Adopting a Frame of Reference for Confidence in the Cloud

John Weigelt
Chief Technology Officer
Microsoft Canada
@Thumbtackhead
Enterprise Leaders in 2015

**CEO priorities**

- **Enhancing the customer experience**: Outperforming enterprises are 54% more likely to engage employees and satisfy customers.

- **Transforming to a digital business**: 79% of C-level executives believe they make better and faster tech decisions than IT.

- **Becoming more responsive**: 70% of CIOs would increase risk to reduce IT costs and accelerate business agility.

**Enhancing the customer experience**

- 60% of CxOs now look for partners who will have an equal hand in creating business value.

- 7 in 10 CEOs believe social/digital interaction is the new imperative.

- 37% of decision makers prioritize enhancing customer experience.

**Transforming to a digital business**

- 27% of tech budgets are controlled by departments other than IT.

- 79% of C-level executives believe they make better and faster tech decisions than IT.

- 7 in 10 CEOs believe social/digital interaction is the new imperative.

**Becoming more responsive**

- 70% of CIOs would increase risk to reduce IT costs and accelerate business agility.

- 60% of CxOs believe social/digital interaction is the new imperative.

- 7 in 10 CEOs believe social/digital interaction is the new imperative.

**Dual goals**

- Responding to ongoing needs for efficiency and growth.

- Exploiting a fundamentally different digital paradigm.
Canadian C-suite executives do not have a solid grasp on cloud computing

1 IN 10 C-SUITE EXECUTIVES Are familiar with the cloud

Do not know what cloud services are used for

45% Couldn’t correctly identify the definition of cloud computing

57% Of c-suite executives Are not involved in Or discussing Cloud computing
Security and privacy should be a top leadership concern
Managing risk in an increasingly connected world

“This Nexus of Forces is impacting security in terms of new vulnerabilities.”


243 median # of days attackers are present on a victim network before detection

$3.5M Average cost of a data breach to a company

15% increase YoY

Implications
Security is a CEO level issue

Job security  Customer loyalty
Brand reputation  Legal liability
Intellectual property

Impact of cyber attacks could be as much as $3 trillion in lost productivity and growth
Remember that server you used to have
Microsoft’s Datacenter Evolution

<table>
<thead>
<tr>
<th>Year</th>
<th>Location</th>
<th>Datacenter Generation</th>
</tr>
</thead>
<tbody>
<tr>
<td>2005</td>
<td>Quincy and San Antonio</td>
<td>Generation 1</td>
</tr>
<tr>
<td>2006</td>
<td>Chicago and Dublin</td>
<td>Generation 2</td>
</tr>
<tr>
<td>2007</td>
<td>Modular Datacenter</td>
<td>Generation 3</td>
</tr>
<tr>
<td>2008</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2009</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Deployment Scale Unit**

- **Server**: Capacity
- **Rack**: Density and Deployment
- **Containers**: Scalability and ...Sustainability
- **IT PAC**: Time to Market, Lower TCO

**Facility PAC**
Huge infrastructure scale is the enabler

24 Regions Worldwide, 19 ONLINE...huge capacity around the world...growing every year

- 100+ datacenters
- Top 3 networks in the world
  - Coverage, Speed, Connections
- 2x AWS + Google Combined
Trusted Cloud Principles
Commitment to principles worthy of your organization’s trust

<table>
<thead>
<tr>
<th>Security</th>
<th>Privacy &amp; Control</th>
<th>Compliance</th>
<th>Transparency</th>
</tr>
</thead>
<tbody>
<tr>
<td>The confidentiality, integrity, and availability of your data is protected.</td>
<td>No one is able to use your data in a way that you do not approve.</td>
<td>Your content is stored and managed in compliance with applicable laws, regulations and standards.</td>
<td>You have visibility into how your data is being handled and used.</td>
</tr>
</tbody>
</table>
Data Handling
Operational
Transparency and control: running the service

Most operations are automated

Data Center operations do not require access to customer content

Rare occasions where humans need access to run data center operations

Humans have to meet clearance requirements and require 2 factor auth to request access

Any access is highly controlled with multiple levels of approval using Lockbox
Lockbox

Scoped, least privileged access
Just-in-time access for limited duration
Audit logs for all access
Customer Lockbox

Now we want to extend Lockbox approval to you for human access to customer content

Customer controls authorization of Office 365 personnel access
Security

Physical
Network
Host Security
Application
Data

Identity and access management
Configuration and vulnerability scanning
24x7x365 Incident response

An example of Defense-in-Depth
Digital Crimes Unit & Cybercrime Center

Making an impact

- **Taking down botnets**, in partnership with governmental and commercial organizations, to clean and protect tens of millions of devices
- **Improving products** by embedding collected data and intelligence into our platform and services
- **Disrupting and dismantling cybercriminal operations** that promote a range of illegal goods and services
- **Developed PhotoDNA** to protect children from online exploitation

Big data | Investigations | Legal action

Malware disruption

IP Protection

Protection of vulnerable populations
Protecting your data privacy

You have a right to expect:

• Your content should only be accessed as permitted by you, and should not be shared with third parties unless permitted by you.
• You should always have access to your content, and should be able to delete it or take it with you if you leave.

What we’re doing about it:

• We allow you to keep the data you upload in the region you specify.
• We will not use your data for advertising or commercial purposes.
• We will not disclose your information outside of Microsoft except with your consent or when required by law.
• We provide a variety of tools to extract your data.
• Azure will fully delete your data within 180 days after expiration or termination.
<table>
<thead>
<tr>
<th>Key Principles – Cloud providers must:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not use data for advertising or marketing unless express <strong>consent</strong> is obtained</td>
</tr>
<tr>
<td>Be <strong>transparent</strong> about data location and how data is handled</td>
</tr>
<tr>
<td>Be <strong>accountable</strong> to determine if customer data was impacted by a breach of information security</td>
</tr>
<tr>
<td><strong>Communicate</strong> to customers and regulators in the event of a breach</td>
</tr>
<tr>
<td>Provide customers with <strong>control</strong> over how their data is used</td>
</tr>
<tr>
<td>Have services <strong>independently audited</strong> for compliance with this standard</td>
</tr>
</tbody>
</table>
You have a right to expect:

• You should have a clear, plain-language explanation of how your cloud provider uses, manages and protects your organization’s content.

• You should be told how your cloud provider will respond to law enforcement requests to access your organization’s content.

What we’re doing about it:

• We provide understandable and strict policy of what we will—and will NOT—use your content for.

• When responding to law enforcement requests, we strive to defend your rights and privacy, and ensure due process is followed.

• For each of our services, we provide you with information on where your content may be stored and processed.

Microsoft NDA-To be shared under NDA only
Master Controls Approach

AREAS OF REGULATORY CONCERN
- Patching
- Malware
- Training
- Physical
- SDL
- Mgt
- Policy
- Assets

COMMON CONTROLS FRAMEWORK
- SLAM
- IcM
- QE
- ...
- ...
- ...
- ...
- Cn

ISO 27001
NIST 800-53
CSA
UCF
SOC1
SOC2

Engineering
Operations
Security
MCIO
HR
Legal
Procurement
Sales
Selection vs Specification
## Getting Comfortable

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select a service to be provided</td>
<td></td>
</tr>
<tr>
<td>Assess the compliance environment</td>
<td></td>
</tr>
<tr>
<td>Review the current &quot;as-is&quot; environment</td>
<td></td>
</tr>
<tr>
<td>Conduct preliminary PIA &amp; TRA</td>
<td></td>
</tr>
<tr>
<td>Pilot the service</td>
<td></td>
</tr>
<tr>
<td>Assess the risk delta</td>
<td></td>
</tr>
<tr>
<td>Review the SLA</td>
<td></td>
</tr>
<tr>
<td>Build out the business case</td>
<td></td>
</tr>
<tr>
<td>Decide and manage the risk</td>
<td></td>
</tr>
<tr>
<td>Consume the cloud service</td>
<td></td>
</tr>
</tbody>
</table>
John Weigelt
Johnwei@microsoft.com
@Thumbtackhead