Your Time Is Now
Cloud Systems and What They Mean to Your Company

Troy Sherman, Security Sherpa
BRKCLD-2000
Agenda

• Introduction/Security
• What We Do
• Types of Clouds
• Security Concerns by Type
• Standards, Certifications, Policies
• Conclusion
Who am I?

- My name is Troy Sherman
- I have worked at Cisco for over 19 years
- I have worked on security for over 15 years
- I have worked on security on routers, switches, voice/video, software, cloud, etc.
- Unlike many people you will meet this week from Cisco, I do not know everything
Introduction

• What to expect out of this session:
  • What is the cloud to you?
  • What types of clouds are there?
  • Is the cloud for your company?
  • What type of cloud is best for your company?
  • How do you control this cloud?
  • What does security look like in the cloud?
  • What do Cloud Providers/Vendor own?
The Black Hole
Cloud Security Example
WebEx Security Defined

- WebEx does not store any data other than meeting recordings
- This means that we are less interesting then people who store data (think money)
- Even today, Webex’s largest area of attempted theft is dial tone (you read that correctly)
- Even though we are less interesting then many, we have a great deal of security
WebEx Security Routine

• Security test teams
  • Internal security code review
  • All open source systems/packages reviewed automatically daily for security issues
  • Internal attacks based on being on Cisco’s network – apps and network (internal and contract security teams)
  • External attacks from the internet (internal and contract security teams)
  • External security teams rotated at least 1 time a year, usually 6 months
  • Manual review – data from tech owners or security teams found on external website
  • At least weekly security meetings for both network and software issues review
  • Source code review by internal security teams
WebEx Security Routine

• Security test teams
  • Weekly InfoSec scans of network and applications –
    • Authenticated for OS, apps, network gear and network configs
• Audits
  • Source code
  • ISO audits
  • FedRAMP audits
  • SOX audits
  • Open Source audits
  • Source code

Additional security applied to the US government environment
Enterprise Data Systems

- Enterprise Data is deep in the network
- Layers and layers of protection
Types of Clouds
Types of Clouds

• Private
• Public
• Hybrid vs. Pure Cloud
• Infrastructure as a Service
• Platform as a Service
• Software as a Service
• ETC…
Private Cloud

• Just as it sounds, it is private
• Can be hosted on premise or in a private cloud provider
• In many cases you have to be at the company to access the data
Private Clouds

• Usually the company owns and runs the software

• The company owns the security
  • If the company security is lax, their private cloud security will most likely be lax

• Security can be very good – but many not need to be
  • Not exposed to the internet
  • Can only see the service if you are at work if you VPN to the company
  • Control is like any other application internal

• Kind of funny actually, email is a hosted cloud at your company
Car as a Service

On Prem/Hosted

- Car
- Finance
- Depreciation
- Servicing
- Oil/Tires/etc.
- Insurance
- Road Tax
- Garage
- Fuel
- Tolls
- Driver

<table>
<thead>
<tr>
<th>Car is Owned</th>
<th>Managed by Company</th>
<th>Managed by Cloud Provider/Vendor</th>
</tr>
</thead>
</table>

- You/The Company owns the car
- The company owns maintaining the car
  - Keeping systems up to date
  - Monitoring security
- The company owns the software or applications
- The company owns the network and network security
- The company has no one to blame if things do not go well
Public Clouds

- As it sounds – the application or service is now open to the public
- The system can be located at your company or by a provider
- Usually allows anyone to access some or all of the data
Public Clouds

- Usually the company owns the software
- Company usually owns the security
  - If security is lax, it does not matter if it is remote or local, the security can be weak
- Security can be very good
  - Hosted on site can be controlled by the IT department
  - Hosted in remote data center can still be controlled by IT and have good security
  - Can control the data that is exposed
  - Depending on the application very little security is needed
- Classic public cloud things can be a webserver
Hybrid Cloud

• A system that is hosted in a private cloud and also in a public cloud

• Usually the systems add functionality to each other
  • Functionality stays local and the company can control it
  • Functionality can move in the public cloud
  • Usually get increased functionality with the cloud interconnect
Hybrid Cloud

• Thinks start to get interesting with this deployment
  • The company has to trust security of the cloud systems

• Company can control security on site, but not remote in the cloud
  • Have to start asking what the cloud security is
  • How do the two or more systems talk to each other
  • What protocols do I need to allow in and out of my network

• Many companies start this way with clouds because they have a degree of control
  • Go on a date but not get married
  • Have most of what the company needs still local on prem
IaaS – Infrastructure as a Service

- Cloud Provider Supplies the infrastructure
  - Hypervisors/Containers to run virtual machine
  - Network infrastructure
  - Load balancing
  - Compute power

- Security is supplied by the cloud provider, but only for the parts they own

- Companies like this system because all they have to do is move their VM’s right?
Car as a Service

- The company no longer owns the car, leased
- The company does not own the network and network security
- The company does not own the compute or Hypervisors
- The company owns maintaining the car
  - Keeping systems up to date
  - Monitoring security
- The company owns the software or applications
- The company can only blame the provider if they stop making the car payments (keep the lights on)
PaaS – Platform as a Service

- Cloud Provider Supplies the infrastructure and other systems
- On top of what was listed in IaaS
  - Virtual Machines and OS’s
  - Webservers
  - Databases
  - ETC
- The company builds software that runs on the providers system
Car as a Service

- The company no longer owns the car, Car Hired
  - Network and network security
- The company does not own maintaining the car
  - Keeping systems up to date
    - OS, Compute, Hypervisor, network, etc
  - Monitoring security
- The company owns the software or applications
- The company’s only responsibility is to pay to drive the car (keep the applications running)
SaaS – Software as a Service

• The full on cloud experience
• Nothing comes from the company at all
  • Provider does all the OS, systems, supporting software
  • The application is owned by the provider
  • There is nothing installed at the customer site
    • Can be on premise in some cases, but not usually
• All security is controlled by the provider
  • Network
  • Applications
  • OS’s
Car as a Service

- The company no longer owns the car - Uber
  - Network and network security
- The company does not own maintaining the car
  - Keeping systems up to date
    - OS, Compute, Hypervisor, network, etc
  - Monitoring security
- The company does not own the software
- The company does not even drive the car – it is an Uber, someone drives you around
Car as a Service

- **On Prem/Hosted**
  - Car
  - Finance
  - Depreciation
  - Servicing
  - Oil/Tires/etc.
  - Insurance
  - Road Tax
  - Garage
  - Fuel
  - Tolls
  - Driver

- **IaaS**
  - Car
  - Finance
  - Depreciation
  - Servicing
  - Oil/Tires/etc.
  - Insurance
  - Road Tax
  - Garage
  - Fuel
  - Tolls
  - Driver

- **PaaS**
  - Car
  - Finance
  - Depreciation
  - Servicing
  - Oil/Tires/etc.
  - Insurance
  - Road Tax
  - Garage
  - Fuel
  - Tolls
  - Driver

- **SaaS**
  - Car
  - Finance
  - Depreciation
  - Servicing
  - Oil/Tires/etc.
  - Insurance
  - Road Tax
  - Garage
  - Fuel
  - Tolls
  - Driver

- **Uber**
  - Car
  - Finance
  - Depreciation
  - Servicing
  - Oil/Tires/etc.
  - Insurance
  - Road Tax
  - Garage
  - Fuel
  - Tolls
  - Driver

Colors:
- Blue: Managed by Company
- Green: Managed by Cloud Provider/Vendor

- **Car is Owned**
- **Car Lease**
- **Car Hired**
- **Uber**
Security by Clouds Types
Security for Private, Public, Hybrid

- All of these styles of deployments are owned by the company
  - Can be shared, but for today we will consider security a company issue
- We are really not here to talk about what your company might do for security in these deployments
- These types of systems usually just mirror what the company already does with internal applications
IaaS
Security for IaaS

• Partnership – IaaS and company have to work together
  • Both systems have to be secure for end to end protection

• Systems that the company no longer controls
  • The network
  • The hypervisor
  • The base compute systems
  • Connections to move your data
  • Connections to move your images

• What is still the company’s ownership
  • OS’s
  • Applications running in the systems
  • Policies and procedures for deployment
Security for IaaS - Network

• The network
  • How are you segregated from other groups or companies
  • What security do they place in the network
    • North – South – in and out of the network
    • East – West – Side to side with your neighbors
    • High availability
    • Security between Data Centers
    • How many upstream providers

• Not traditional security like a DMZ
  • The provider job is to face the internet all the time
  • There is no internal network to protect like at a company

• Incident response and forensics capabilities
Security for IaaS - Hypervisor

• The hypervisor
  • What system do they use
  • How often is it upgraded
  • Pay service or Open Source
  • Special things they might do
    • Do these added value things lock you into the provider
      • Example – some providers give you load balancing, others do not
      • If you depend on vendor extras it makes moving harder

• What security systems do they have in place

• Who can see your systems from the vendor?
  • What admins can see what of a companies system?

• Where are they managed from?
  • What country, what time zone, etc…
Security for IaaS – Compute and Transport

• The base compute systems (hardware)
  • How are the compute systems checked for security?
  • Do they build their own or off the shelf?
  • How often are they upgraded

• Connections to move your data
  • Connections between your systems
  • Connections for management

• Authentication and authorization
  • Important in all areas
Security for IaaS – Company Owned

• What is still the company’s ownership
  • OS’s
    • Most companies are not prepared for this
    • How hard is the OS?
    • Does root own anything?
    • Are all packages that are not needed removed?
    • How does the company maintain security of the systems that are deployed
    • New bugs every day that will affect deployment
  
• Applications running in the systems
  • How does the company enforce good code
  • Most internal systems don’t care about external attacks, but they have to now
  • Data Leakage – could be both provider and company

• This Means – you just can’t move a VM from internal systems to external and expect it to be secure
Security for IaaS – Company Owned

• What are the polices for the company
  • Who can spin things up?
  • Spinning up cost money and can decrease security
  • Controls in place to manage the OS’s and applications
  • Consider polices and procedures before the company deploys
  • Where is the data at the vendor stored?
  • Great shirt – I don’t code often, but when I do I test in production……

• How do you do incident response?
  • Who owns outbound messaging
  • When do you announce the company has had an issues
  • How much damage will the event cause
  • What does legal have to say about the event
Security for IaaS Summary

- Understand what the Vendor controls and what the company controls
- Make sure they are providing the best security they can to run your OS and applications
- The vendor does security for the cloud every day all day, the company moving to IaaS does not
  - How good is the security of everything the company controls
  - How good are the policies at the company
  - Don’t wait for an event, who owns what when a security event happens
  - If everything the vendor owns is up and running, and the company's application or OS is down, the vendor has done their job
Car as a Service

- The company no longer owns the car, leased
- The company does not own the network and network security
- The company does not own the compute or Hypervisors
- The company owns maintaining the car
  - Keeping systems up to date
  - Monitoring security
- The company owns the software or applications
- The company can only blame the provider if they stop making the car payments (keep the lights on)
PaaS
Security for PaaS

• Partnership – PaaS and company have to work together
  • Both systems have to be secure for end to end protection

• Systems that the company no longer controls
  • The network
  • The hypervisor
  • The base compute systems
  • OS
  • Packages it takes to run your application

• What is still the company’s ownership
  • Applications running in the systems
  • Policies and procedures for deployment

• Builds on the security for IaaS – ownership moves
Security for PaaS

• Vendor owns
  • Network
  • Hypervisor
  • Compute and Transport
  • New ownership – OS and packages

• Incident response for everything but the applications is now owned by the vendor
  • All earlier rules still apply just ownership changes

• As in the IaaS – is the application really ready for the net?
  • The vendor can sometimes help in this area
  • The vendor does not own the security anyone's application
  • If an application goes down, but all other systems are up, the vendor has done his job
Security for PaaS

- Very much like the IaaS but what the company owns is smaller
- PaaS provider does security for the OS and packages
  - PaaS provider does this security every day
  - Could be better security than IaaS because company no longer owns the OS
  - Package should be more up to date than what companies usually run
  - This is not a hard and fast rule, but again, they do this for a living

- Data leakage and data protection becomes more of the vendors issue
  - What systems are in place to protect your data
  - What rules or standards does your data require?
    - HIPPA, SOX, ETC.

- What controls are in place that the company can use to protect systems and applications?
  - Examples
    - Single Sign-on integrations, Cert Management, Key Management, ETC.
Car as a Service

- The company no longer owns the car, Car Hired
  - Network and network security
- The company does not own maintaining the car
  - Keeping systems up to date
    - OS, Compute, Hypervisor, network, etc
  - Monitoring security
- The company owns the software or applications
- The company’s only responsibility is to pay to drive the car (keep the applications running)
SaaS
Security for SaaS

• Vendor owns everything

• Systems that the company no longer controls
  • All of it, the vendor owns everything but local admin functions

• What is the company responsible for
  • Access to the applications
  • Management of the application
    • Remote management settings based on the application
    • Setting like SSO, what users can see what data, what users can change data, ETC.

• Builds on the security for IaaS and PaaS – Almost all ownership move to vendor

• All security in this deployment is the providers reasonability
Security for SaaS

• Incident response for everything is now owned by the vendor
  • All earlier rules still apply just ownership changes

• Unlike the IaaS and PaaS – the application is ready for the net
  • This is all the vendor does
  • If something fails it is the providers issue
  • What SLA or up time guaranty?
  • Incident response to customers
  • What interconnects do they have to a company?
    • SSO, API, ETC.
Car as a Service

- The company no longer owns the car - Uber
  - Network and network security
- The company does not own maintaining the car
  - Keeping systems up to date
    - OS, Compute, Hypervisor, network, etc
  - Monitoring security
- The company does not own the software
- The company does not even drive the car – it is an Uber, someone drives you around
Types of Attacks
Attacks

• Attack are pretty much universal to any cloud system
  • It is just who owns the issue or prevention

• Types of attacks
  • Account hijacking
  • Data leakage
  • Denial of service
  • Data Manipulation in the application – sql injection
  • VM Control – take over one and then the one next door
  • VM used to attack your systems (many AWS systems are attack systems)
  • Spoofing networks
  • Bad or no authentication on systems – API, Web, Other
  • No encryption on paths in and out of the system
  • Lazy enforcement of general security systems
    • Password length
    • Password Expire
    • Failed login attempts – admins and users
Standards/Controls/Acts
Standards/Controls/Acts

- HIPPA
  - Health Insurance Portability Accountability Act
- PCI
  - Payment Card Industry
- FedRAMP
  - Systems needed to pass to sell cloud systems to the US government
- FERPA
  - Family Educational Rights and Privacy Act
- CIPA
  - Childs Internet Protection Act
- FISMA
  - Federal Information Security Management Act
Standards/Controls/Acts

- Safe Harbor
  - The old way to protect data with the EU

- EU-US Privacy Shield
  - The new way to protect data in the EU
  - Pushing companies to more and more personal protection
  - PII is more important - Personally identifiable information
  - No Mass surveillance
  - Ability to be forgotten
  - Harder to get information from the EU to the US
    - More conditions for this information
Standards/Controls/Acts

• PII

  • Taking into account every country – everything is PII
    • Names can be defined as – first and last, first, last, login name, screen name, nickname, handle, email domains (more than one)
    • Addresses – Full address or partial addresses of – country, state, city, postal code, geo location
    • Any type of Identification Number – SSN, passport, credit card, IP address, telephone number, ETC.
    • Information about the user – facial recognition, finger print, handwriting, age, gender, race, job position, health, medical records

• How do companies control this PII?
  • Where is it?
  • Is it encrypted?
  • Who gets to look at it?
    • Places people forget - Logs
Standards/Controls/Acts

• Nation States
  • Many have more laws over and above the groups they are in
    • Germany and Spain have very restrictive PII laws
    • I think history has made them more informed about privacy (personal opinion)
  • Some make you keep the data on people in their country
  • Some are about to force providers to have back doors to spy on
  • If the company is the provider of the service, where is the cloud service allowed?
    • Example – in India you cannot use VoIP to bypass the telephone companies
      • How does that affect a meeting SaaS like WebEx that uses phones?
      • Data voice traffic was not allowed in settings
Conclusion

• If your company is moving to the cloud be careful
  • Your management needs to understand the risk
  • Things are not as safe as they are at home
  • Everyone needs to understand what they own and how to protect it
  • Understand what needs to be protected and how to do it
  • Have a plan in place when there are security issues
  • Look at all the regulations that might affect you world wide
  • Understand where your customer is at and what PII controls they have
Conclusion

• The providers responsibility to you or your company is
  • How they handle security issues
  • Who they contact
  • What security they have in place for internet real-estate
  • How they protect data
  • What they use to protect people and systems that your company uses
Security Joins the Customer Connection Program
Customer User Group Program

• **Who can join**: Cisco customers, service providers, solution partners and training partners

• **Private online community** to connect with peers & Cisco’s Security product teams

• Monthly **technical & roadmap briefings** via WebEx

• Opportunities to **influence product direction**

• Local **in-person meet ups** starting Fall 2016

• **New member thank you gift** & badge ribbon when you join in the Cisco Security booth

• **Other CCP tracks**: Collaboration & Enterprise Networks

---

Join in World of Solutions

Security zone → Customer Connection stand

- Learn about CCP and Join
- New member thank-you gift*
- Customer Connection Member badge ribbon

---

Join Online

[www.cisco.com/go/ccp](http://www.cisco.com/go/ccp)

Come to Security zone to get your new member gift* and ribbon

---

* While supplies last
Participate in the “My Favorite Speaker” Contest

Promote Your Favorite Speaker and You Could Be a Winner

• Promote your favorite speaker through Twitter and you could win $200 of Cisco Press products (@CiscoPress)

• Send a tweet and include
  • Your favorite speaker’s Twitter handle <Speaker—enter your Twitter handle here>
  • Two hashtags: #CLUS #MyFavoriteSpeaker

• You can submit an entry for more than one of your “favorite” speakers

• Don’t forget to follow @CiscoLive and @CiscoPress

• View the official rules at http://bit.ly/CLUSwin
Complete Your Online Session Evaluation

• Please complete your Online Session Evaluations after each session

• Complete 4 Session Evaluations & the Overall Conference Evaluation (available from Thursday) to receive your Cisco Live T-shirt

• All surveys can be completed via the Cisco Live Mobile App or the Communication Stations

Don’t forget: Cisco Live sessions will be available for viewing on-demand after the event at CiscoLive.com/Online
Continue Your Education

• Demos in the Cisco campus
• Walk-in Self-Paced Labs
• Table Topics
• Meet the Engineer 1:1 meetings
• Related sessions
Thank You
Your Time Is Now