Started as system administrator at SheerSite, passed to Rapid7 in 2000, and have been at Qualys since 2003.

Work mainly with CAC40 companies.
Agenda

Just Say No!

Adoption despite the risks

Friend or Foe Filter
The Cloud - Just Say No!

“Understanding what drugs cloud can do to your children information system, understanding peer business pressure and understanding why they turn to drugs cloud is... the first step in solving the problem.”

The Real Risks of the Cloud

Q22. Selon vous, les facteurs suivants représentent-ils un risque faible, modéré ou fort en ce qui concerne l'utilisation du Cloud ? *Base : ensemble (141 répondants)*

<table>
<thead>
<tr>
<th>Un Risque fort</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Difficulté de contrôle des accès et audits</td>
<td>57%</td>
</tr>
<tr>
<td>Stockage des données dans des datacenters à l'étranger, hors du droit français</td>
<td>55%</td>
</tr>
<tr>
<td>Non effacement des données</td>
<td>55%</td>
</tr>
<tr>
<td>Confidentialité des données vis-à-vis de l'hébergeur</td>
<td>50%</td>
</tr>
<tr>
<td>Non restitution des données</td>
<td>47%</td>
</tr>
<tr>
<td>Non-maîtrise des paramètres de sécurité / chiffrement faible de la part de l'hébergeur</td>
<td>42%</td>
</tr>
<tr>
<td>Non-maîtrise de l'utilisation qui en est faite par les salariés de votre entreprise</td>
<td>42%</td>
</tr>
<tr>
<td>Traitement Big Data à notre insu</td>
<td>36%</td>
</tr>
<tr>
<td>Indisponibilité des données</td>
<td>30%</td>
</tr>
<tr>
<td>Non-alimentation du SOC (interne ou externe) en données provenant du Cloud</td>
<td>28%</td>
</tr>
<tr>
<td>Propagation systémique des attaques et erreurs humaines</td>
<td>26%</td>
</tr>
<tr>
<td>Disparition de l'hébergeur</td>
<td>24%</td>
</tr>
<tr>
<td>Attaque par rebond depuis l'hébergeur</td>
<td>23%</td>
</tr>
<tr>
<td>Piégeage d'application hébergée</td>
<td>20%</td>
</tr>
<tr>
<td>Corruption de base de données</td>
<td>15%</td>
</tr>
</tbody>
</table>

06/01/2017

“opinionway”

CESIN
Meanwhile the business is adopting

This is the Shadow IT that many fear.

Innovation and flexibility: 18 month application life cycles.

HR, Finance, Marketing, CRM, and Storage services already widely used - more so in media, retail, or telco.

Converting assets into services.
Q20. Certaines des données de votre entreprise sont-elles stockées dans un Cloud ?

*Base : ensemble (141 répondants)*

- Oui, dans des Clouds publics : 43%
- Oui, dans des Clouds hybrides : 20%
- Oui, dans des Clouds privés seulement : 19%

82% des réponses ont été oui, 18% non.

06/01/2017
Because if you listen to the security people, you’ll end up like Hollande.

Perhaps you’ll be in security, but you’ll be dead.

- Emmanuel Macron, Avril 2017
Challenge or be challenged

Who owns the largest taxi company?
Who owns the largest network of hotels?
Who owns the largest messaging application?
Who owns the largest movie house chain?
Largest music service provider?
Challenge or be challenged

Who owns the largest taxi company? (Uber, 2009)
Who owns the largest network of hotels? (AirBnB, 2008)
Who owns the largest messaging application? (WhatsApp, 2009)
Who owns the largest movie house chain? (Netflix 1997, 2007)
Largest music service provider? (Spotify, 2006)

It’s not anymore about risk of adoption - it’s the risk of failing to adopt.

(AWS came on-line in 2006...)
Clear and Present Danger

AOL vs. Netflix: The Broadband Era Illustrated

AOL (Yellow) vs. Netflix (Red) Subscribers, Millions

*Streaming-only subscribers starting in 2012.
Digital Transformation

Web Scale ✔

Automation Generation ✔

Consumer acts directly upon the value chain ✔

95% of CSOs report that “Digital Transformation” is of strategic importance to the enterprise.
Innovation sees inertia as a bug and will route around it.
Control the Flow

Core concerns remain unchanged!

CIAT? Technical and Processes...

Ownership/Liability/Responsibility/Regulation? Legal...
The Cloud is More Secure
The Cloud is More Secure


It’s about the economy of scale.
Aligning interests.
Change the Rules

Ownership/Liability/Responsibility/Regulation:

- work with the cloud vendor to meet your needs
- work with the regulator to compromise
Risk Management Life Cycle

Office of the Comptroller of the Currency bulletin 2013-29

Guidance for assessing and managing risks associated with third-party relationships.

Practice effective risk management regardless of whether the activity is performed internally or through a third party.
Procurement in the Cloud Era

Many risks are already covered by procurement:

- Financial (stability of the vendor/supplier)
- Legal (intellectual property, liability, ...)
- Brand (quality of the product, fit for purpose, ...)
- Regulatory or sectoral compliance (where applicable)

Managing third party risk to the supply chain.
Many risks are already covered by procurement:

- Financial (stability of the vendor/supplier)
- Legal (intellectual property, liability, …)
- Brand (quality of the product, fit for purpose, …)
- Regulatory or sectoral compliance (where applicable)
- Cyber risk to the supply chain (vendor audits, integrated information security policies, …)

Managing third party risk to the supply chain.
Procurement in the Cloud Era

In 2012 a large French enterprise created a review board for service outsourcing.

In 2014 the Energy Sector Control Systems Working Group updated the “Cybersecurity Procurement Language for Energy Delivery Systems”

Some Qualys customers have very close ties at the CSO level, using CIS as a baseline around which to integrate information systems security policies.
Mission of a Review Board

Control externalized information systems and their associated risks.

- Make business units aware of the risks introduced by externalisation.
- Give guidance on the externalized information systems regarding security, legal, procurement, protecting assets, brand, ...
- Publish recommendations and best practices.

Bonus: you can now map out all the externalized information system components you used.
Two New Requirements

Two requirements were formulated:

- The business information system managers must be consulted when projects start for either new or updating components;
- The information system managers must submit a case to a review board.
What Should be Submitted to a Review Board

1. Context and objectives
2. Perimeter and constraints
3. Actors
4. Macro-planning
5. Security of immaterial assets
6. Data protection
7. Technical architecture
8. Organisation of maintenance
9. Financial study
10. Procurement and contracting
11. Risk analysis
12. Summary document
Risks are evaluated and compensating controls identified and a residual risk calculated by a review board.

The requesting business unit must accept the risks and implement the identified compensating controls.
Procurement and Contracts

1. Deploy the service
2. Life of the service
3. Reversibility

Annex: Information System Security

Annex: Data Protection (GDPR, ICO, CNIL, ...)

Include SaaS specific requirements
Conclusions

Adopting the cloud is unavoidable.

Get management buy-in to adjust existing procurement processes to encompass the special needs of externalized/cloud information systems.

Create a streamlined, clearly understood, process to review and validate all cloud projects. No exceptions!

Business unit owners are ultimately best placed to weigh the cost/benefit of a project - this includes cloud solutions.
Questions?
Thank You