ADDRESSING THE MISMATCH

SANS CLOUD SUMMIT

Ben Johnson | Co-Founder & CTO

OBSIDIAN
Background Check // Ben Johnson

Co-Founder and CTO, Obsidian
Co-Founder and Former CTO, Carbon Black
Former CNO/Cyber // NSA, CIA, DoD
Today’s Goal?

TO SPARK CONTEMPLATION

(and give you something to remember!)
Transformation
Digital Transformation

LET’S IMPLEMENT CLOUD COMPUTING SO I HAVE SOMETHING TO TALK ABOUT AT THE EXECUTIVE MEETING.

TELL THEM WE’RE EVALUATING IT. THAT WAY NEITHER OF US NEEDS TO DO ANY REAL WORK.

I LIKE IT WHEN YOU DO REAL WORK.

SORRY. I THOUGHT YOU WERE LEADING BY EXAMPLE.

I HIRED A CONSULTANT TO HELP US EVOLVE OUR PRODUCTS TO CLOUD COMPUTING.

BLAH BLAH CLOUD. BLAH BLAH CLOUD. BLAH BLAH CLOUD. BLAH BLAH CLOUD.

IT’S AS IF YOU’RE A TECHNOLOGIST AND A PHILOSOPHER ALL IN ONE!

/// BLAH BLAH PLATFORM.
Lots of benefits of cloud adoption … we aren’t really here for that.
IT and the Cloud

IT

“IT is the broad subject concerned with all aspects of managing and processing information, especially within a large organization or company.”

Cloud

Cloud computing is an information technology (IT) paradigm that enables ubiquitous access to shared pools of configurable system resources and higher-level services that can be rapidly provisioned with minimal management effort, often over the Internet. Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to a public utility.
IT and the Cloud (Reality)

“Let’s stop managing hardware and a lot of the software”

“Let’s scale up and down as necessary”

“Let’s get access to cool new technologies more quickly”

“Uptime is [mostly] someone else’s problem”
Information Security and the Cloud

InfoSec

“Information security, sometimes shortened to InfoSec, is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information.”

Cloud

Cloud computing is an information technology (IT) paradigm that enables ubiquitous access to shared pools of configurable system resources and higher-level services that can be rapidly provisioned with minimal management effort, often over the Internet. Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to a public utility.
Information Security and the Cloud (Reality)

“IT is going from 0 to 100 in the cloud and leaving security in the dust”
- Fmr. CISO, Lending Club

“We’re blind to all these new SaaS accounts”
- Director, Cyber Intelligence, Top Athletics Brand

“We don’t know what users are doing on our AWS/Azure accounts”
- Too Many Organizations
Modern Times are Leaky

Booz Allen
OneLogin
The RNC
Verizon
Accenture
Dow Jones
Viacom
Deloitte
Sweden
California
Recent Headlines

- Deloitte Hack May Have Exposed Emails, Passwords Of Clients And Staff
- Booz Allen Hamilton leaves 60,000 unsecured DOD files on AWS server
- Dow Jones customer data exposed in cloud error
- OneLogin security chief reveals new details of data breach
- Another AWS leak exposes 150,000 Patient Home Monitoring Corp. client records
- Viacom Leak May Have Exposed Hundreds of Digital Properties—Paramount Pictures, Comedy Central, MTV, and More
- Verizon Suffers Cloud Data Leak Exposing Data on Millions of Customers
- Sweden Accidentally Leaks Personal Details of Nearly All Citizens
- Data of almost 200 million voters leaked online by GOP analytics firm
Data Breaches
Data Breaches: Not Just IaaS

Deloitte reportedly suffered hack during email migration to Office 365

As of now, Deloitte cannot be "100% sure what was taken" by the hackers

Breach Fatigue Anyone?

Anyone getting CLOUD breach fatigue?

If not you, do you think others are?
Causation
Confusion Over Responsibility
Providers Have Challenges

Goals are Misaligned

Focus is on availability of variety of services with a minimum layer of security built-in

Failure Can Be Easy

A simple click can share huge amounts of data publicly (e.g. S3)

Monitoring is Extra Work

Logging & monitoring often have to be enabled separately

Mo’ People, Mo’ Complexity

Identities and policies are often complex to manage (maybe an understatement?)

Sweet Spot is Elusive

Policy and control options either feel too flexible or too rigid
Customers Have Challenges

Lack of Understanding

The notion of shared responsibility and the differences in built-in security are often foreign.

Taking the Plunge

Departments race to the cloud, leaving security scrambling. (Is security slowing down adoption?)

Bending the Rules

Unsanctioned cloud use or lack of reporting to security what is in use.

New Environment, Same Security Team

Surface area is expanding, changing, and dynamic, yet security team isn’t as agile.

“Operators think that once it’s in the cloud it’s no longer their responsibility”

- Fmr. CIO of the Air Force
Current Trends Making Things Harder

SKILLS GAP
DEPLOY-AND-DECAY
LACK OF CYER SELF-ESTEEM
HUGE DATA
HACKER SUCCESSES
IT and Security Disconnect

IT
Authentication
Authorization
Enablement
Provisioning

Security
Activity
Threat Management
Anomaly Detection

DISCONNECTED
Obligation
Cloud Service Provider:

responsible for security **OF** the cloud

Customer:

responsible for security **IN** the cloud
AWS Responsibilities?

CUSTOMER

RESPONSIBLE FOR SECURITY “IN” THE CLOUD

CUSTOMER DATA
PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT
OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION
SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)
NETWORK TRAFFIC PROTECTION (ENCRYPTION/INTEGRITY/IDENTITY)

AWS

RESPONSIBLE FOR SECURITY “OF” THE CLOUD

COMPUTE
STORAGE
DATABASE
NETWORKING

AWS GLOBAL INFRASTRUCTURE

REGIONS
AVAILABILITY ZONES
EDGE LOCATIONS
AZURE Responsibilities?

Microsoft understands how different cloud service models affect the ways that responsibilities are shared between CSPs and customers.

<table>
<thead>
<tr>
<th>Responsibility</th>
<th>On-Prem</th>
<th>IaaS</th>
<th>PaaS</th>
<th>SaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data classification &amp; accountability</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client &amp; end-point protection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity &amp; access management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application level controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Host infrastructure</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical security</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Figure 1: Shared responsibilities for different cloud service models*
The SaaS Provider handles all aspects except for identity and access management, client devices controls, and data accountability.

The Customer, therefore, must understand users, devices & data related to that service.
Microsoft handles the underlying infrastructure, including patching and updating, and handles accessibility of the service.

You are responsible for what is emailed, who accesses the email, and how they access the email.
# AZURE Responsibilities?

**Hackers want this!**

## Shared responsibilities

Microsoft understands how different cloud service models affect the ways that responsibilities are shared between CSPs and customers.

<table>
<thead>
<tr>
<th>Responsibility</th>
<th>On-Prem</th>
<th>IaaS</th>
<th>PaaS</th>
<th>SaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data classification &amp; accountability</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client &amp; end-point protection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity &amp; access management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application level controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Host infrastructure</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical security</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

@chicagoben | @obsidiansec

---

*Figure 1: Shared responsibilities for different cloud service models*
AWS Responsibilities?

Hackers want this!
Amelioration
Awareness, Auditing, Adaptation, Automation
Awareness

๏ Where are you using the cloud?
๏ What “clouds” are you using?
๏ Why are you using the cloud?
๏ How are you using the cloud?
๏ Who’s responsible for what’s in the cloud?
Auditing

- Understand current state (IT)…assets, users, devices.
- Understand current state (Security).
- Understand initiatives that involve cloud.
- Understand security capabilities related to cloud.
Adaptation

- Put policies and checks in place for new deployments
- Update security scans and tests to account for cloud
- Enable tracking of all changes from current state
- Have a process for monitoring all new accounts, assets, etc.
Change your processes to reduce risk!

Security audits should be automated.

Cloud Providers have APIs – write code or use integrations to automate the collection of data, the taking of actions, the verification of changes.

Avoid manual activities.
Hygiene
Triple-A!

**Authentication**

- Industry focus

**Authorization**

- Neglected

**Accounting**

- Forgotten

@chicagoben | @obsidiansec
## IT and Security: Hand-in-Hand

<table>
<thead>
<tr>
<th>Where are you using the cloud?</th>
<th>Put policies and checks in place for new deployments</th>
</tr>
</thead>
<tbody>
<tr>
<td>What “clouds” are you using?</td>
<td>Update security scans and tests to account for cloud</td>
</tr>
<tr>
<td>Why are you using the cloud?</td>
<td>Enable tracking of all changes from current state</td>
</tr>
<tr>
<td>How are you using the cloud?</td>
<td>Have a process for monitoring all new accounts, assets, etc.</td>
</tr>
<tr>
<td>Who’s responsible for what’s in the cloud?</td>
<td>Change your processes to reduce risk!</td>
</tr>
<tr>
<td></td>
<td>Security audits should be automated.</td>
</tr>
<tr>
<td></td>
<td>Cloud Providers have APIs – write code or use integrations to automate the collection of data, the taking of actions, the verification of changes.</td>
</tr>
<tr>
<td></td>
<td>Avoid manual activities.</td>
</tr>
</tbody>
</table>

- Understand current state (IT)...assets, users, devices.
- Understand current state (Security).
- Understand initiatives that involve cloud.
- Understand security capabilities related to cloud.
IT and Security: Hand-in-Hand

Understanding Surface Area

Update processes and policies

Understand Details and Processes

Automate Change to Reduce Error and Risk
Security teams often focus where they have the most autonomy; they get comfortable in this never-ending journey vs. driving toward new destinations.
Engineering vs. Analysis
Take-Aways

Understand where, how, and why you are using cloud. Understand who is responsible.

Providers need to do more.
They could reduce users shooting themselves in the foot, improve default security levels, and better show surface area. (Please encourage them to do more!)

The rest is on you:
(Awareness, Auditing, Adaptation, Automation)!

Oh, yeah, Triple-A:
(Authentication, Authorization, Accounting)!

(and don’t forget hygiene.)
Cloud: Massive Opportunity for Unifying IT & Security

IT
Enablement
Provides Appropriate Tech

Security
Enablement
Provides Appropriate Risk

CONNECTED?
THANK YOU!

Ben Johnson, CTO

ben@obsidiansecurity.com

@chicagoben | @obsidiansec