Cloud Computing

Here to Stay … but Transparency is Key for Vendors as Regulation tightens

The Key Questions CIOs should ask when evaluating a Cloud solution today

mavinTree

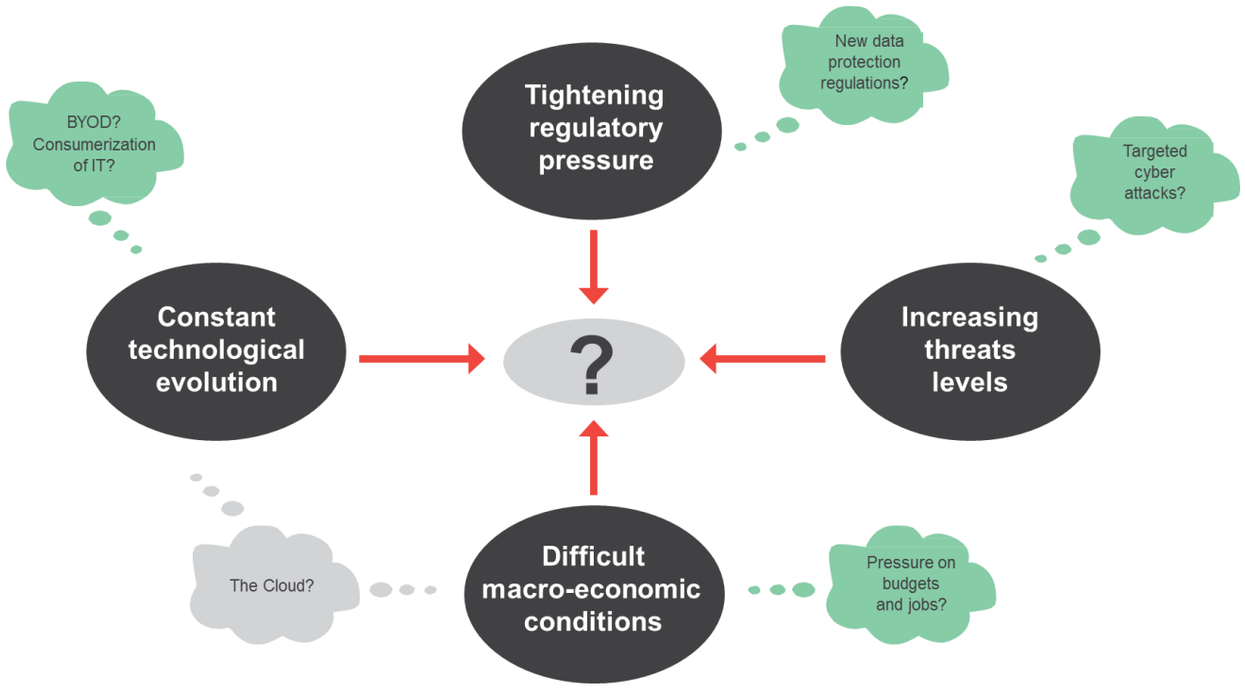
corix partners

Corix Partners first analysed “Security in the Cloud” back in 2012

In 2012, the pressure on the CIO and other C-level executives was principally to reduce cost whilst also increasing flexibility.

- Corix Partners whitepaper: “A balanced approach to cloud computing”

Mostly, this meant moving activities previously done in-house into the Cloud, in the context of the early stages of what has become know as “Digital Transformation”



However, there was a significant, and largely unquantified, reluctance by many to move into the Cloud, cyber security being seen as the dominant blocking factor

How has Cloud Computing changed since 2012

The pressures on the CIO and other C-level executives has continued to grow but there is a much greater emphasis on flexibility and agility

- Digital Transformation is gathering pace and disrupting most business sectors
- Cost effectiveness is still important but often not the primary driver

Cloud Acceptance has continued to grow steadily in spite of any security concerns

Many new digital services are being created in the Cloud and do not exist elsewhere or without it

Cloud Service providers have considerably matured their offerings and the market has consolidated at the top end

Cloud vendor assessments have become common place

- In today's increasingly complex business environment, many organisations are both customers and suppliers of digital services

The use of the Cloud is unavoidable and the question has shifted from IF to HOW to use the Cloud

Today's Cloud Marketplace

The Cloud marketplace is dominated by a number of major players:

- Amazon
- Google
- IBM
- Microsoft

Many of the smaller Cloud Service providers are leveraging the infrastructure provided by one of the major players

- Consequently, the supply chain is more complex and may not be obvious

"The Cloud" is not just one concept and hides many different products and combinations

- In our 2012 whitepaper, we highlighted that IaaS, PaaS and SaaS are all seen as part of "the Cloud" but are in fact very different products
- Pure IaaS appears to be in decline and Hybrid Cloud solution (a mix of external and internal services) have become very common

Commoditisation has reached a point where Cloud-based services are almost dematerialised and it is simply their availability which is now key to users

- Irrespective of any underlying technology components (networks, servers, datacentres, etc.) which are still present but are treated as a mere – invisible – utility managed by the Cloud Service providers

Transparency of Cloud Service providers over their operations and their supply chain is becoming critical to engineer customers' trust

Consequence of Commoditisation is Compromise

The main advantages of the Cloud are directly derived from the commoditisation of computing resources

- Cost – pay for want you use when you use it
- Flexibility – scale up and down on demand

Consolidation of the Cloud marketplace over recent years has led to the emergence of new industry giants and the reinforcement of others

- Cloud Service Providers deliver the same services to multiple customers so cannot allow a single customer to potentially impact their other customers
- Individual organisations cannot expect to exert as much influence over the Cloud Service Providers as they used to
- Traditionally, organisations have required service providers to comply with the purchasing organisation's own IT Policies and Standards: It may now become a matter of compromise

Understanding the extent of such compromise and establishing an achievable and realistic level of assessment of Cloud services is becoming key for most organisations, as regulation tightens (e.g. GDPR in the EU, in addition to pre-existing regulations such as PCI DSS etc…)

Business units, IT, Information Security, Risk and Compliance need to work hand in hand on these matters

The tightening of regulations such as GDPR in the EU will force organisations to leverage on transparency, trust and relationships with Cloud Service Providers to demonstrate compliance

Cloud Service providers must also compromise in the face of increased regulations for their clients

Major Cloud Service Providers have developed mature technology offerings, often originally based on their own internal IT requirements

However, the potential complexity of their supply chain makes it more important to have well defined and understood security processes

Cloud Service Providers must expect increasing compliance demands from their clients as they themselves come under increased compliance pressure

Cloud Service Providers must expect that they will have to be more transparent and demonstrate full adherence to security good practices

- Industry standards play a significant role in defining good practices
- But independent verification that Cloud Service Providers adhere to these good practices is key, and is more important than only obtaining certification

Failure to respond positively and transparently to data security and compliance demands from clients could push business away, as compliance pressure and higher fines reduce the market's appetite for the "commoditisation compromise"

Cloud Service Providers will be judged by their ability to deliver a demonstrably secure and compliant service and this will determine which are successful and prevail

Mid-Term View > GDPR to force a tightening of assessment and relationships with Cloud vendors

GDPR has been adopted within the European Union and will come into full force by 25th May 2018

- GDPR – General Data Protection Regulation (Regulation (EU) 2016/679)

GDPR gives back control of personal data to EU citizens and provides a regulatory environment for international business active within the EU

GDPR re-enacts and strengthens many aspects of earlier legislation (data transfers, data residency) and introduces obligatory disclosure of data breaches together with much heavier fines

All organisations conducting business in the EU or with EU citizens will be impacted and this should drive a significant increase of attention towards data protection and privacy

There is evidence that the major Cloud vendors are already taking this seriously and are determined to ensure their services are endorsed by the EU commission

- Microsoft won in US Court of Appeals so it does not have to disclose data on one of its servers in Ireland to the US Government (14th July 2016)

Data Protection remains the responsibility of each organisation, and they will need to manage all suppliers more actively, including Cloud Service providers, to avoid major fines and reputational damage

Long Term View > Competition for talent and ongoing digital transformation to drive acceleration of move towards the Cloud

Major Cloud Service providers are able to attract, retain and invest in talent more easily because of their scale

- Better career opportunities for technical specialists are likely to exist with major Cloud Service providers
- Other organisations will find it increasingly difficult to attract skilled specialists and there is likely to be a significant premium

The rarity and/or cost of specialist skills required to run commodity services “in-house” (e.g. email and office automation) will lead more organisations to turn to Cloud Services providers for these services

Digital Transformation is radically changing the way IT Services are procured, delivered and operated

- “Shadow IT” is already common place and could become mainstream as the business can just procure IT Services which are then run externally without the involvement or even knowledge of the CIO

The role of the CIO needs to evolve to retain control as the Cloud becomes the only dominant platform to deliver digital services, or the CIO will just be left running internal legacy IT Services

Summary of Key Points

- The use of the Cloud is unavoidable and the question has shifted from IF to HOW to use the Cloud

- Transparency of Cloud Service providers over their operations and their supply chain is becoming critical to engineer customers' trust

- The tightening of regulations such as GDPR in the EU will force organisations to leverage on transparency, trust and relationships with Cloud Service Providers to demonstrate compliance

- Cloud Service Providers will be judged by their ability to deliver a demonstrably secure and compliant service and this will determine which are successful and prevail

- Data Protection remains the responsibility of each organisation, and they will need to manage all suppliers more actively, including Cloud Service providers, to avoid major fines and reputational damage

- The role of the CIO needs to evolve to retain control as the Cloud becomes the only dominant platform to deliver digital services, or the CIO will just be left running internal legacy IT Services

The Key Questions CIOs should ask when evaluating a Cloud solution today

- **Business Sensitivity:** What are the business processes associated with the solution, and what is their overall importance and value for the organisation?
- **Data Sensitivity:** What is the legal or regulatory sensitivity of the data required or supplied to execute those processes?
- **Security & Compliance:** Does the sensitivity of the data and associated business processes impose specific requirements on the solution, over and above you internal security policies, and what are those? (e.g. data residency, data encryption etc…)
- **Transparency & Risk:** Is the real supply chain supporting the solution transparent enough (suppliers and their sub-contractors) and have you got access to all the information you need to assess the real risk profile of the solution?
- **Consistency of Approach:** Are you assessing risk consistently across all architectural components of the solution (internal / external / hybrid)?
- **Validity of Costs Model:** Have you factored the costs of investigating and handling potential data breaches in your ongoing operating model?

Contact

For further information please contact:

Jean-Christophe Gaillard
Managing Director
Corix Partners
+44 (0)7733 001 530
jcgaillard@corixpartners.com

Neil Cordell
Director
Corix Partners
+44 (0)7701 015 275
neilcordell@corixpartners.com

www.corixpartners.com

Rick Warley
Managing Director
mavinTree Limited
+44 (0)7771 838 001
rick.warley@mavintree.co.uk

www.mavintree.co.uk

Many thanks to our focus group members, contributors & reviewers

Contributors

Stephen Deakin, Eccton
Julie George, Post Office
Francois Gratiolet, Business Digital Security
Natasha McCabe, Royal Mail
Richard Preece, Oakas
Julia Harris, Post Office
Alastair Upton, ATG Media
Alan Watkins, StoneShot
Peter Wenham, Trusted Management

Reviewers

Paul Ferron, CA
Blandine Marcelin-McPherson, Fujitsu
Matt Saxon, WorldPay