keep using legacy models. These legacy models are often not cloud-friendly and potentially limit some of the benefits associated with the cloud.
2	With the fact of cloud being agile, why do you think that security seems to follow cloud adoption over trying to lead it.	This usually happens when the existing security provision is not suitable for cloud-based environments, due to lack of resources or skills, and when security doesn't evolve into a business enabler function. Being security experts, Reply believes that sooner or later the cloud - in some shape or form - will be feature in every organisation. It is no longer a matter of "if", just a matter of "when", so companies need to start preparing for it. This means transforming security departments from their legacy role of "requirements and constraints producers" into their new role of "business enablers" to provide the business with all of the capabilities needed to implement new technical solutions and enable new business models. It also requires a change in mentality, which the majority of the organisations still need to go through, including those with on-premise systems. The flexibility and the agility of the cloud is driving the importance of culture change.
3	Many of the consumer facing services provided today are made up of more than one cloud based service, how do we manage consistent security across them all?	From our point of view, multi-cloud security is based on 4 main pillars: 1. One set of cloud-security policies, applicable across clouds, that leverage abstraction of concepts to define the overarching security policy 2. The translation of those policies in CSP-specific security requirements 3. Automation (or at least simplification) of CSP-specific security requirement assessments and enforcements 4. Monitoring and remediation This approach is based on the following: - Security principles should not depend on specific underlying technologies - Cloud environments can be very heterogeneous, hence why the enforcement of a security principle usually requires deep knowledge of the cloud platform

		- Providing documentation is not enough, enforcement and monitoring are key Tools, which provide visibility and assessment and which define security guardrails across several IaaS/SaaS platforms, are already available, even if they usually don't offer the same level of coverage for all of the supported CSPs.
4	What are some common cloud security risks that seem small but can actually be quite large?	The most underestimated risk is the exit strategy. Vendor lock-in is a key concern for many customers, who tend to adopt countermeasures by using multi cloud and/or hybrid environments. However, not every customer has a well-defined, tested and maintained exit strategy and related transition plan. Whilst companies tend to rely on theirs CSPs, these are not 100% fool proof either. Companies therefore always need to be ready to migrate data and workload from one CSP to another. This migration can be organisationally and technically complex and depends on many variables such as deployment model (IaaS, PaaS, SaaS), CSP etc. This aspect is also addressed by the EBA: "the outsourcing institution should plan and implement arrangements to maintain the continuity of its business in the event that the provision of services by an outsourcing service provider fails or deteriorates to an unacceptable degree." Disaster recovery is another critical aspect that is not always fully addressed.

REPLY

Reply [MTA, STAR: REY] specialises in the design and implementation of solutions based on new communication channels and digital media. As a network of highly specialised companies, Reply defines and develops business models enabled by the new models of big data, cloud computing, digital media and the internet of things. Reply delivers consulting, system integration and digital services to organisations across the telecom and media; industry and services; banking and insurance; and public sectors. www.reply.com