

# **OMG: They're *Still* Inside The Walls And Going To "The Cloud"**

Joe St Sauver, Ph.D. (stsauver@fsi.io)  
Farsight Security, Inc.

Resort at the Mountain, Welches OR  
ACPENW 2015, Thursday May 7<sup>th</sup>, 2015  
12:30-1:45 PM, Altitude Room

<https://www.stsauver.com/joe/acpenw-cloud/>

# Preface: My Odd Slide Style

- If you're not familiar with my slide style, let me get that "out of the way" right up front: I produce **detailed slides**. This style drives some people **crazy**, so I like to explain why I use it.
- I've tried the more-typical 3-4 bullets/slide with ~15 slides for an hour long talk model, but I find myself getting **sidetracked, rambling/running over**, or I end up **missing/skipping stuff**.
- I also deal with **complex issues**, and I **HATE** to be misquoted.
- My slide style prevents a lot of those problems, and means that **you don't need to try to take notes**.
- That said, I'm **not going to read my slides word-for-word for you**. You don't need to try to do so, either, although they are a sort of "closed captioning" if you're deaf or hard-of-hearing.
- I also write detailed slides to help people looking at them after the fact, and for indexing by web search engines.

# **1. Introduction**

# Context

- It's a pleasure to be here with you today at the Resort at the Mountain in Welches, Oregon. Thank you for inviting me to talk!
- Back in December 2013, I did a talk for ACPE's Ashland, Oregon meeting, and I followed that up with a talk at ACPE's Spokane, Washington meeting in March 2014.
- The title for my talks in both cases was "OMG: They're Inside the Walls," a *very* creative title that was chosen for me by ACPE's leadership, thank you ladies and gentlemen.
- During *this* week's meetings, they've asked me to address two topics that they hope might be of interest to you:
  - This talk, "OMG: They're Still Inside The Walls And Going To The Cloud," obviously builds on my earlier talks, and
  - Tomorrow, I have a multifactor authentication talk whose title somehow managed to avoid including the prefix "OMG" :-)

# My Background With Respect to Cloud Security

- I first began thinking about cloud security in the fall of 2011, in conjunction with the work that I was doing then for Internet2 as their Nationwide Security Programs Manager (work I performed under contract through the University of Oregon).
- As part of that work, I provided recommendations with respect to how Internet2 and the U.S. higher education community might approach cloud security assessment.
- During the next following couple of years, in support of Internet2's NET+ cloud services program, I had the opportunity to work closely with multiple cloud service providers as they progressed through the "service validation" process to get approved to become part of the NET+ program.

## UO → Farsight Security, Inc.

- While I'd been at UO for 28 years, in November 2014 it was my honor to accept a new position as a Distributed System Scientist, working for Paul Vixie's new company, **Farsight Security, Inc.** (see <https://www.farsightsecurity.com/> )
- FSI is a data-driven cyber security company with deep expertise in DNS-related areas. For more about what FSI does, please check out our website, catch me during the meeting, or drop me a note.
- **Note: If you'd like to help fight cyber crime and abuse, AND you run your site's recursive resolvers (name servers), we should talk about opportunities for you to potentially contribute anonymized DNS data for FSI's passive DNS archive, DNSDB.**
- I'd also like to thank Farsight for allowing me the time to prepare my talks for ACPE and to be with you this week.
- That said, all opinions expressed are solely my own.

# A Few Additional Disclaimers About Today's Talk

- There's a LOT of hype associated with cloud computing. I'm sorry about that, but there's not much I can do about **THAT**.
- Cloud computing is a huge topic. It encompasses diverse models and technologies, even though users and the trade press tend to lump them all together under a single overarching name. Fully covering all cloud security issues in 75 minutes is impossible.
- For that matter, please note that we're still discovering many of the security issues which will challenge/change cloud computing. Why? Cloud computing is very much a work-in-progress. It would be nice if we could just sit back and wait for things to jell up so we could fully understand and address the security issues associated with the cloud, but we can't. Cloud computing has incredible momentum, and is a production reality today. You need to understand it, and figure out how you'll cope with it, now.

# I Believe In Active Learning

- I want to explicitly encourage you to **ask questions** as we go along.
- Feel free to **question/challenge** the things I may say, particularly if you've been working extensively with cloud-based services.
- I truly want this to be a **conversation**, not just me yammering on at you for 75 minutes.

# A Quick "Whip Around The Room" (If We Can)

- I'm not sure how big our room will be today, or how many attendees will be in this session, but if the audience is of manageable size, let's do a quick whip around the room to hear a little from YOU.
- **As we go around, please share:**
  - 1. The ONE most important way your school currently uses the cloud, OR**
  - 2. Your SINGLE biggest cloud-related security concern, OR**
  - 3. The ONE thing you really wish you could change about the cloud (but currently can't)**

**2. Why Talk About "The Cloud?"**  
**Why Talk About Cloud Security?**  
**Why Talk About Cloud Security HERE?**

# It Seems As If EVERYONE's Now At Least Considering the Cloud

- "94% of Enterprises are at least discussing cloud or cloud services"

"Avoiding the Hidden Costs of the Cloud," PDF page 4,  
<http://www.symantec.com/content/en/us/about/media/pdfs/b-state-of-cloud-global-results-2013.en-us.pdf>

[There are a MILLION stats/surveys/reports about all things cloud, as you'll quickly see]

# What's Driving That Interest in Cloud Computing?

- Thought leaders: Amazon, Google, Microsoft and many other Internet thought leaders have all aligned behind "the cloud"
- The economy: Because cloud computing should theoretically help sites avoid major new capital expenditures (capex) while also controlling some ongoing operational expenses (opex), cloud computing is potentially a lifesaver for financially strapped businesses, including our elementary and secondary schools
- Mobile devices: Smart phones, tablets and Chromebooks typically have limited on-device storage and processing power may also be limited due to intentional use of energy-efficient processors. The cloud is a perfect compliment to those mobile devices, offering virtually unlimited storage and infinite processing power.

# Ultimately, Sites Either Use Cloud Services, Or They Don't. What Drives That Decision?

- Is it a substantive/technical matter of the features/functionality available from cloud provider's products or services?
- Is it a business matter, perhaps how much the product or service cost, or the terms of the agreements offered?
- Or is the problem one with infrastructure issues, maybe?  
For example, perhaps a potential service doesn't integrate well with your other current identity management systems, or requires network capacity you don't currently have?
- **Many times, security (or privacy, or compliance) may be the problem...**

# Security and Cloud-Based Services

- Security (along with pricing economics) may have a material impact on how cloud-based services get adopted and used.
- For cloud-based services to be embraced, they need to make financial sense, *and* they need to be adequately secure.
- We had an early "heads up" on this: during early higher education meetings where some cloud-based services were being announced, a member of the audience stood up and asked, "So what about security?"
- That question continues to come up today, anywhere you look.

# Security As A Potential Barrier To Adoption

- *During a keynote speech to the Brookings Institution policy forum, "Cloud Computing for Business and Society," [Microsoft General Counsel Brad] Smith also highlighted data from a survey commissioned by Microsoft measuring attitudes on cloud computing among business leaders and the general population.*

*The survey found that while 58 percent of the general population and 86 percent of senior business leaders are excited about the potential of cloud computing, **more than 90 percent of these same people are concerned about the security, access and privacy of their own data in the cloud.***

<http://www.microsoft.com/presspass/press/2010/jan10/1-20BrookingsPR.mspx>

## Another Study

- "PC Connection, in partnership with Cisco, recently released the results of its 2013 Outlook on Technology: Cloud Computing Survey. The survey, the results of which are available at InfoWorld, queried over 500 organizations of all sizes to ascertain what they are seeking in a cloud solution, what concerns they have about the technology and what obstacles they see between their organization and further cloud adoption. [...] **Perhaps the most surprising information gleaned from the cloud computing usage survey is that security is the top obstacle to cloud adoption, according to 65 percent of the survey responses.** Integration was the next biggest obstacle, but it was listed in just 34 percent of responses."

"Cloud Computing Usage: Security Still Considered a Barrier,"

<http://midsizeinsider.com/en-us/article/cloud-computing-usage-security-still-co>

# Security: Still A Top Concern

- "Many IT decision makers are hesitating on making the switch to cloud as far as mission critical apps are concerned because of the unknown variables posed by cloud security risks. A KPMG report mentions that **cloud security is still a top concern** as IT executives look for ways to reduce costs. The report mentions that **45% of respondents said data loss and data privacy were their top hesitations in regards to cloud implementations.**"

## **The Top Two Cloud Computing Security Concerns of 2015**

<http://www.cloudwedge.com/top-two-cloud-computing-security-concerns-2015/>

# Many Proceed To Move To The Cloud, Even If There Are or May Be "Security Issues"...

- 'A new report by the agency's Office of the Inspector General says that NASA needs to work on strengthening its information technology security practices. [...] **According to the report, NASA had five contracts for cloud hosting and none of these "came close" to meeting data security requirements.** [...] Over the past year, NASA spent less than 1 percent of its \$1.5 billion annual IT budget on cloud computing. However, moving forward, the agency plans to dedicate much more to cloud security and initiatives. **Within the next five years, NASA is planning to have up to 75 percent of its new IT programs begin in the cloud and 100 percent of the agency's public data stored in cloud.'**
- "NASA Falls Short on Its Cloud Computing Security," [http://news.cnet.com/8301-1009\\_3-57596053-83/nasa-falls-short-on-its-cloud-computing-security/](http://news.cnet.com/8301-1009_3-57596053-83/nasa-falls-short-on-its-cloud-computing-security/)

# What Gets Moved Into The Cloud May Not Stay There. Why? "Security Concerns"...

- "IDG Enterprise recently published Cloud Computing: Key Trends and Future Effects Report, showing how enterprises continue to struggle with security, integration and governance [...] IDG's methodology is based on interviews with 1,358 respondents [...] **42% of cloud-based projects are eventually brought back in-house, with security concerns (65%),** technical/oversight problems (64%), and the need for standardization (on one platform) (48%) being the top three reasons why. [...] **For IT, concerns regarding security (66%),** integration stability and reliability (47%) and ability of cloud computing solutions to meet enterprise/industry standards (35%) challenge adoption.
- <http://www.forbes.com/sites/louiscolombus/2013/08/13/idg-cloud-computing-survey-security-integration-challenge-growth/>

# The Cloud and ACPE

- All of the preceding is well and good, but why talk about cloud security here? How is the cloud and cloud security relevant to ACPE and its membership?
- I know this audience makes heavy use of mobile devices, including smart phones and tablets and Chromebooks, all devices which tend to rely heavily on cloud services
- Many of you are already using the cloud for school-wide services, and other are thinking about it (or may be being pushed to do so)
- Just like everyone else, you need to decide what you're going to do, cloud-strategy-wise.

### **3. What Is "The Cloud"?**

# Cloud Computing Is Many Different Things to Many Different People

- All of the following have been mentioned from time to time as examples of "cloud computing:"
  - Amazon Web Services (including the Elastic Compute Cloud (EC2), Amazon Simple Storage Service (S3), etc.)
  - Google's App Engine
  - Microsoft's Azure Platform
  - outsourced campus email services (to Gmail or Office365), or outsourced spam filtering
  - use of virtualization (e.g., VMware) to host departmental systems either on local servers, or on outsourced VPS
- In reality, some of those activities are not (strictly speaking) what's usually defined as "cloud computing,"

# Some Generally Accepted Characteristics

- Most people would agree that **true** cloud computing...
  - usually has low (if not zero) up front capital costs
  - largely eliminates operational responsibilities (e.g., if a disk fails or a switch loses connectivity, you don't need to fix it)
  - for the most part, cloud computing eliminates knowledge of WHERE one's computational work is being done; your job is being run "somewhere" "out there"
  - offers substantial elasticity and scalability: if you initially need one CPU, that's fine, but if you suddenly need 999 more, you can get them, too (and with very little delay!) If/when demand drops, you can scale your usage back, too
  - cloud computing leverages economies of scale (running mega data centers with tens of thousands of computers is far less expensive (per computer) than running a small machine room with just a modest cluster of systems)

# Three Types of Cloud Services

- Infrastructure (compute cycles, storage, database, etc.) available on demand from a pre-provisioned pool (example: Amazon AWS, see <http://aws.amazon.com/> ), normally referred to IAAS ("infrastructure as a service"). Often HUGE outfits.
- Apps that run somewhere "out there" on infrastructure you don't run or rent (examples: Adobe Creative Cloud, Google Apps for Education, or Salesforce). Normally called SAAS ("software as a service"). May be a small entrepreneurial operation.
- And then, largely for developers, there's "Platform as a service" (PAAS) outfits; one example of this would be RedHat's OpenShift, see <https://www.openshift.com/> , running somewhere "in between IAAS and SAAS." Think of this as being a way to outsource the parts of an app that you might not want to have to handle yourself (such as mail delivery, authentication, etc.)

# I'm Renting a Server From A Hosting Company. Am I Using "The Cloud?"

- No. Just outsourcing the hosting of a server isn't enough to make you a user of "the cloud."
- Why? Most notably, your capacity isn't "highly elastic." If you get "Slashdotted" and temporarily need a lot more capacity, you can't quickly get it. You may need to enter into a year long contract, and if you no longer need the contracted server after a few weeks, well, that's just too bad.
- You may also still need to administer the system from the "bare iron" on up, which again is inconsistent with "cloud" concept. In the cloud, you don't (or shouldn't) need to worry about actual infrastructure devices.
- You may even know where "your" server is located (example: server 26, rack 209, datacenter foo, Dallas, TX)

# I'm An End User Using Gmail. Am I Using "The Cloud"?

- Yes. Gmail (and associated applications such as Google Apps for Education) are in many respects a perfect example of "software as a service."
- Another very common example of a cloud-based SAAS application is a file sharing service, such as Box or DropBox.
- Peer-to-peer file sharing services, on the other hand, such as BitTorrent, wouldn't typically be considered to be "in the cloud."

# I'm Backing Up Stuff From My Smartphone Online Somewhere. Am **\*I\*** Using the Cloud?

- Yes. Backups of content from mobile devices (such as smart phones and tablets) would be a prime example of how users may be engaging with the cloud.
- In fact, mobile devices largely REQUIRE cloud-based backups because on-device storage may be limited, and opportunities for external expansion may be limited.
- Backups are particularly important for mobile devices given that mobile devices disproportionately often end up lost, stolen, or broken...

# My School Is Running a "Private Cloud" – Surely I'm Using "The Cloud," Aren't I?

- From my POV, it depends. Some people have taken to calling a local compute cluster a "private cloud" because "private cloud" sounds cool/trendy.
- To *really* qualify as a private cloud service, I'd be looking for:
  - A substantial pool of resources shared among many users with plenty of headroom for handling peaking loads
  - An interface that's compatible with things like the Amazon EC2 public cloud (for examples: Ubuntu's OpenStack)



# Ubuntu private cloud is compatible with the Amazon EC2 public cloud

- Immediacy and elasticity behind the firewall
- Migrate between public and private clouds easily
- Burst to public clouds when needed

## Why Ubuntu?

### Private Cloud » Ubuntu Enterprise Cloud

Private clouds offer immediacy and elasticity in your own IT infrastructure. Using Ubuntu

### Public Cloud » Ubuntu on Amazon EC2

Amazon's Elastic Computing (EC2) cloud allows you to build on-demand virtual systems with

**4. Is "Cloud" Security Different Than  
"Regular" IT Security?**

# In Many Ways, "Cloud Computing Security" Is The SAME AS Than "Regular Security"

- For example, many applications interface with end users via the web. **All the normal OWASP web security vulnerabilities** -- things like SQL injection, cross site scripting, cross site request forgeries, etc. -- are just as relevant to applications running in the cloud as they are to applications running on conventional servers locally or at a hosted datacenter.
- Similarly, consider **physical security**. A data center full of servers supporting cloud computing is internally and externally indistinguishable from a data center full of "regular" servers. In each case, it will be important for the data center to be physically secure against unauthorized access or potential natural disasters, but there are no special new physical security requirements which suddenly appear simply because one of those facilities is supporting cloud computing

# Physical Security at an Oregon Cloud Provider



# In Other Ways, The Cloud IS VERY Different...

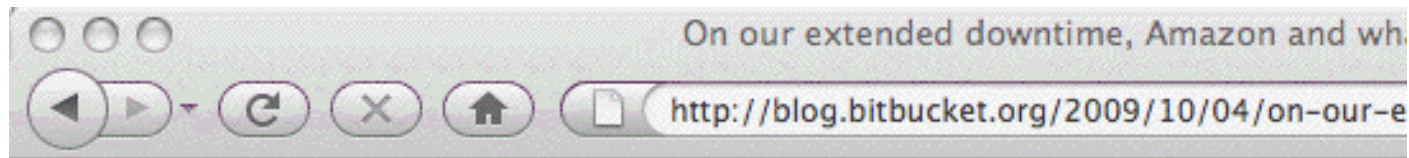
- In the cloud, customers can't directly assess the security of the facilities (they wouldn't let me in for a tour!), or the hardware-level OS install, or the configuration of the routers and firewalls and intrusion detection systems; we need to trust the expertise of the cloud provider's team, instead
- Security capex/opex is fixed and bundled in as part of the service; my choice is effectively "do it" or "don't do it" (or nag/pick at the provider in an effort to potentially get them to make changes). Most services do not offers tiers of security.
- Will I get to see the cloud provider's audit reports? No. (Well, they might share selected general bits and pieces with me)

## **5. Cloud Risks: Availability**

# The "A" in The Security "C-I-A" Objectives

- Computer- and network-security is fundamentally about three objectives:
  - confidentiality (C)
  - integrity (I), and
  - availability (A).
- **Availability is the area where cloud based infrastructure appears to have had its largest (or at least most highly publicized) challenges to date.**
- For example, consider some of the cloud-related outages which have been widely reported...

# Bitbucket, DDoS'd Off The Air



## On our extended downtime, Amazon and what's coming

As many of you are well aware, we've been experiencing some serious downtime the past couple of days. Starting Friday evening, our network storage became virtually unavailable to us, and the site crawled to a halt.

We're hosting everything on Amazon EC2, aka. "the cloud", and we're also using their EBS service for storage of everything from our database, logfiles, and user data (repositories.)

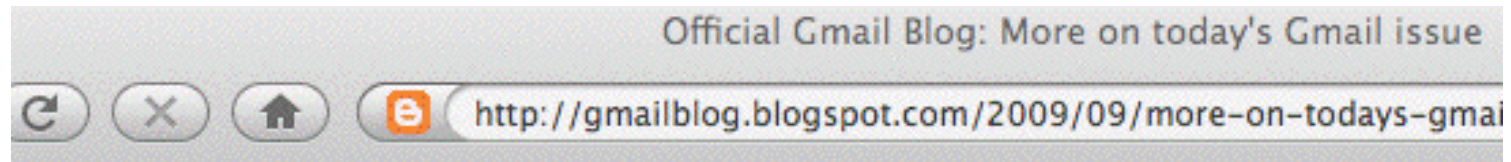
Amazon EBS is a persistent storage solution for EC2, where you get high-speed (and free) connectivity from your instances, while it's also replicated. That gives you a lot for free, since you don't have to worry about hardware failure, and you can create periodic "snapshots" of your volumes easily.

While we were down, it was unknown to us what exactly the problem was, but it was almost certainly a problem with the EBS store. We've been working closely with Amazon the past 24 hours resolving the issue, and this post will outline what exactly went wrong, and what was done to remedy the problem.

### Symptoms

What we were seeing on the server was high load, even after turning off anything that took up CPU. Load is a result of stuff "waiting to happen", and after reviewing iostat, it became apparent that the "iowait" was very high while the "tps" (transactions per second) was very low for our

# Maintenance Induced Cascading Failures



## More on today's Gmail issue

Tuesday, September 01, 2009 6:59 PM

Posted by Ben Treynor, VP Engineering and Site Reliability Czar

Gmail's web interface had a widespread outage earlier today, lasting about 100 minutes. We know how many people rely on Gmail for personal and professional communications, and we take it very seriously when there's a problem with the service. Thus, right up front, I'd like to apologize to all of you — today's outage was a Big Deal, and we're treating it as such. We've already thoroughly investigated what happened, and we're currently compiling a list of things we intend to fix or improve as a result of the investigation.

Here's what happened: This morning (Pacific Time) we took a small fraction of Gmail's servers offline to perform routine upgrades. This isn't in itself a problem — we do this all the time, and Gmail's web interface runs in many locations and just sends traffic to other locations when one is offline.

However, as we now know, we had slightly underestimated the load which some recent changes (ironically, some designed to improve service availability) placed on the request routers — servers which direct web queries to the appropriate Gmail server for response. At about 12:30 pm Pacific a few of the request routers became overloaded and in effect told the rest of the system "stop sending us traffic, we're too slow!". This transferred the load onto the remaining request routers, causing a few more of them to also become overloaded, and within minutes nearly all of the request routers were overloaded. As a result, people couldn't access Gmail via the web interface because their requests couldn't be routed to a Gmail server. IMAP/POP access and mail processing continued to work normally because these requests don't use the same routers.

# It's Not Just The Network: Storage Is Key, Too

## T-Mobile: we probably lost all your Sidekick data

By Chris Ziegler  posted Oct 10th 2009 3:45PM

BREAKING

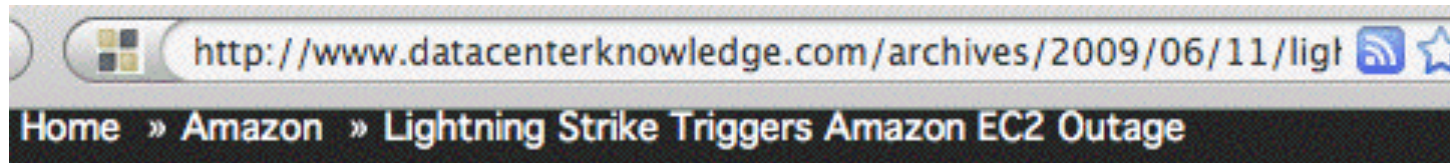


Well, this is shaping up to be one of the biggest disasters in the history of cloud computing, and certainly the largest blow to Danger and the Sidekick platform: T-Mobile's now reporting that personal data stored on Sidekicks has "almost certainly has been lost as a result of a **server failure** at Microsoft/Danger." They're still looking for a way to recover it, but they're not giving users a lot of hope -- meanwhile, servers

See <http://www.engadget.com/2009/10/10/t-mobile-we-probably-lost-all-your-sidekick-data/>

However, see also: Microsoft Confirms Data Recovery for Sidekick Users  
<http://www.microsoft.com/Presspass/press/2009/oct09/10-15sidekick.mspx>

# And Let's Not Forget About Power Issues



## Lightning Strike Triggers Amazon EC2 Outage

June 11th, 2009 : Rich Miller

Some customers of Amazon's EC2 cloud computing service were offline for more than four hours Wednesday night after an electrical storm damaged power equipment at one of the company's data centers. The problems began at about 6:30 pm Pacific time, and most affected customers were back online by 11 p.m., according to Amazon's [status dashboard](#). The company said the outage was limited to customers in one of Amazon's four availability zones in the U.S.

"A lightning storm caused damage to a single Power Distribution Unit (PDU) in a single Availability Zone, the company reported. "While most instances were unaffected, a set of racks does not currently have power, so the instances on those racks are down. We have technicians on site, and we are working to replace the affected PDU."

EC2 previously experienced extended outages in [February 2008](#) and [October 2007](#).

# Mitigating Cloud Computing Availability Issues

- Risk analysts will tell you that when you confront a risk, you can try to eliminate the risk, you can mitigate/minimize the impact of the risk, or you can simply accept the risk.
- If you truly require non-stop availability, you can try using multiple cloud providers, or you could use public and private cloud facilities to improve redundancy.
- Some cloud computing services also offer service divided into multiple "regions." By deploying infrastructure in multiple regions, isolation from "single-region-only" events (such as the power outage mentioned previously) can be obtained.
- Sometimes, though, it may simply make financial sense for you to just accept the risk of a rare and brief outage. (Remember, 99.99 availability==> 52+ minutes downtime/yr)

# How Do We Know That We're Appropriately "Managing" Risk (Assuming We Are)

- *Professional Expertise* ("I'm not *detecting* us getting hit, and I'm not *hearing reports* that we've been hit, and I've managed all the security risks I've been able to, so...")
- *Historical Reputation*: we haven't been hacked previously, so we must be okay ("prior performance doesn't guarantee future...")
- *Expenditures*: we're spending everything we've been able to get for securing things (but what if you've got a security person who's bad at playing "budget war games"?)
- *Audit*: the auditor doesn't return any findings (but what if we've got a crumby auditor who's asleep at the switch?)
- *Common Sense Test*: if something bad happens, will what we're currently doing pass the public "sniff test"? That is, are we doing what a reasonable person would normally do?
- **Remember**: not everything is "mission critical."

## Instagram, Vine stop working at same time; people use Twitter to freak out

August 25, 2013 at 1:28 pm by [Taylor Soper](#) 7 Comments

Share this:



Like

126



164



Share

4



+1

68

**New post:** [AWS server issues take down Instagram, Airbnb, Flipboard](#)

**Original post:**

If you want to Instagram another [selfie](#) or post a [hilarious Vine video](#), it looks like you'll need to wait as both Instagram and Vine are currently out-of-order.

It appears both social media hubs went down sometime around 1 p.m. PST. Both [Vine.co](#) and [Instagram.com](#) are down, as confirmed by Down For Everyone Or Just Me.

Facebook (which owns Instagram) still works, and Twitter (which owns Vine) is also working. Instagram has more than [100 million users](#), while [Vine has 40 million](#).

I was actually trying to post a photo to Instagram a few minutes ago and got a little frustrated when it kept stalling, even after restarting my phone.

But there seem to be [some people on Twitter](#) — which is still up and running just fine — quite a bit more angry than me (see below).

[Amazon.com went down for 40 minutes last week](#), presumably costing the Seattle online giant millions in sales. Two days before that, [all of Google's services went down](#) for five minutes. The New York Times also [went down for two hours](#) two weeks ago, and [GitHub also experienced outages](#).



# Digging Down On A Specific Technical Availability Risk: Network Connectivity

- In the (public) cloud computing model, users are local but critical resources are hosted elsewhere. Network connectivity is the glue that puts them together.
- Connectivity thus is of paramount importance: if the network is "down," you won't be able to reach "the public cloud." Some things to think about:
  - What might cause a network outage? Fiber cut? DDoS? Other?
  - Is the outage local, remote, or somewhere in between?
  - How much network is "between" me and my cloud provider?
  - How long might an outage last? Minutes? Hours? Days?
  - What would we do while we're down?
  - Do I need more network redundancy?
  - **If I need to buy more redundancy, what will that cost?**

# Death of 10,000 Dropped Packets: Network Quality

- Besides just being available, you should also think about the quality of your network connections. Will they be good enough to support the cloud app you're thinking of fielding? Voice and video can be surprisingly demanding (try <https://meet.jit.si/> with ten collaborators for a terrific stress test):
- Do I have enough aggregate bandwidth?
- What sort of throughput can a single user achieve?
- Are there latency issues?
- Are there jitter issues?
- Am I going to be NAT'd, or will I have publicly addressable IPs? Are those addresses "clean," or do those addresses have reputation issues from previous users?
- Can I get IPv6 connectivity if I want or need it? **(Remember, ARIN will exhaust its last IPv4 address space around July 5<sup>th</sup>, 2015!)**

# A Dire Contingency: Provider Bankruptcies

blogs.wsj.com/venturecapital/2013/10/01/nirvanix-files-for-chapter-11-bankruptcy/

October 1, 2013, 6:11 PM

## Nirvanix Files for Chapter 11 Bankruptcy

Article    Comments (4)

Email    Print    f    t    +    in    A    A

By **DEBORAH GAGE** [CONNECT](#)

Cloud storage company [Nirvanix Inc.](#) on Tuesday filed for Chapter 11 bankruptcy in Delaware federal court, the culmination of a startling flop for what was once seen as a high-flier among cloud startups.

The filing comes on the heels of a notice the company posted on its website last week saying that it was working with International Business Machines Corp. to either return customers' data or help them move it to another cloud storage provider and would try to be available through October 15.



Kharisma Tarigan/Agence France-Presse/Getty Images

Nirvanix had raised more than \$70 million in venture capital since its founding in 2007, according to VentureWire records. In May 2012 after the last funding round, which was \$25 million, [former Chief Executive Scott Genereux told VentureWire](#) that Nirvanix was growing and headed toward profitability and a possible IPO.

Its largest equity holders are [Khosla Ventures](#) and [TriplePoint Capital](#), which may

# Cloud Bankruptcy Concerns...

- If you prepaid (to lock in prices/get a multiyear discount), is that prepaid money in escrow somewhere (and able to be refunded), or is it flat out **gone**?
- Can you find a replacement provider that will be able to take over when it comes to providing the same service that your former cloud provider delivered? (standardized services offered by multiple providers will obviously be easier to replace than unique or bespoke applications)
- If there were custom modifications made to the software you were using, do you have copies of what was changed, and could you replicate them elsewhere?
- Perhaps most critically: can you get your data out, and in format that's usable elsewhere? Proprietary formats should make the hair on the back of your neck stand up.

# Cloud Lock-In: If You Want To Exit The Cloud, Will You Still Have the Required Local Expertise?

- One risk of letting someone else do the heavy lifting for you for a while is that if you need to resume doing that work yourself, it can be a lot harder to get back up to speed than you might think.
- Will you still have key staff?
- Will you still have critical equipment and facilities?
- Can you deliver the professional quality of the services or application you got from the cloud? (you might not think I think so, but truly, some parts of the cloud work pretty dang well)
- Or is this a case of "Welcome to Hotel California:" you can check out, but you can never leave?

## **6. Cloud Risks: Confidentiality**

# Data Confidentiality and Breaches

- Let's not get rat holed on availability. It's a big issue, but not the only one.
- Executives and IT leaders don't get fired for services going down (at least as long as they don't go down for TOO long). IT people do get fired when big data breaches involving PII occur.
- Therefore, most executives and IT people worry a lot about the security of private data, including its security if stored off-site.
- Should they? In some cases, yes. For example...

## Adobe Data Breach: Will Skeptical Cloud Users Exit?

Chris Talbot | *Talkin' Cloud*

Oct. 4, 2013



EMAIL



COMMENTS 0

Adobe's Creative Cloud and Revel customers are among the worst affected by a data breach that has left the personal data of 2.9 million Adobe customers open to hackers. Exactly who and what was affected by the breach are still unknown, but it looks like Adobe's cloud services may have been hit hardest.

This was the last thing [Adobe](#) needed: Another blemish to tarnish the reputation of its [cloud services](#). As Adobe tries to shift customers to cloud services like [Creative Cloud](#), the company has suffered a setback. Hackers have exposed approximately 2.9 million users' personal data.

Although it's not yet clear how many of those users were cloud users, the Internet gossip is that Creative Cloud and [Revel](#) users are among the worst affected by the data breach. What seems to have happened is hackers broke into Adobe's servers to swipe software source code, and according to a [blog post](#) by Brad Arkin, Adobe's chief security officer, Adobe has been attracted more and more attention from cyber-attackers.

And things look pretty bad.

"Our investigation currently indicates that the attackers accessed Adobe customer IDs and encrypted passwords on our systems. We also believe the attackers removed from our systems certain information relating to 2.9 million Adobe customers, including customer names, encrypted credit or debit card numbers, expiration dates, and other information relating to customer orders," Arkin wrote.

# Protecting Data Confidentiality in the Cloud

- Protecting data in the cloud is often largely a matter of how you encrypt private data at rest, and how you encrypt it when it is in transit/on the wire.
- For web based applications, encryption of data on the wire normally involves use of SSL/TLS ("https"). While all SSL/TLS web sites may look more or less the same, **the quality of the encryption used by any given web site may vary dramatically.**
- I'd encourage you to check the SSL/TLS practices of sites you care about using <https://www.ssllabs.com/ssltest/> (caution: sometimes you may be disappointed!)

# Encrypting Data at Rest

- Encrypting data at rest is often trickier.
- Some sites may do whole disk encryption *when the system is quiescent*, but leave all data decrypted once the system has booted up. That reduces (cough) the utility of things like whole disk encryption for systems that are always up and spinning
- Nonetheless, strive to encrypt everything as much as possible, as routinely as possible, and be sure to think about secure cryptographic key storage (e.g., use a hardware security module when possible). See an example of a service that's offering HSM service in the cloud on the next slide.

# Amazon's CloudHSM Service

aws.amazon.com/cloudhsm/

## AWS CloudHSM

The AWS CloudHSM service helps you meet corporate, contractual and regulatory compliance requirements for data security by using dedicated Hardware Security Module (HSM) appliances within the AWS cloud.

AWS and AWS Marketplace partners offer a variety of solutions for protecting sensitive data within the AWS platform, but for applications and data subject to rigorous contractual or regulatory requirements for managing cryptographic keys, additional protection is sometimes necessary. Until now, your only option was to store the sensitive data (or the encryption keys protecting the sensitive data) in your on-premise datacenters. Unfortunately, this either prevented you from migrating these applications to the cloud or significantly slowed their performance. The AWS CloudHSM service allows you to protect your encryption keys within HSMs designed and validated to government standards for secure key management. You can securely generate, store, and manage the cryptographic keys used for data encryption such that they are accessible only by you. AWS CloudHSM helps you comply with strict key management requirements without sacrificing application performance.

The AWS CloudHSM service works with Amazon Virtual Private Cloud (VPC). CloudHSMs are provisioned inside your VPC with an IP address that you specify, providing simple and private network connectivity to your Amazon Elastic Compute Cloud (EC2) instances. Placing CloudHSMs near your EC2 instances decreases network latency, which can improve application performance. AWS provides dedicated and exclusive access to CloudHSMs, isolated from other AWS customers. Available in multiple Regions and Availability Zones (AZs), AWS CloudHSM allows you to add secure and durable key storage to your Amazon EC2 applications.

**Contact Us »**

To sign up or to get more information, please [click here](#)

This page contains the following categories of information. Click to jump down:

- ↓ **AWS CloudHSM Functionality**
- ↓ **Service Highlights**
- ↓ **Pricing**
- ↓ **Resources**
- ↓ **Detailed Description**
- ↓ **Intended Usage and Restrictions**

# Compulsory Access to Your Data

- Cloud providers may, under some circumstances, be required to provide government authorities with access to your data. This may be due to a court order, or as a result of national security program, as was revealed in Edward Snowden's recent leaks (see next slide)
- You may not be notified of government access, particularly if the order served on your cloud provider prohibits the provider from even disclosing the existence of that order to you.
- As is true for other potential confidential vulnerabilities, your best bet is to use strong encryption so that your cloud provider doesn't have the ABILITY to disclose confidential information in unencrypted form.

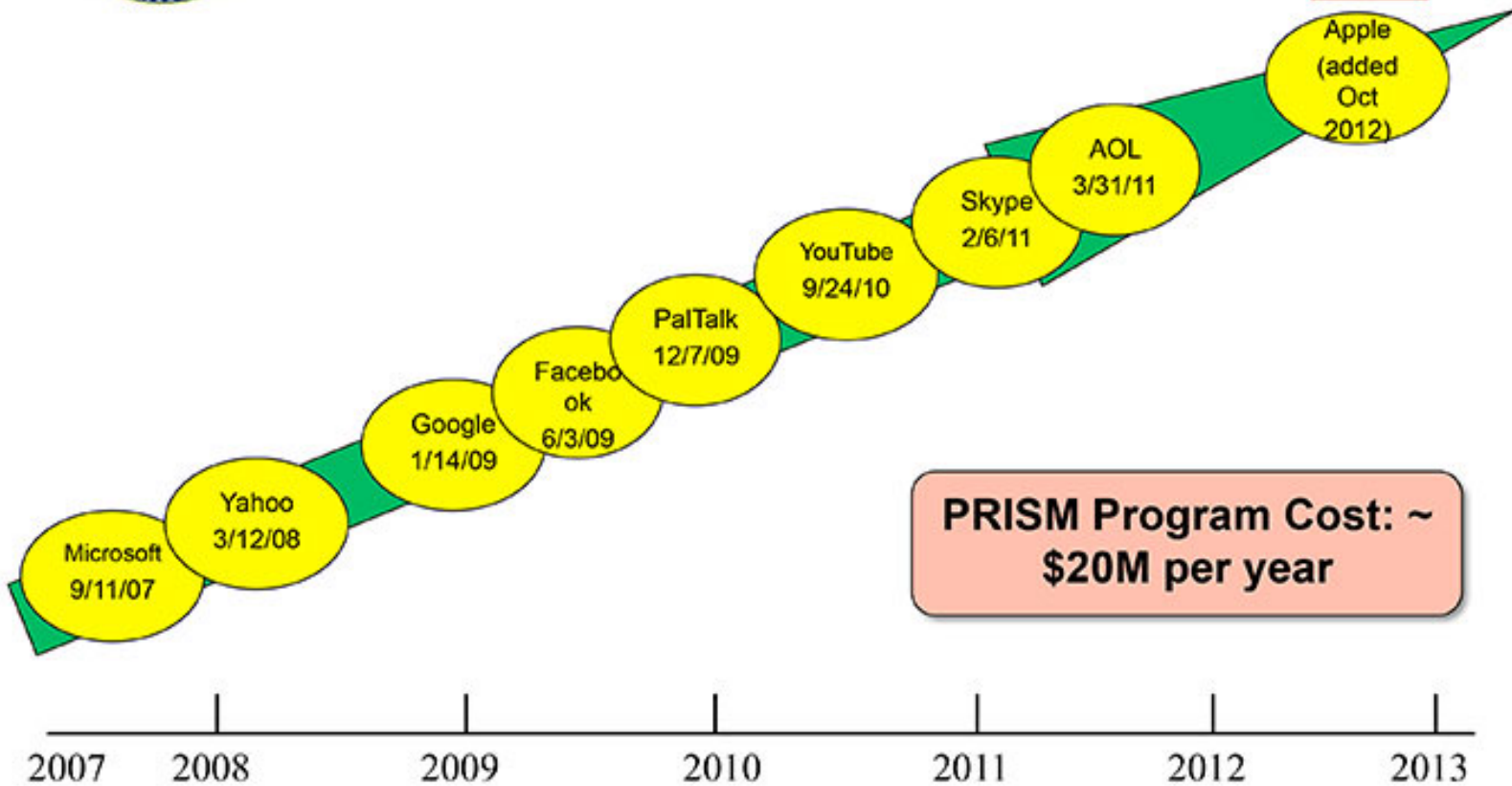


Hotmail

YAHOO!



# (TS//SI//NF) Dates When PRISM Collection Began For Each Provider



**PRISM Program Cost: ~ \$20M per year**

[http://upload.wikimedia.org/wikipedia/commons/c/c7/Prism\\_slide\\_5.jpg](http://upload.wikimedia.org/wikipedia/commons/c/c7/Prism_slide_5.jpg)

## **7. Cloud Risks: Integrity**

# What About Data Integrity in The Cloud?

- Data integrity often seems to be the "red-headed step child" of cyber security: many people seem to pretend this issue doesn't exist.
- How do we rigorously know that the GB (or TB!) worth of files we have stored are correct and un-tampered-with?
- Some of us may checksum critical files, but do we religiously check those file checksums to ensure that nothing's changed? And what about all the files we DON'T check, eh?
- Some might ask "Is data integrity really that big a deal?"
- Sure it is. We just don't think about it as "data integrity" or "files being tampered with," we tend to run into it as "sites getting hacked" or "defaced" or maybe systems getting hit with "ransomware"

# WordPress Plugin Issues: One Path To Unauthorized File Modifications

## Executive Summary

Checkmarx's research lab identified that more than 20% of the 50 most popular WordPress plugins are vulnerable to common Web attacks, such as SQL Injection. Furthermore, a concentrated research into e-commerce plugins revealed that 7 out of the 10 most popular e-commerce plugins contain vulnerabilities. This is the first time that such a comprehensive survey was prepared to test the state of security of the leading plugins. In total, 8 million vulnerable WordPress plugins were downloaded.

The impact? Hackers can exploit these vulnerable applications to access sensitive information such as personally identifiable information (PII), health records and financial details. Other vulnerabilities allow hackers to deface the sites or redirect them to another attacker-controlled site. In other cases, hackers can take control of the vulnerable sites and make them part of their botnet heeding to the attacker's instructions.

[http://www.checkmarx.com/wp-content/uploads/2013/06/  
The-Security-State-of-WordPress-Top-50-Plugins3.pdf](http://www.checkmarx.com/wp-content/uploads/2013/06/The-Security-State-of-WordPress-Top-50-Plugins3.pdf)

# vBulletin CMS Exploit → Full Control

www.net-security.org/secworld.php?id=15743



WhatsApp encryption  
flaw revealed, POC  
code published



Dangerous vBulletin  
exploit in the wild



The cost and frequency  
of cyber attacks on the  
rise



Several IT workers  
among "Operation  
Payback" indicted  
suspects



What can we learn from  
ICS/SCADA security  
incidents?



Linux command line  
cheat sheet

● Top IT predictions for 2014 and

## Dangerous vBulletin exploit in the wild

Posted on 09 October 2013.



vBulletin is a popular proprietary CMS that was recently reported to be vulnerable to an unspecified attack vector. vBulletin is currently positioned 4th in the list of installed CMS sites on the Internet. Hence, the threat potential is huge.

Although vBulletin has not disclosed the root cause of the vulnerability or its impact, we determined the attacker's methods. The identified vulnerability allows an attacker to abuse the vBulletin configuration mechanism in order to create a secondary administrative account. Once the attacker creates the account, they will have full control over the exploited vBulletin application, and subsequently the supported site.

### Initial analysis

Although vBulletin has not disclosed the root cause of the vulnerability or the impact on customers, they did provide a workaround in a [blog](#) post encouraging customers to delete the /install, /core/install in vBulletin 4.x and 5.x respectively.

Additionally, on vBulletin internal forums a victimized user [shared](#) his server's Apache log, providing some visibility into the attacker's procedure:

```
"GET /forum/core/install/upgrade.php HTTP/1.1" 404 613 "-" "-"  
"GET /forum/install/upgrade.php HTTP/1.1" 404 613 "-" "-"
```

# Recovering From Data Corruption Issues

- The most common approach to recovering from data corruption/unauthorized file modifications -- once they're somehow detected -- is to restore data from a trusted backup. When you're running systems locally, you also probably arrange for them to be backed up, periodically testing those backups for usability, etc.
- But what about in the cloud? **Are you backing up data that's there, too, somehow? Or are you trusting your cloud vendor to do it for you?**
- Data loss may be more common (and catastrophic) than you think...

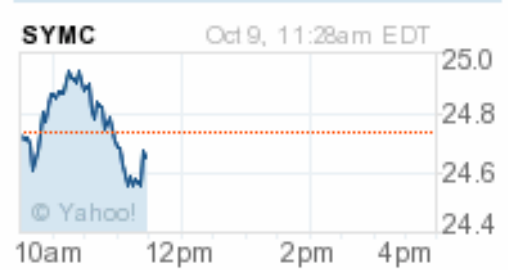
# Cloud Computing Users Are Losing Data, Symantec Finds

INVESTOR'S BUSINESS DAILY\* Investor's Business Daily - Wed, Jan 16, 2013 3:55 PM EST

Email Recommend 18 Tweet Share +1 Print

## RELATED QUOTES

Symbol	Price	Change
<b>SYMC</b>	<b>24.63</b>	<b>-0.11</b>



<b>AMZN</b>	<b>297.45</b>	<b>-5.78</b>
-------------	---------------	--------------

Cloud computing is a ticket to losing data for two in five companies, a new study finds.

"It's really kind of astounding," said Dave Elliott, a cloud marketing manager at storage and security company Symantec (SYMC). The company polled more than 3,200 organizations to gauge hidden costs of the cloud and ways to mitigate problems.

"Forty-three percent of respondents have lost data in the cloud and have had to recover from backups," Elliott said. And the recovery process has failed at least once for most.

# Amazon 2011



The screenshot shows a web browser window with the URL [www.businessinsider.com/amazon-lost-data-2011-4](http://www.businessinsider.com/amazon-lost-data-2011-4). The page features the Business Insider logo and navigation tabs for Tech, Finance, Politics, and Strategy. The main headline reads "Amazon's Cloud Crash Disaster Permanently Destroyed Many Customers' Data". Below the headline, it is attributed to Henry Blodget, dated April 28, 2011, at 7:10 AM, with 92,221 views and 75 comments. Social media sharing icons for Facebook, LinkedIn, and Twitter are visible, along with buttons for "EMAIL" and "+ MORE".

In addition to taking down the sites of dozens of high-profile companies for hours (and, in some cases, days), Amazon's [huge EC2 cloud services crash](#) permanently destroyed some data.

The data loss was apparently small relative to the total data stored, but anyone who runs a web site can immediately understand how terrifying a prospect any data loss is.

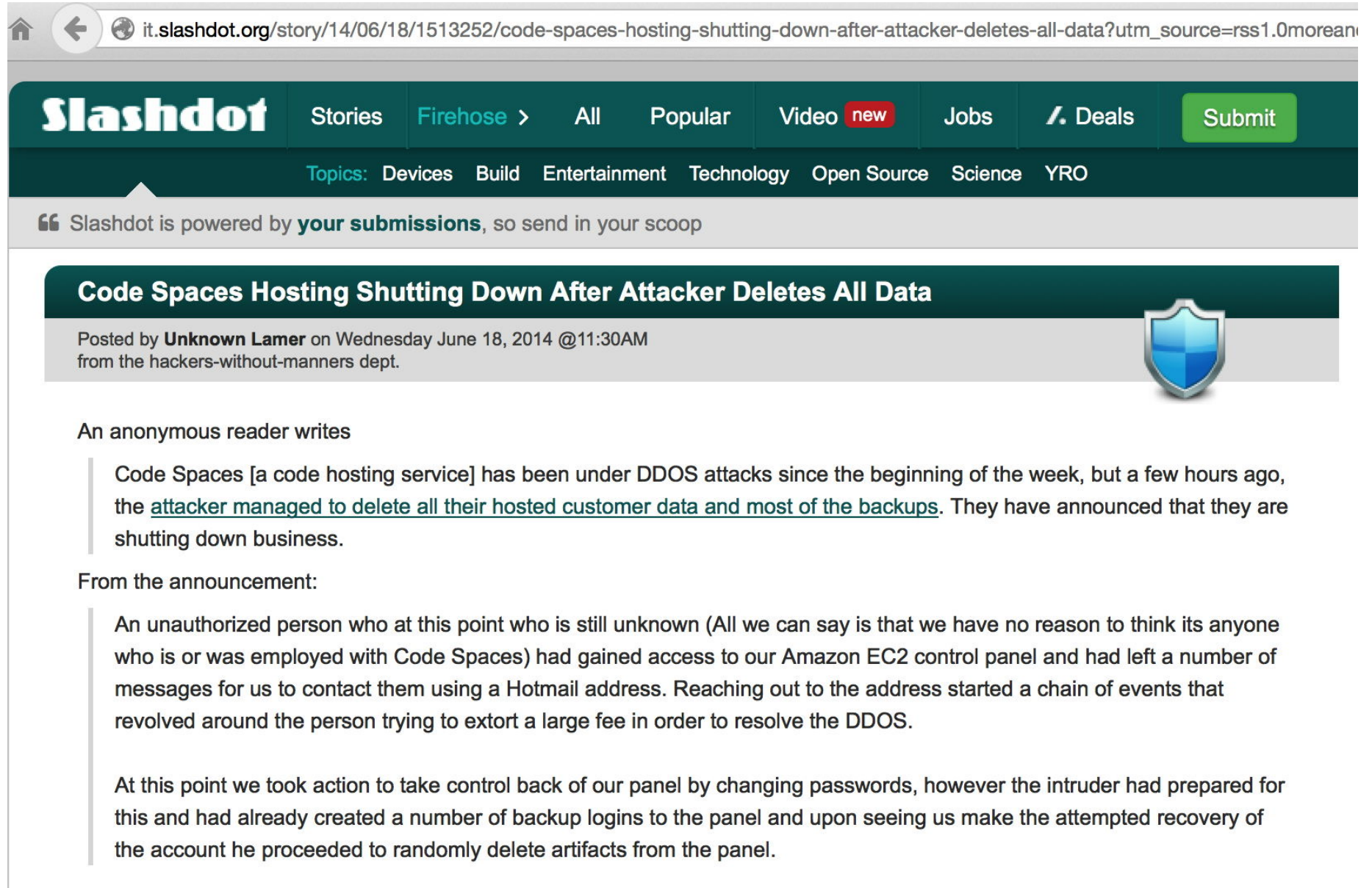
(And a small loss on a percentage basis for [Amazon](#), obviously, could be catastrophic for some companies).

[Amazon](#) has yet to fully explain what happened when its mission-critical and supposedly bomb-proof systems crashed, but the explanation will be



Um...

# Codespaces: Out of Business Entirely



The image is a screenshot of a web browser displaying a Slashdot article. The browser's address bar shows the URL: [it.slashdot.org/story/14/06/18/1513252/code-spaces-hosting-shutting-down-after-attacker-deletes-all-data?utm\\_source=rss1.0morean](http://it.slashdot.org/story/14/06/18/1513252/code-spaces-hosting-shutting-down-after-attacker-deletes-all-data?utm_source=rss1.0morean). The Slashdot navigation bar is visible, with the 'Submit' button highlighted in green. Below the navigation bar, a banner reads 'Slashdot is powered by your submissions, so send in your scoop'. The article title is 'Code Spaces Hosting Shutting Down After Attacker Deletes All Data', and it is attributed to 'Unknown Lamer' on Wednesday, June 18, 2014, at 11:30 AM. The article text describes a DDOS attack on Code Spaces that resulted in the deletion of all customer data and backups. The author mentions that an unauthorized person gained access to the Amazon EC2 control panel and attempted to extort a large fee to resolve the DDOS. The author also notes that they took action to take control back of their panel by changing passwords, but the intruder had already created backup logins and deleted artifacts from the panel.

Code Spaces Hosting Shutting Down After Attacker Deletes All Data

Posted by **Unknown Lamer** on Wednesday June 18, 2014 @11:30AM  
from the hackers-without-manners dept.

An anonymous reader writes

Code Spaces [a code hosting service] has been under DDOS attacks since the beginning of the week, but a few hours ago, the attacker managed to delete all their hosted customer data and most of the backups. They have announced that they are shutting down business.

From the announcement:

An unauthorized person who at this point who is still unknown (All we can say is that we have no reason to think its anyone who is or was employed with Code Spaces) had gained access to our Amazon EC2 control panel and had left a number of messages for us to contact them using a Hotmail address. Reaching out to the address started a chain of events that revolved around the person trying to extort a large fee in order to resolve the DDOS.

At this point we took action to take control back of our panel by changing passwords, however the intruder had prepared for this and had already created a number of backup logins to the panel and upon seeing us make the attempted recovery of the account he proceeded to randomly delete artifacts from the panel.

# When You Start Looking at Cloud Backup

- Be sure to distinguish between backing up data TO the cloud, and backing up what you currently have IN the cloud.
- Remember that our worry is "What happens when the data that was IN the cloud that needs to be restored?" Depending on what caused data to be lost or corrupted, some strategies may NOT save you (example: mirrored data can perfectly mirror data corruption caused by an application flaw, right?)
- Some cloud providers have chosen to specifically focus on cloud backup as a core competency, see for example:  
<http://aws.amazon.com/backup-storage/>  
<http://www.windowsazure.com/en-us/services/backup/>  
<http://www.rackspace.com/cloud/backup/>

## **8. "Integrating" With The Cloud: Another Area of Potential Concern**

# Authentication

- In addition to the big three issues of availability, confidentiality and integrity, you may also see more subtle cloud-related security risks. For example, some cloud providers may not do a very clean job of integrating with your school's identity management system (whatever that may be).
- Some providers may want to do something really, really broken, like periodically syncing a copy of your credential store to their systems (ooh, not good, not good at all), or they may want to use your campus LDAP servers (also not a good model).
- Other providers may substitute their own identity management system as a replacement for yours (hello, OpenID providers).

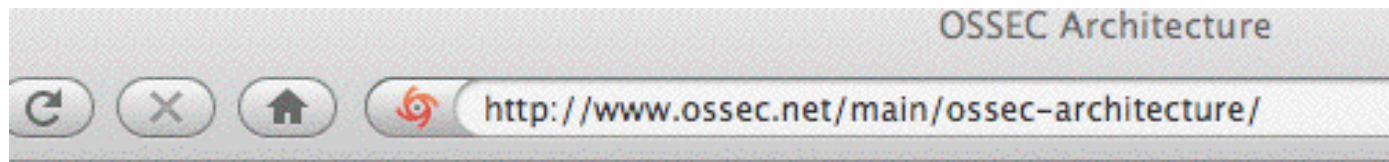
# Cloud Computing And Perimeter Security

- While I'm **not** a huge fan of firewalls (as I've previously discussed in "Cyberinfrastructure Architectures, Security and Advanced Applications," see <http://www.uoregon.edu/~joe/architectures/architecture.pdf> ), at least some sites do find value in sheltering at least some parts of their infrastructure behind a firewall.
- There may be a misconception that cloud computing resources can't be sheltered behind a firewall (see for example "HP's Hurd: Cloud computing has its limits (especially when you face 1,000 attacks a day)," Oct 20th, 2009, <http://blogs.zdnet.com/BTL/?p=26247> )
- Contrast that with "Amazon Web Services: Overview of Security Processes." AWS has a mandatory inbound firewall configured in a default deny mode, and customers must explicitly open ports inbound.

# Cloud Computing & Host-Based Intrusion Detection

- While I'm not very enthusiastic about firewalls, I am a big fan of well-instrumented/well-monitored systems and networks.
- Choosing cloud computing does not necessarily mean forgoing your ability to monitor systems for hostile activity.

One example of a tool that can help with this task is OSSEC (the Open Source Host-Based Intrusion Detection System), an IDS which supports virtualized environments:



## Virtualization/Vmware

OSSEC allows you to install the agent on the guest operating systems or inside the host (Vmware ESX). With the agent installed inside the VMware ESX you can get alerts about when a VM guest is being installed, removed, started, etc. It also monitors logins, logouts and errors inside the ESX server. In addition to that, OSSEC performs the CIS checks for Vmware, alerting if there is any insecure configuration option enabled or any other issue.

# Pen Testing; Working Incidents In The Cloud

- Standard pen testing processes which you may use on your own infrastructure may not be an option in an outsourced environment (the cloud provider may not be able to distinguish your tests from an actual attack, or your tests may potentially impact other users in unacceptable ways)
- If you do have a security incident involving cloud-based operations, how will you handle investigating and working that incident? Will you have the access logs and network traffic logs you may need? Will you be able to tell what data may have been exfiltrated from your application?
- What if your system ends up being the origin of an attack? Are you comfortable with your provider's processes for disclosing information about you and your processes/data?

# Use The Cloud -- Lose Your Logs?

- One of the really useful things you get when you run services locally is log files. You get to see how your services are used, and how people attempt to abuse it. Hopefully you're doing that local logging to a central log server, and processing that data with a SIEM (security information and event management system).
- Often, when you move to the cloud, you may lose access to log files, and that can really hurt when it comes to your situational awareness. A major attack may be going on, and you might not ever know (until it is potentially too late).
- In other cases, logs are available for "web-based" review, but not for integration with your SIEM.
- In yet other cases, logs may be available upon request, but only to help you deal with particular incidents, not for routine review.

# Cloud Computing Also Relies on the Security of Virtualization

- Because cloud computing is built on top of virtualization, if there are security issues with virtualization, then there will also security issues with cloud computing.
- For example, could someone escape from a guest virtual machine instance to the host OS? While the community has traditionally been somewhat skeptical of this possibility, that changed with Blackhat USA 2009, where Kostya Kortchinsky of Immunity Inc. presented "Cloudburst: A VMware Guest to Host Escape Story", see <http://www.blackhat.com/presentations/bh-usa-09/KORTCHINSKY/BHUSA09-Kortchinsky-Cloudburst-SLIDES.pdf>
- Kostya opined: "VMware isn't an additional security layer, it's just another layer to find bugs in" [put another way, running a virtualization product increases the attack surface]

# Cloud Provider Location

- You actually want to know (roughly) where your cloud lives.
- For example, one of the ways that cloud computing companies keep their costs low is by locating their mega data centers in locations where labor, electricity and real estate costs are low, and network connectivity is good.
- Thus, your cloud provider could be working someplace you may never have heard of, such as The Dalles, Oregon, where power is cheap and fiber is plentiful, or just as easily someplace overseas.
- If your application and data do end up at an international site, those systems will be subject to the laws and policies of that jurisdiction. Are you comfortable with that framework?
- Are you also confident that international connectivity will remain up and uncongested? Can you live with the latencies involved?

# Cloud Provider Employees

- If you're like most sites, you're probably pretty careful about the employees you hire for critical roles (such as sysadmins and network engineers). But what about your cloud provider? If your cloud provider has careless or untrustworthy system administrators, the integrity/privacy of your data's at risk.
- How can you tell if your cloud provider has careful and trustworthy employees? Ask them!
  - Do backgrounds get checked before people get hired?
  - Do employees receive extensive in-house training?
  - Do employees hold relevant certifications?
  - Do checklists get used for critical operations?
  - Are system administrator actions tracked and auditable on a *post hoc* basis if there's an anomalous event?
  - Do administrative privileges get promptly removed when employees leave or change their responsibilities?

# End User Support and the Cloud

- You are probably used to locally supporting users of local applications. One of the trickiest things to get used to is recognizing that in the cloud, support may be a another delegated responsibility.
- If a user has a problem, you may not be *able* to answer their question. You may need to refer the user to a cloud provider's support infrastructure, and *that* support infrastructure may be outsourced to a third party overseas.
- Support may suffer, and in some cases that may negatively impact the security of user's work.
- You will also need to learn to live with not being able to have direct access to a ticketing system operated by the cloud provider, so you may not even KNOW what users are struggling with.

# Choice of Cloud Provider

- Cloud computing is a form of outsourcing, and you need a high level of trust in the entities you'll be partnering with.
- It may seem daunting at first to realize that your application depends (critically!) on the trustworthiness of your cloud providers, but this is not really anything new -- today, even if you're not using the cloud, you already rely on and trust:
  - network service providers,
  - hardware vendors,
  - software vendors,
  - service providers,
  - data sources, etc.

Your cloud provider will be just one more entity on that list.

## **9. Assessing Cloud Providers: What's The Basic Question Again?**

**Oh Yeah... "Should We Go Ahead  
With Cloud Provider Foo, Or Not?"**

# "Go Ahead With Cloud Provider Foo?"

- Only two basic answers, after all, "Yes," or "No."
- Presumably you make comparable go/no-go decisions for **local** technologies all the time:
  - Is the campus data center secure enough?
  - What operating systems should we recommend (or ban)?
  - How can we mitigate the risks arising from malware?
  - Is our learning management system FERPA-compliant?
  - Do we need a new policy to deal with unencrypted data on desktops or laptops?
- For **local** stuff, you have myriad sources of local data and advice to help you reach a decision...

# Getting Local Security Intelligence

- For local stuff, you can...
  - Look at your logs
  - Check your passive monitoring infrastructure
  - Actively scan the relevant systems
  - Reach out via phone/email/IM
  - Have meetings with coworkers and users
  - Consult your ticketing system
  - Walk over and pick up a compromised system for forensic review
  - Talk to local developers
  - Discuss issues with district legal
- This is the sort of stuff you're used to doing every day.

# By Contrast: Cloud As "Tycho Magnetic Anomaly"

- The cloud may normally be represented by a fluffy white blob, but the cloud's is actually more like a "black box." You end up needing to figure out what's happening inside of it without being able to open it up or even touch it.
- Remember Arthur Clarke's *Space Odyssey* books? If not, see [http://en.wikipedia.org/wiki/Monolith\\_%28Space\\_Odyssey%29](http://en.wikipedia.org/wiki/Monolith_%28Space_Odyssey%29)
- **Think of a cloud provider as being just like one of Clarke's black monoliths: even though it may have some sort of mysterious force field that keeps you from directly touching it, you still have to decide what it means, if it's safe to have around, and what (if anything) you need to do about it.**
- When you get right down to it, the primary way you're going to do that is by **asking questions.**

# Asking Questions About Cloud Provider Security

- But do you actually want to directly ask questions of the cloud provider? Or are you willing to just "take the cloud provider's word for what they're doing," perhaps by just reviewing some security reports they've already written?
- If you do want to ask questions of the providers, do you want to ask a bunch of questions that you yourself personally dreamed up, perhaps uniquely-well tailored to probe special security aspects of that particular provider?
- Or would you prefer that a qualified auditor/external assessor asked the questions, and you just got to see an audit report? (Would you be willing to sign an NDA to get it?)
- Or do you want to ask questions of others who currently use that cloud-based service? (But what if it's a brand new service, and you are one of the first users of it? Or they've signed NDAs?)

# Taking the Provider's Word For It....

- If you're tempted to try this route, you might hear...
- "Check out their security website. It's all there, and they won't tell us anything beyond what's on it anyhow, so I guess we'll just have to take their word for it."
- "Millions of other users trust these guys, so it's probably safe for us to do so too, right? They're really big, and they seem really smart, so surely they wouldn't screw up anything important about their security, would they?"
- "They're much cheaper (or "free!"), so it's worth taking a chance on them -- heck we couldn't afford to do [insert service name] ourselves if we couldn't get it from them..."
- "Legal okayed it. Don't second guess the attorneys. If something goes go wrong, they'll sue the cloud provider for us."

## Asking Your Own Set of Questions...

- If you try this route, hypothetically you might hear...
- "We'll schedule a conference call, and you can ask any security questions you might have then."
- "[on the call] Let's just start with your half dozen biggest questions. We don't want to get hung up over 'hundreds' of 'techy' security questions..."
- "[next call] What? You've got still more questions? I thought we took care of all those during the last fifteen minutes of the last call... it isn't "fair" to just keep coming up with new security question after question..."
- "[by email] Look. We've got thousands of customers. We can't answer long lists of unique security questions for each customer... We'd have to charge 100X what we currently do..."

# "We'll Review Their Audit Reports"

- What exactly will you be looking for? **What would be a "deal breaker,"** if you saw it in an audit report?
- Some new providers may NOT have been audited at all. Getting audited "just for you" may be expensive, and not something they're interested in doing. What then?
- Not all audit reports are the same, so which one(s) do you want? For example, assume your choice is SOC-1, SOC-2, or SOC-3? (FWIW, AWS offers all three SOC reports, see <https://aws.amazon.com/compliance/#third-party> )
- Providers may be reluctant to share a non-redacted audit report with you (although a major potential customer who is willing to sign an NDA to get access to an audit report may have better luck than a smaller-scale customer who is not willing to sign an NDA)
- How often will any audit need to be repeated?

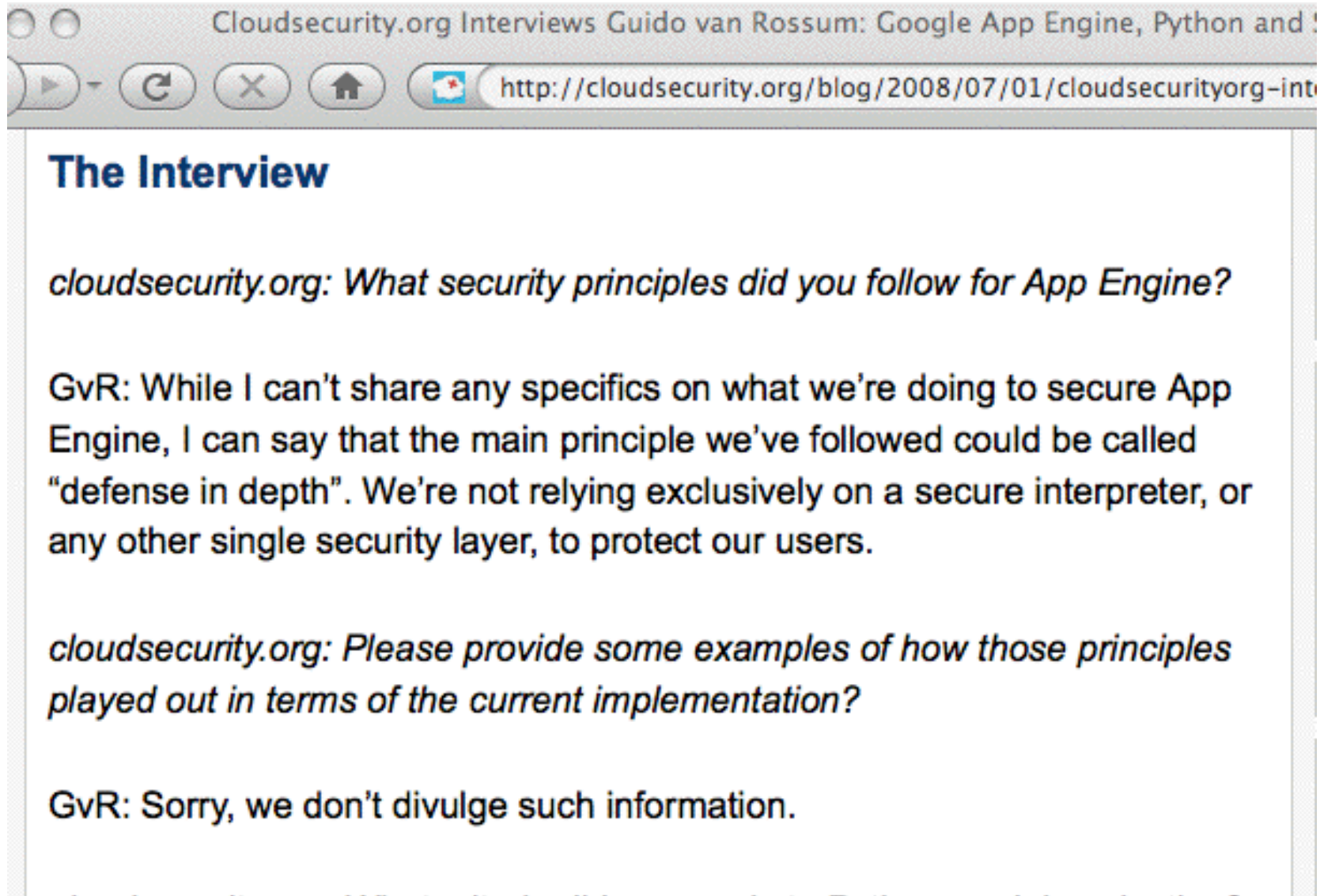
# "Checking References"

- Asking others who may be using the cloud service may give you some insights into what they've seen, but...
- Your site and the reference site(s) may not have the same infrastructure, or the same planned usage, or the same tolerance for risk, etc.
- Pesky NDA terms may limit a colleague's ability to candidly share what they've learned (at least "on the record"/for attribution)
- Just like talking to references for a new potential employee, you usually end up getting referred only to those who have positive opinions (for some reason)
- Oral reports are not very comparable, if you're trying to evaluate multiple potential options side-by-side.

# Cloud Provider Transparency

- You will only be able to assess the sufficiency of cloud provider security practices if the cloud provider is willing to disclose its security practices to you.
- If your provider treats security practices as a confidential or business proprietary thing, and won't disclose their security practices to you, you'll have a hard time assessing the sufficiency of their security practices. Unfortunately, if you run into this, you may need to consider using a different provider.
- Remember: "Trust, but verify." [A proverb frequently quoted by President Reagan during arms control negotiations]

# An Example of The *Wrong* Approach



Source: <http://cloudsecurity.org/blog/2008/07/01/cloudsecurityorg-interviews-guido-van-rossum-google-app-engine-python-and-security.html>

# Using a Standardized Security Framework

- If we want to do a systematic review of cloud provider security, maybe it would make sense to use some sort of **standardized security framework**?
- If we all agree to use the **same one**, a provider would only need to complete one framework, and because the framework would be standardized, we could:
  - Be comfortable that we haven't overlooked anything
  - Easily compare the responses from provider A with the responses from provider B
  - Not have to wait while a provider answers a newly written set of security questions
- If we could all agreed to use the same security framework, providers could just complete that one, confident that it would handle the lion's share of the questions from all users.

# Whose Security Framework Should We Use?

- Cloud security frameworks have been developed by many agencies/organizations, including:
  - Cloud Security Alliance
  - ENISA
  - GSA
  - ISO
  - Jericho Forum
  - NIST
- Just like Goldilocks and the Three Bears, some cloud security frameworks may be too simple, other cloud security frameworks may be too complex. The trick is finding one that's "just right."

# Which Security Framework Should We Use?

- Even if we pick a particular organization, such as the Cloud Security Alliance, they may still have multiple security frameworks available.
- For example, CSA has the Consensus Assessments Initiative Questionnaire (CAIQ) as well as the Cloud Controls Matrix (CCM).
- There may even be multiple editions of each standard...

## One possibility: CSA STAR Registry

- There are many companies listed on the CSA STAR (Security, Trust & Assurance Registry) list, see:  
[https://cloudsecurityalliance.org/star/#\\_registry](https://cloudsecurityalliance.org/star/#_registry)
- Listing on the STAR registry is based on completion of a relatively simple self-assessment, the CSA CAIQ (pronounced "CAKE"). Many of these items require only a "Yes" or "No" response (you can review CAIQ self-assessments for providers of interest on the web site), perhaps plus a brief note.
- If a provider makes just a *pro forma* yes/no response to each item, in my opinion, that's really not very helpful. It's *\*too\** much of just a "checklist" approach.

# **10. Cloud Security Alliance Cloud Controls Matrix**

# CSA Cloud Controls Matrix

- The CSA Cloud Controls Matrix (CSA CCM) is the security framework that I've previously recommended, and continue to recommend folks use for evaluating the maturity and completeness of cloud provider security programs.
- Sometimes folks wonder how the CSA CAIQ and the CSA CCM relate... While the CSA CAIQ aligns with the CSA CCM, the CAIQ is basically a checklist while the CCM provides an outline that would be suitable for preparation of a narrative whitepaper covering relevant security topics in depth
- The CSA CCM approach also avoids any problems that may be associated with completing a checklist but NOT FIXING any issues that may be exposed as a result. If you complete a CSA CCM-based whitepaper talking about your approach to security, it becomes quite difficult to gloss over/ignore areas where obvious deficiencies exist.

# CSA CCM 3.0.1

- The current version of the CSA CCM, 3.0.1, which was released July 16, 2014. It has 133 questions spanning 16 different security domains.
- 133 questions is simultaneously a LOT of questions, yet far fewer than some other assessment instruments. We think CSA got the length and scope of coverage about right.
- As new versions of the CSA CCM come out, some may wonder if they should move to them. My recommendation would be yes, continually update and use the new versions of the CSA CCM, as they get released.

# What Controls ("Rows") Are In The CSA CCM?

- To see, download a copy at <https://downloads.cloudsecurityalliance.org/initiatives/ccm/ccm-v3.0.1.zip>
- Its 133 "controls" are grouped into 16 topical areas:
  - 1) Application & Interface Security
  - 2) Audit Assurance & Compliance
  - 3) Business Continuity Management & Operational Resilience
  - 4) Change Control & Configuration Management
  - 5) Data Security & Information Lifecycle Management
  - 6) Datacenter Security
  - 7) Encryption & Key Management[continued on the next slide]

# What Controls ("Rows") are in CSA CCM? (2)

- 8) Governance and Risk Management
  - 9) Human Resources
  - 10) Identity & Access Management
  - 11) Infrastructure & Virtualization Security
  - 12) Interoperability & Portability
  - 13) Mobile Security
  - 14) Security Incident Management, E-Discovery & Cloud Forensics
  - 15) Supply Chain Management, Transparency and Accountability
  - 16) Threat and Vulnerability Management
- Many of the items in each of these areas are pretty basic "common sense" items.

# Items From One of Those 16 Areas: Threat and Vulnerability Management

- **TVM-01, Anti-Virus / Malicious Software:**

Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.

# Items From One of Those 16 Areas: Threat and Vulnerability Management (2)

- **TVM-02, Vulnerability/Patch Management:**

Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g. network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies and procedures and identified weaknesses especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.

# Items From One of Those 16 Areas: Threat and Vulnerability Management (3)

- **TVM-03, Mobile Code:**

Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of unauthorized mobile code, defined as software transferred between systems over a trusted or untrusted network and executed on a local system without explicit installation or execution by the recipient, on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.

# The Columns In the CSA CCM

- When you look at the CSA CCM and patiently scroll across, you'll see that there are also multiple columns in the spreadsheet:
  - A: Major control area and control name (e.g., "Threat and Vulnerability Management: Mobile Code")
  - B: Control ID number (e.g., TVM-03)
  - C: Control specification (narrative text of the control)
  - D-I: Architectural Relevance (compute? storage? net?)
  - J: Corp Governance Relevance?
  - K-M: Cloud Service Delivery Model Applicability (Software as a Service? Platform as a Service? Infrastructure as a Service?)
  - N-O: Supplier Relationship (Service Provider? Tenant/Consumer?)
  - plus lots of security frameworks [COBIT, ENISA, NIST 800-53, etc]

# The CSA CCM Does Not Highlight Controls That **OTHER** Frameworks Require That Are Missing

- If you were to take SP 800-53 R3, and build a new spreadsheet where each row was one control required by SP 800-53, you could then check to see which of those controls are (or aren't) covered by the CSA CCM.
- You CAN'T get that information from the current CSA CCM spreadsheet because the **ONLY** controls listed in the CSA CCM are the ones that the CSA CCM ALREADY HAS.
- That is, the CSA CCM lets us answer the question, "Is what the CSA CCM requires consistent with what other security frameworks require?" (And the answer would be largely "yes")
- It does **NOT** help us answer the **OTHER** (perhaps more interesting) question, "Are there things other frameworks require that are **missing** from the CSA CCM?"

# What's A "Passing Score" on the CSA CCM?

- For example, does a site need to have all controls perfectly addressed? 90% of them? A majority of them in some form or another? What if they're all just TBD/in progress?
- There's no right or wrong answer to any item, and many different approaches could work. A stronger response to one item might offset a weaker response to another.
- Sometimes, just seeing HOW a company responds to a CSA CCM item can be very instructive -- do they take the process seriously? Do they just try to get it out of the way as quickly as they can, treating it as if it were a checklist? Do they have answers that appear to be internally inconsistent?
- Academics understands grading essay exams. :-)

# Every Site's Needs May Be Different

- Another reason why there's no "passing score" on the CSA CCM is that even if we agree on the set of questions we're going to ask, what's an acceptable answer to those questions may vary from site-to-site.
- For example, site A may be interested in offering an easy-to-use free application for student recreational use, and they may have minimal security concerns as a result.
- Site B, on the other hand, might want to deploy an application for use with special education students, triggering significant worries about accessibility, data privacy, compliance, etc.
- Different sites, different requirements, different thresholds for what's acceptable.
- One uniform "passing score" wouldn't work for everyone.

# The Goal: Give YOU The Data You Need

- Because every site's different, the goal should be to give you at least most of the data you need to make an informed decision, without making you pry it out of the cloud provider yourself.
- Ideally, the data should even be publicly available so you don't even need to screw around requesting it, you should just be able to click on the data you need in a public repository. (If a provider is reluctant to publicly share their CSA CCM results, that might be something worth exploring, too).
- If something doesn't look right to you, you can follow up with the cloud provider directly, digging in on the issue of concern to you. Maybe the issue is just a matter of a misunderstanding, and something that can be easily rectified.

# "Couldn't a Provider Just Lie When Doing Their CSA CCM Writeup?"

- That's always a possibility, but if they've provided a written statement describing what they're doing, and that statement subsequently proves to be factually inaccurate or intentionally misleading, you likely have a good basis for talking with legal counsel if things go awry.

- I discuss this and more in a draft two page document you can retrieve from:

<http://www.stsauver.com/joe/using-the-ccm-with-net+.docx>

- If you're really worried, you can always ask for audits (but if you really don't trust them, well...)

# Another Reality: You May Have Limited Luck Seeking Major Changes From a Huge Cloud Provider

- Cloud providers are all about offering standardized services at scale.
- As such, they may not be willing (or even able) to consider modifying their service (or their practices/procedures) to meet your preferences/needs.
- If they did make changes to meet your needs, they might find those changes aren't welcomed by an equal number (or more!) existing customers, customers who liked how the provider traditionally did things. Therefore, you may need to live with "off the rack" rather than custom tailored offerings.
- Small entrepreneurial cloud providers, on the other hand may be potentially much more flexible.

# CSA CCM and "Recursive Cloud Providers"

- As we worked with the CSA CCM, we quickly came to realize that some parts of it are not applicable to (or even easily answered by!) a cloud app vendor that is hosting their cloud app on cloud infrastructure.
- For example, when it comes to the "Data Center Security" section of the CSA CCM, a typical cloud application vendor may have no idea how to respond to those items, because they don't run the data center they're using, some other cloud provider does.
- They may still be RESPONSIBLE for how that data center works, but they may need to rely on what they're told by their cloud infrastructure provider.

# Giant Clouds and Teeny-Tiny Clouds

- Another rapid discovery: some cloud providers are giants, with huge staffs (including entire (LARGE!) teams focused on security and compliance and privacy).
- Other cloud providers, particularly entrepreneurial cloud app vendors, might be tiny. If their total staff amounted to half a dozen people, it would be very unlikely that one of them would be devoted entirely to security/compliance/privacy.
- This difference in security "maturity" impacts the security processes the vendor may have, and the amount of help they may need when it comes to completing a framework like the CSA CCM.
- It also shows up in things like "division of responsibility" requirements: tiny entrepreneurial cloud providers may not have enough staff to divide up roles and responsibilities the way large firms do.

# Anything Else Would We'd Really Like To See From Cloud Service Partners?

Providers should follow the model of Amazon Web Services, and have a non-passworded web site that publicly provides transparent information about security, compliance and privacy related issues (see <http://aws.amazon.com/security/> )

# Thanks for The Chance To Talk Today!

- Are there any questions?