RSAConference2015

San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking

SESSION ID: CSV-T08

Six Degrees of Kevin Bacon: Securing the Data Supply Chain

Adrian Sanabria

Senior Security Analyst
451 Research / Information Security Practice
@sawaba

Garrett Bekker

Senior Security Analyst
451 Research / Information Security Practice
@gabekker

Securing *my own* environment is hard enough

- Too many tools and products to manage:
  - AV, firewalls, IPS, email gateways, WAF, SIEM
- Constantly evolving threat landscape:
  - APTs, advanced malware, etc.
- Constantly changing tools and terminology:
  - ‘Advanced’, ‘Next-gen’, ‘Analytics’, ‘Intelligence’, ‘Military-grade’, etc.

And it’s getting harder…

- The ‘bad guys’ always seem to be a step ahead
- “The ‘hurrier’ I go, the ‘behinder’ I get

WHY DO COMPANIES KEEP GETTING HACKED?

ONE REASON IS THAT SECURITY ISN'T ALWAYS A PRIORITY FOR DEVELOPERS IN A RUSH TO BRING A PRODUCT TO MARKET. ANOTHER REASON IS THAT HUMANS ARE STUPID.

BY CHRIS GAYOMALI

LOGISTICS & TRANSPORTATION 5/12/2014 @ 9:46PM | 8,368 views

Windows XP Is Extinct -- So Why Are So Many Companies Still On It?

Why Aren’t More Companies Purchasing Cyber Insurance?

DAVID BISSON

NOV 23, 2014 | FEATURED ARTICLES

NEWS ANALYSIS

No, your data isn't secure in the cloud

Now I have to worry about *your* security?

- Third-parties are an common source of ingress:
  - Outsourcers
  - Hosting providers
  - Managed service providers
  - Partners
  - Suppliers
  - Customers

Defining "third party"

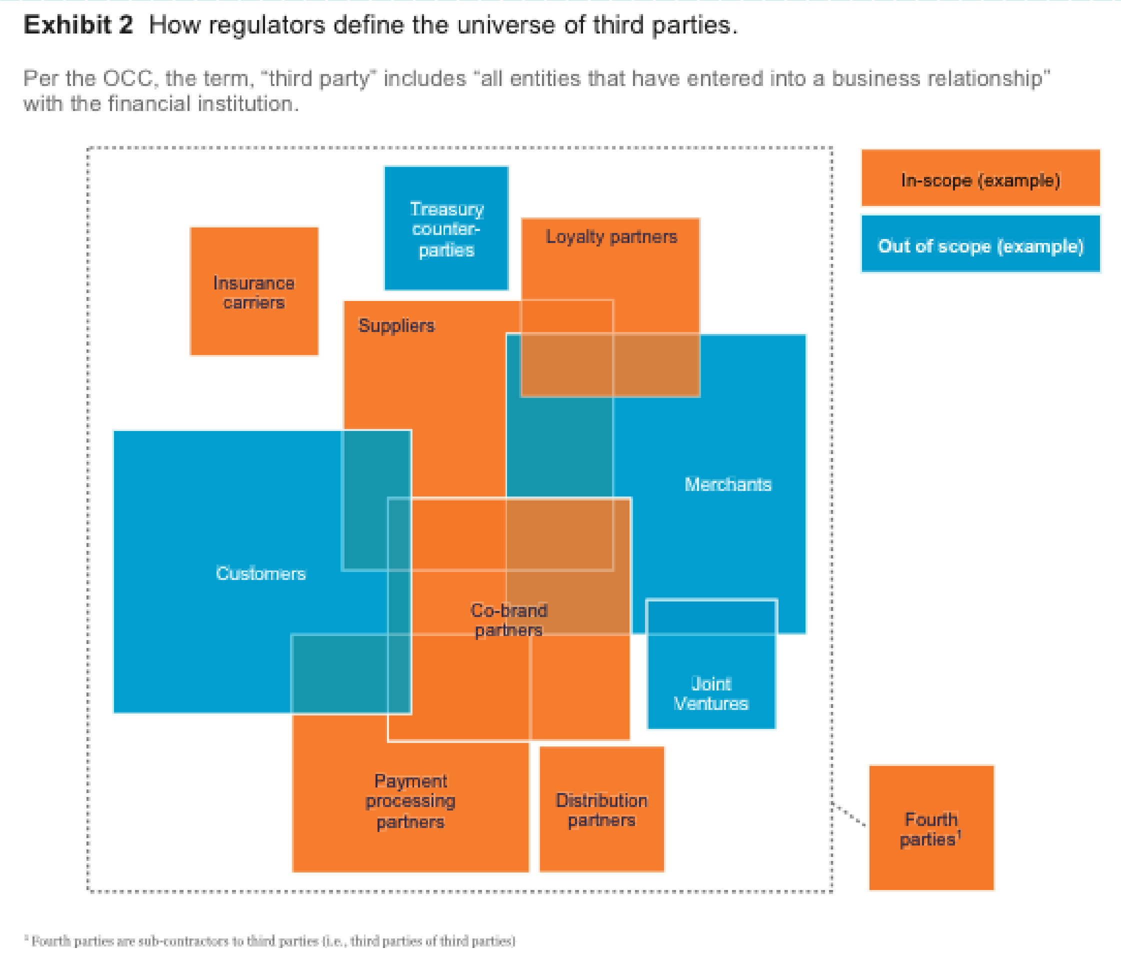


Exhibit 2 How regulators define the universe of third parties.

Per the OCC, the term, "third party" includes "all entities that have entered into a business relationship" with the financial institution.

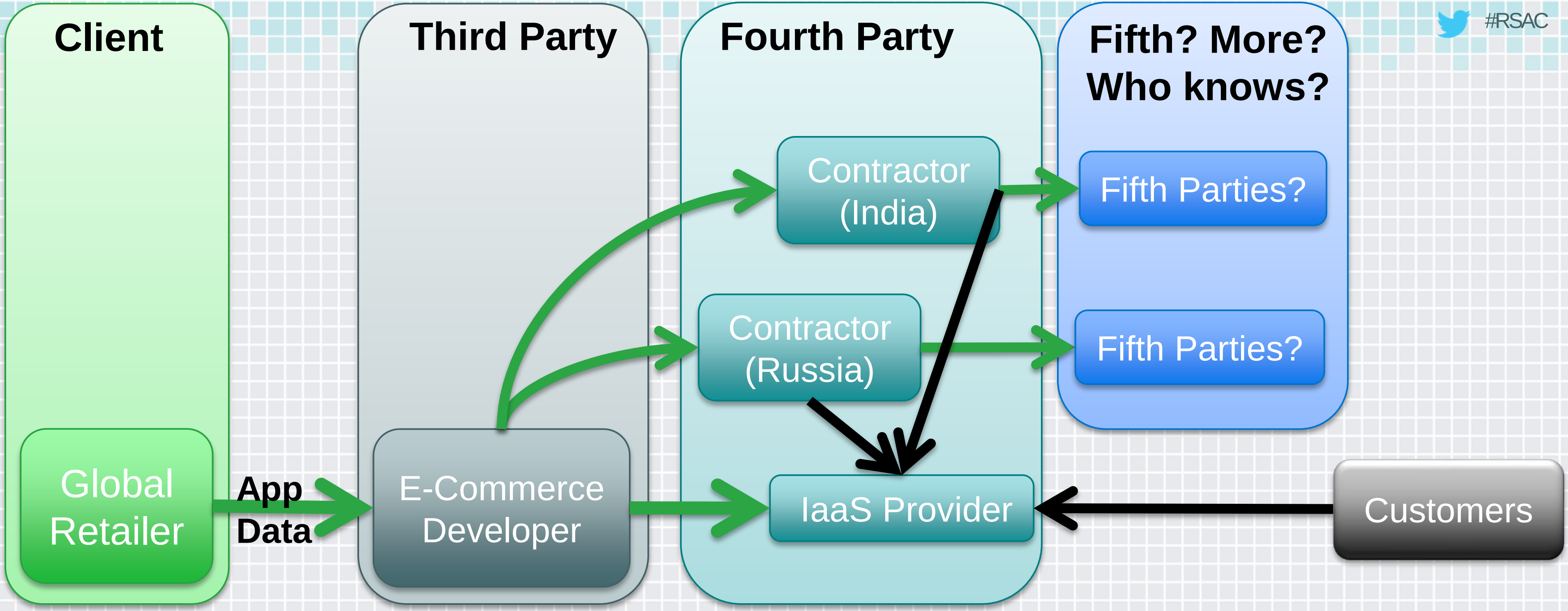
[1] Fourth parties are sub-contractors to third parties (i.e., third parties of third parties)

Slide courtesy McKinsey & Company

Six degrees of Kevin Bacon

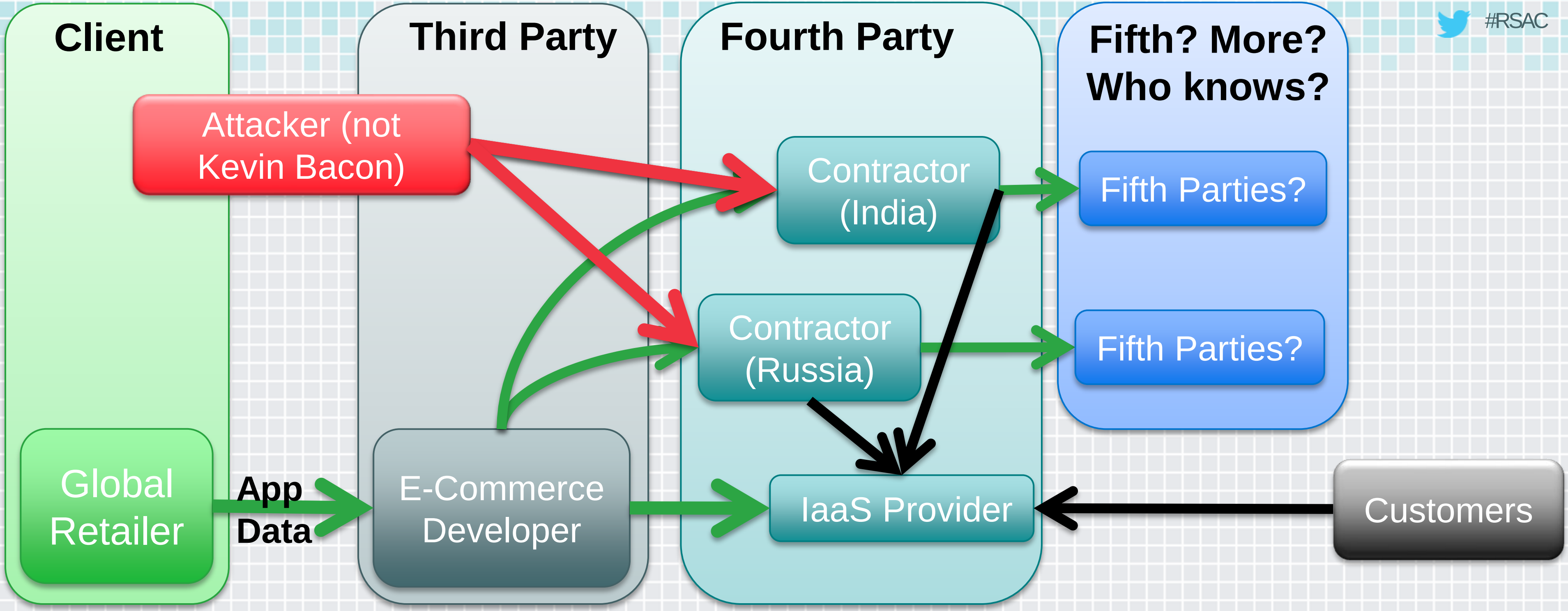
- Target's HVAC vendor was likely only one of thousands, if not tens of thousands of outside vendors providing some type of service to Target or other large enterprises.
- Vendor counts can increase rapidly, and easily run into the thousands.
- For very large firms, external vendor counts can reach 20,000+
- Security incidents related to partners and vendors rose from 20% to 28% in the years just before Target's breach*

*According to PWC's 2010, 2011 and 2012 Global State of Information Security surveys



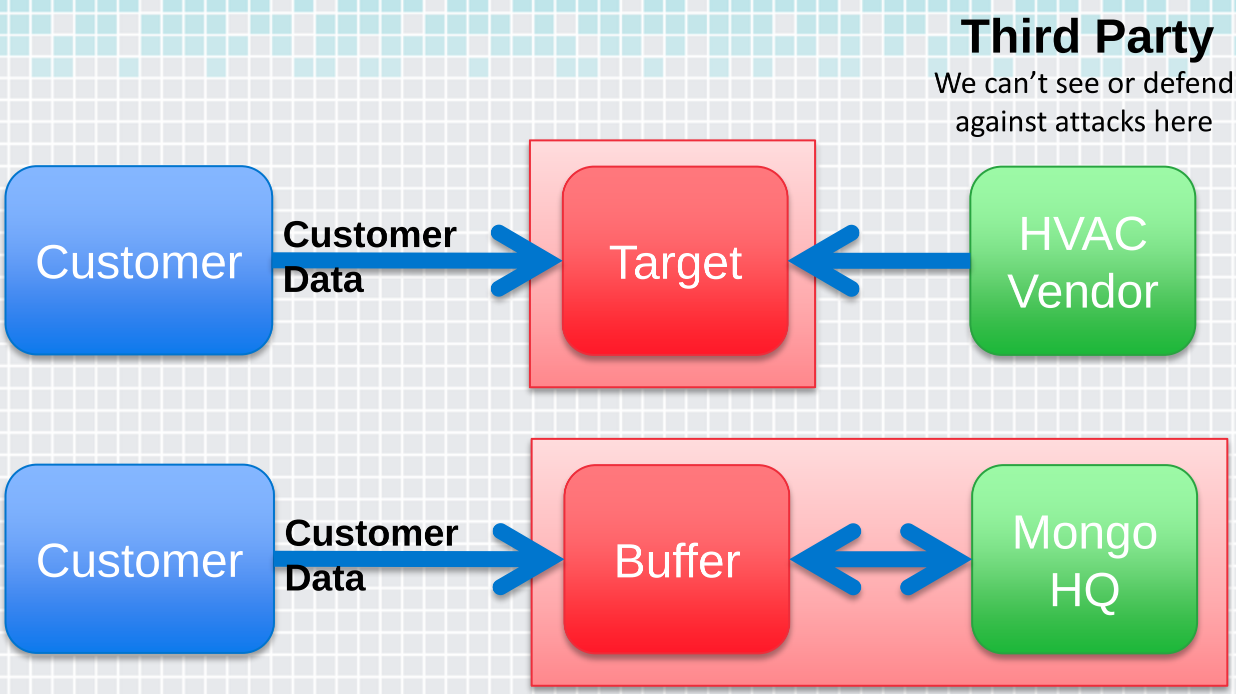
Six degrees of Kevin Bacon

How well do you understand your third party data flow?



Six degrees of Kevin Bacon

How are third parties protecting your data?



Third Party

We can't see or defend against attacks here

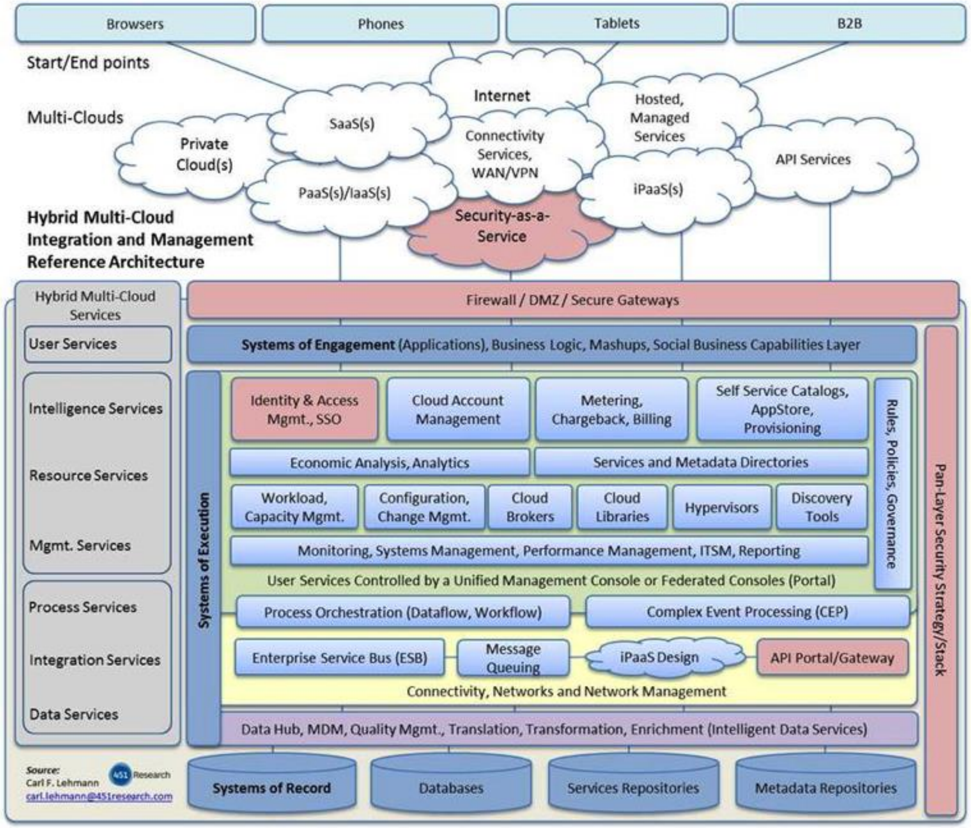
Example 1: Target Breach

Example 2: Buffer/MongoHQ Hack

A few other recent examples

And now cloud?

- IaaS – compute, networking and storage; hardware and servers…
- PaaS – all that, plus software (middleware, OS, etc.)
- SaaS – the full stack
- Private cloud, hybrid multi-cloud…


Browsers
Phones
Tablets
B2B
Start/End points
Multi-Clouds
Private Cloud(s)
SaaS(s)
Internet
Connectivity Services, WAN/VPN
Hosted, Managed Services
API Services
PaaS(s)/IaaS(s)
iPaaS(s)
Security-as-a-Service
Hybrid Multi-Cloud Integration and Management Reference Architecture
Hybrid Multi-Cloud Services
User Services
Intelligence Services
Resource Services
Mgmt. Services
Process Services
Integration Services
Data Services
Firewall / DMZ / Secure Gateways
Systems of Engagement (Applications), Business Logic, Mashups, Social Business Capabilities Layer
Systems of Execution
Identity & Access Mgmt., SSO
Cloud Account Management
Metering, Chargeback, Billing
Self Service Catalogs, AppStore, Provisioning
Rules, Policies, Governance
Economic Analysis, Analytics
Services and Metadata Directories
Workload, Capacity Mgmt.
Configuration, Change Mgmt.
Cloud Brokers
Cloud Libraries
Hypervisors
Discovery Tools
Monitoring, Systems Management, Performance Management, ITSM, Reporting
User Services Controlled by a Unified Management Console or Federated Consoles (Portal)
Process Orchestration (Dataflow, Workflow)
Complex Event Processing (CEP)
Enterprise Service Bus (ESB)
Message Queuing
iPaaS Design
API Portal/Gateway
Connectivity, Networks and Network Management
Data Hub, MDM, Quality Mgmt., Translation, Transformation, Enrichment (Intelligent Data Services)
Pan-Layer Security Strategy/Stack
Systems of Record
Databases
Services Repositories
Metadata Repositories
451 Research

Source:
Carl F. Lehmann
carl.lehmann@451research.com

451 Research

What about the human cloud?

- What about your employees and their 3rd parties (Shadow IT)?
- Are they on your vendor list?
- SHadow-IT-as-a-Service?

Knock-knock. Who’s there? Your auditor.

- Recent regulations targeting third-party risk
  - Office of the Comptroller of the Currency (OCC)
  - PCI Security Standards Council
  - NIST Cybersecurity Framework
  - HIPAA Omnibus
  - CFPB (Consumer Financial Protection Bureau) - Charged with enforcing the new Dodd-Frank regulations for financial firms
- Often accompanied by hefty fines or penalties for noncompliance
- Quarterly or annual review – good luck!

Who spends the most on security? Hmm…

- Financial services (SOX, GLBA, OCC)
- Health Care (HIPAA)
- Government (FISMA)
- Retail and E-Commerce (PCI)
- Reg compliance + budget = $$$
- 451 Research: Third-party risk showed the third highest increase over 2013 in terms of enterprise security pain points

Help is on the way

- There are a variety of tools available for addressing existing as well as emerging vendors
- History suggests innovation will follow the $$, so look for more vendors popping up with new ways to help secure your data supply chain
- More on this near the end of the presentation…

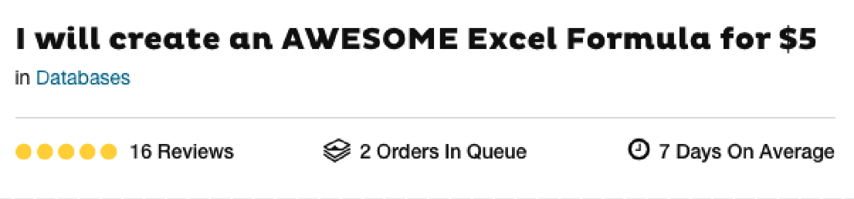
How did we get from 40 third party vendors to 4000?

How did we get here?

Economics

- Someone can always do it cheaper
  - Specialization
  - Services
- How can we *not* take advantage of savings that come with 3rd party services, when competitors will?

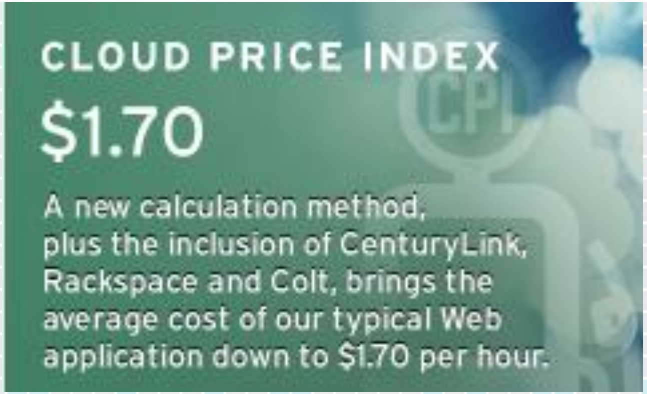
Examples



I will create an AWESOME Excel Formula for $5

in Databases

●●●●● 16 Reviews　2 Orders In Queue　7 Days On Average



CLOUD PRICE INDEX

$1.70

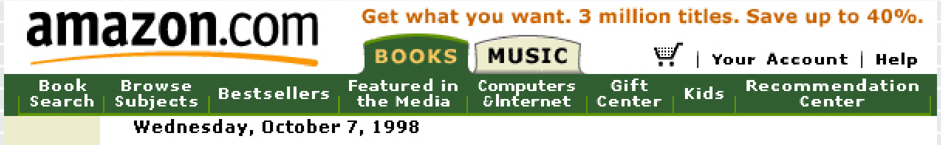
A new calculation method, plus the inclusion of CenturyLink, Rackspace and Colt, brings the average cost of our typical Web application down to $1.70 per hour.

How did we get here?

Efficiency

- If your competitor is saving $50M a year using cloud/SaaS, can you still compete with their margins?
- Once one big business in a vertical has success with new technology, it is a *short* matter of time before the rest follow suit

Examples



amazon.com

Get what you want. 3 million titles. Save up to 40%.

BOOKS | MUSIC | Your Account | Help

Book Search | Browse Subjects | Bestsellers | Featured in the Media | Computers &Internet | Gift Center | Kids | Recommendation Center

Wednesday, October 7, 1998

How did we get here?

Cloud

- Quickly became the most cost efficient way to deliver digital services to businesses and consumers
- Provides a better economic model, efficiency and (if done correctly) more resilience in many use cases

Examples

XBOX

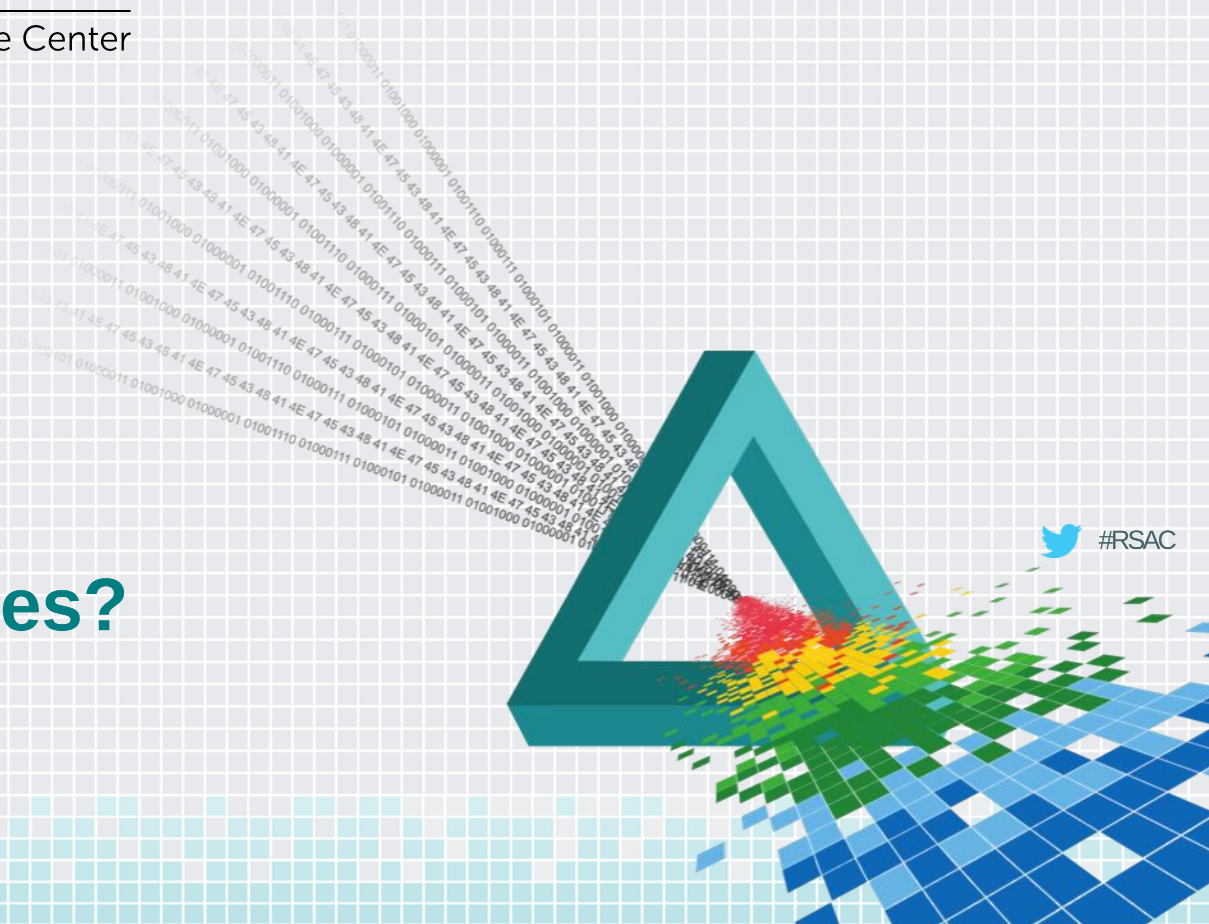
amazon web services™

NETFLIX

Microsoft Azure

RSAConference2015

San Francisco | April 20-24 | Moscone Center



#RSAC

What are the issues?

What are the issues?

1. Data Loss
2. Transparency
3. Due Diligence
4. Legal
5. Terms and Conditions
6. Dangerous assumptions
7. Availability
8. Isolation

What are the issues?

- Data Loss
  - Data: both our greatest challenge and the life blood of the digital industry
  - Rise of a considerable encryption market
- Transparency
  - Visibility into 3rd party operations
  - Ability to perform due diligence on a vendor – would they even answer your questions if you asked?

What are the issues?

- Due Diligence
  - General decline of due diligence
  - Ability to perform due diligence on a vendor
- Legal – run the scenarios!
  - Who is liable?
  - Where do responsibilities lie when incidents occur?
  - Who takes the blame and pays the fines?
  - Applicable data residency/governance requirements?
  - Is encryption a panacea?

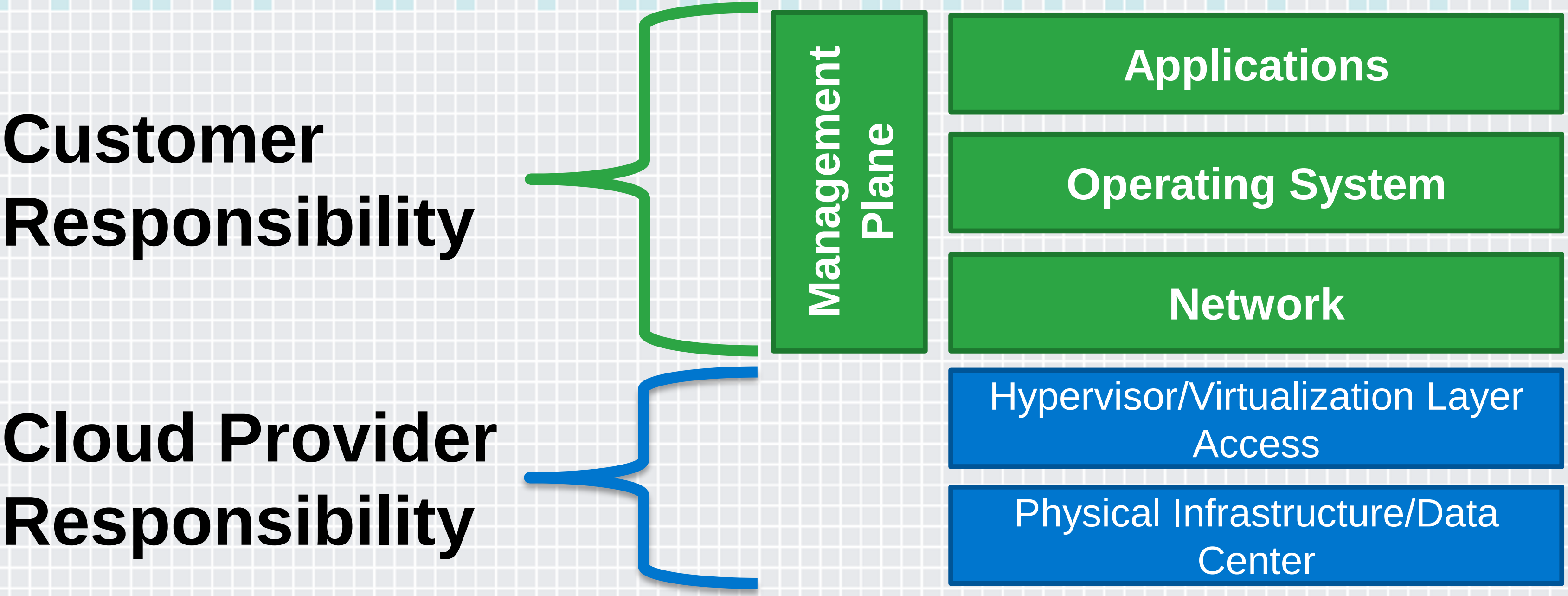
What are the issues?

- Terms and conditions
  - Does your vendor monitor for attacks against your data/assets?
  - If they detected an attack, would they notify you?
  - If they don’t monitor, what are your options?
  - Example: Differences between Amazon AWS and FireHost
- Dangerous Assumptions
  - “Secure because Amazon”
  - AWS: Trusted Advisor is available, but is often not used

Dangerous assumptions: Code Spaces anecdote

“**Code Spaces** have been hosting Subversion and Git Repositories for companies of all sizes for over 5 years, and as a result we have been able to create a wonderful infrastructure to support our business, a large part of this, is having a great hosting partner, at **Code Spaces** we partnered with Amazon”

“Amazon are equally passionate about security, Here is a document detailing some of the security measures Amazon employ.”



Customer Responsibility

Cloud Provider Responsibility

Management Plane

Applications

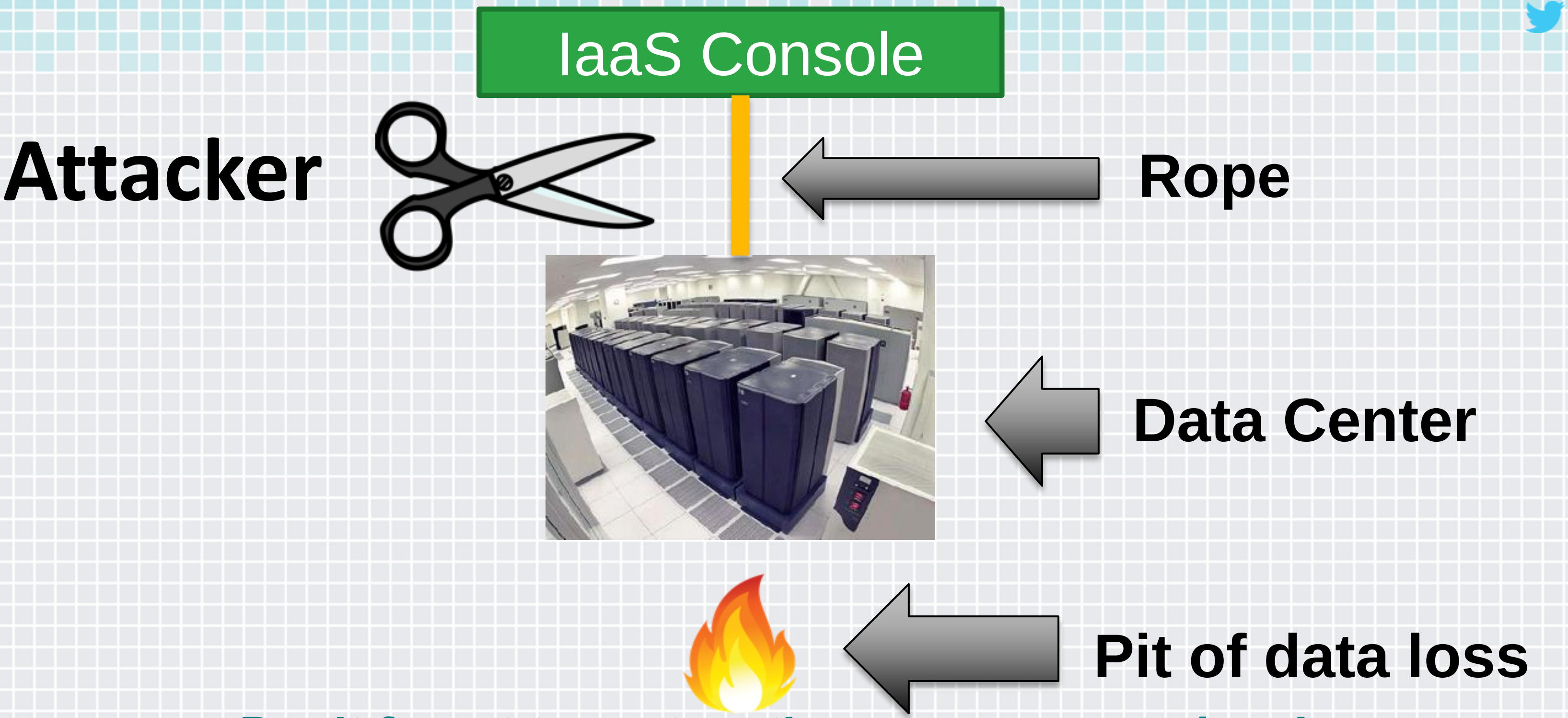
Operating System

Network

Hypervisor/Virtualization Layer Access

Physical Infrastructure/Data Center

Infrastructure as a Service: Provider vs. customer responsibilities



IaaS Console

Attacker

Rope

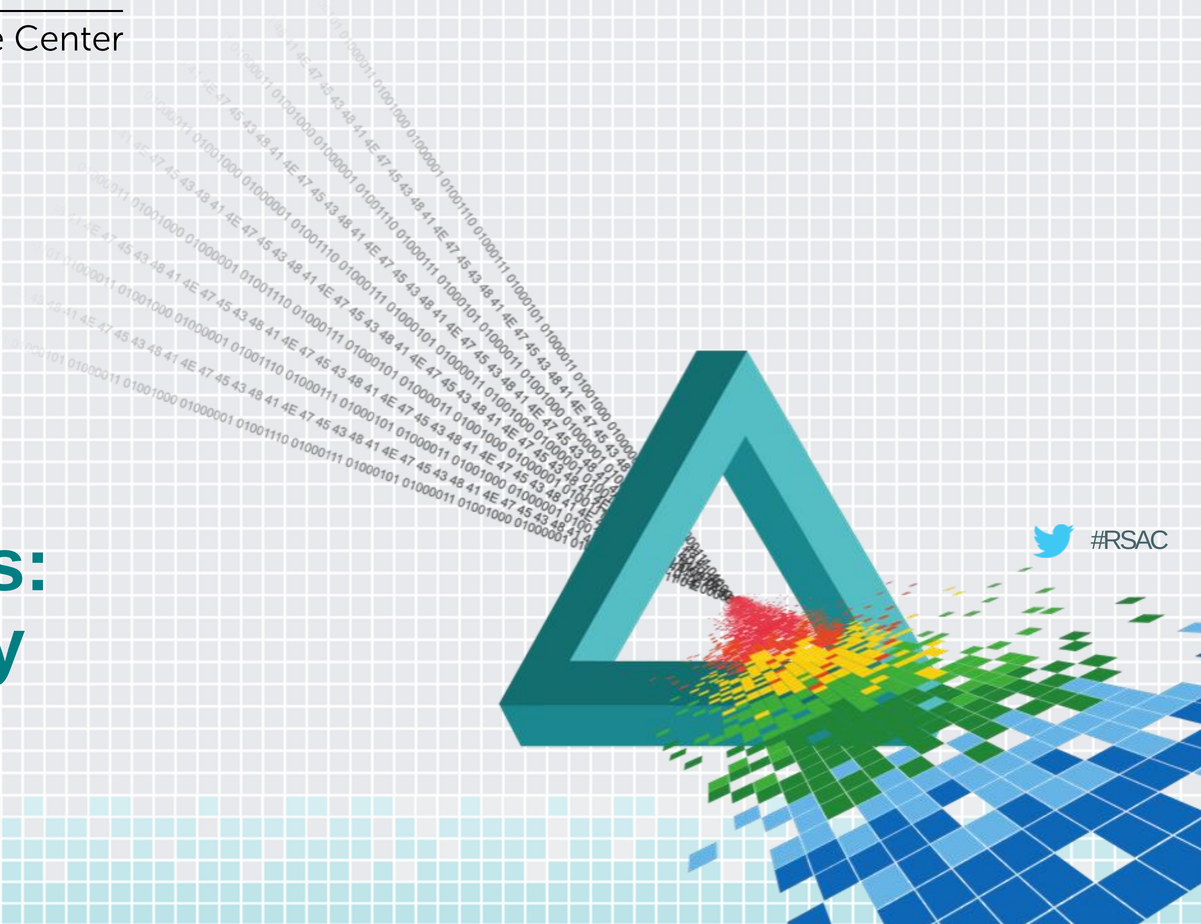
Data Center

Pit of data loss

Don’t forget to protect the management plane!

What are the issues?

- Availability
  - Is your vendor aware of how to do HA properly in the cloud?
  - How robust/scalable is the service?
  - How resilient against spikes in popularity or DDoS (spikes in *unpopularity*)
- Isolation - who has access to my data?
  - Vendor employees?
  - Other customers?
  - 4th Parties (e.g. backup services, database services a la MongoHQ)



Emerging markets: Help is on the way

Creating trust in the supply chain

- Real-time customer-facing risk scores: **Cavirin**, **BitSight**
- Mobile app risk rankings: **MyPermissions**, **Appthority**, **ViaForensics**, **PrivacyGrade**
- SaaS app risk rankings: **CSA**’s STAR, CAC/CASB Market (**SkyHigh**, **Netskope**, **Skyfence**)

Detecting attacks against 3rd party services

- Detecting attacks and preventing issues with the management plane: **Dome9**, **Evident.io**, **Tenable**
- Detecting and preventing attacks against SaaS applications: **Adallom**, **SkyFence**

Increasing awareness

- Grassroots organizations working to increase awareness
- Build It Securely – working with IoT, Belkin, Dropcam
- I Am The Cavalry – bringing attention to medical devices, automotive, home automation, public infrastructure
- Open Crypto Audit Project – TrueCrypt Audit

Streamlining vulnerability discovery and remediation

- Commercial: **Sonatype**, **Vericode**
- Corporate project: **Google Project Zero**
- Bug Bounty Brokers: **BugCrowd**, **HackerOne**, **CrowdCurity**, **Synack**

Risk Management Suites

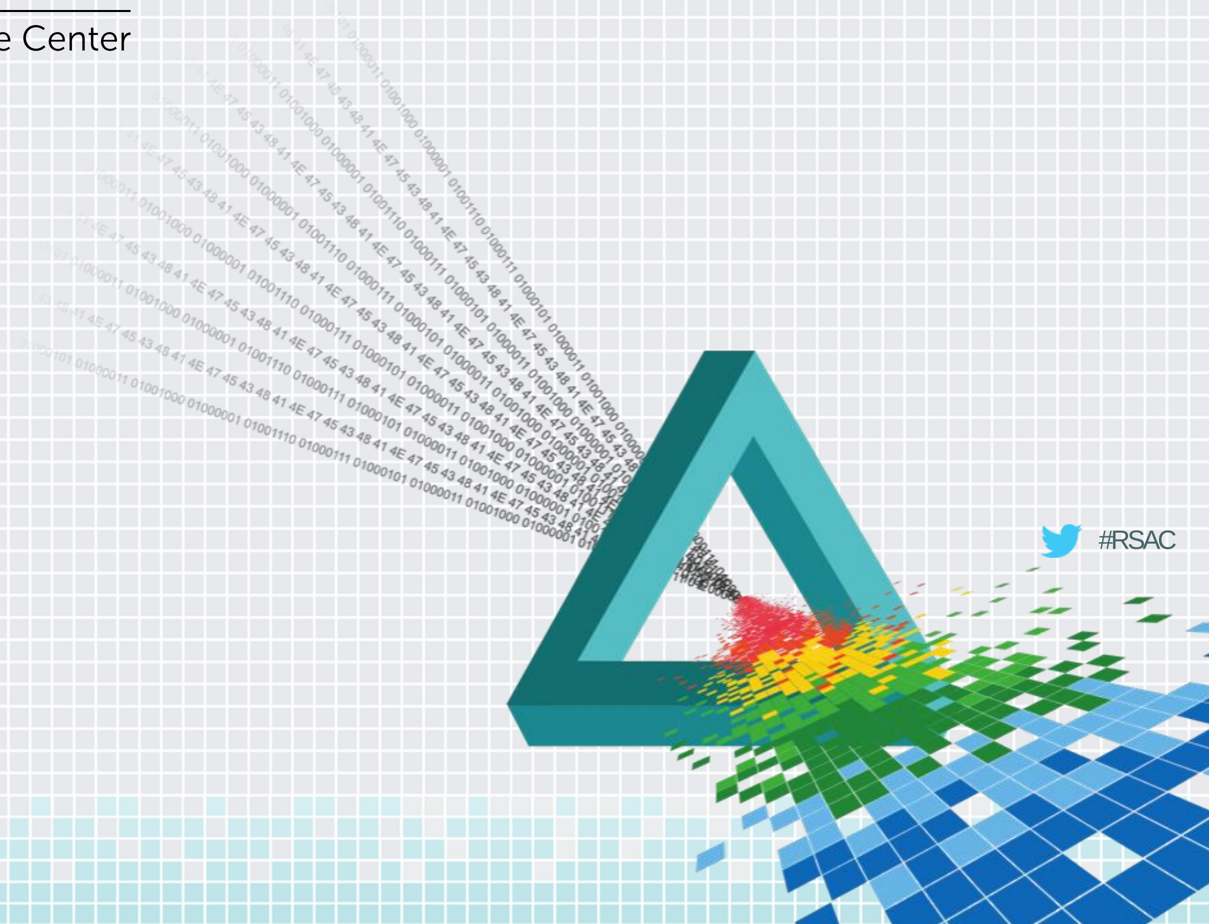
- Third party and/or vendor risk management: **Prevalent, Modulo, TraceSecurity, Aruvio, eGestalt**
- General risk management: **Archer, Allgress, AvePoint, Agiliance**
- Microsoft Excel – *Do you have any mission-critical or 'Tier 0' spreadsheets???*

Encryption

- *If you can't see my data, I can't have a breach, right?*
- FSS Encryption: **Sookasa**, **SafeMonk**, **nCrypted Cloud**, **PKWARE Viivo, Vormetric**
- IaaS Encryption: **Vormetric**, **SafeNet**, **CloudLink**, **PrivateCore** (recently acquired by Facebook)
- SaaS Encryption: **CipherCloud**, **PerspecSys**, **Vaultive**, some CAC/CASB vendors

How can you apply this?

- When you get back to the office
  - Use a NGFW or free/low cost discovery tool from CAC vendors to determine the extent of your digital supply chain
  - Ask procurement for the last few years' invoices, and review for 3rd parties
  - Compare to your existing vendor management list and add any that were missing
- Three months from now
  - Have a fairly comprehensive 3rd party list
  - Plans in place to address risks related to anything on the list that was previously unaccounted for



Thanks!
Questions?