

# *EMBRACING CLOUD COMPUTING*

*Adopting and Adapting Smartly*



Adam Crosby, RVASec 2015


*Why  
Embrace  
Cloud*

---



# *Market realities*

---

- Marketing
    - Your boss and senior leadership is probably getting a ton of magazine/news/etc. emphasis on 'cloud' and doesn't want to feel left out
  - Tech talent
    - What's the last startup you saw building datacenters and hosting equipment?
  - Agility
    - Fail fast, fail cheap is rapidly becoming a tech-side mantra
  - Roadmaps
    - Big name software vendors are looking at delivering their products via SaaS as the Only Future
- 

*Telling folks Windows is insecure hasn't stopped it from proliferating...why would cloud be different?*

*MORE  
IMPORTANTLY,  
YOU'RE ALREADY  
THERE\**

---

\*Probably – AWS doesn't have a million individual customers that are all brand new startups...

*So, Adopt  
Smartly*

---



*HOW?*



*Don't let lawyers pick*

*CHOOSE  
CAREFULLY*

---

# Vendor Selection is Critical

- Look for indicators of success
- Don't sweat SLA terms (think MTBF)
- Don't let Lawyers get wrapped around T&C's



These pictures means my cloud is super secure right?!

**Whether in connection with your account or a service, in no event will either party to this Agreement or its respective directors, officers, employees, or agents be liable to the other party for any special, consequential, indirect or punitive damages, whether any claim is based on contract or tort or whether the likelihood of such damages was known to either party.** The foregoing limitation of liability will not apply where expressly prohibited by the laws governing your account. The Bank will not have any liability to you if there are not

A. The Company will use reasonable efforts to provide Electric Service that is reliable, but the Company does not undertake to guarantee that interruption will not occur.

Your Bank and Power Company have awesome SLA's and Indemnity clauses



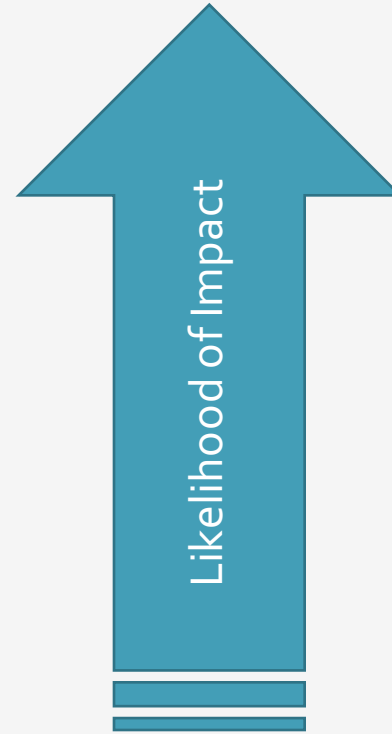
*Most of the old ones still apply too*

*BE AWARE OF  
NEW THREATS*

---

# *The Big 4*

- CSP Account Current-ness
- CSP Biz Stability
- CSP Insider Threat
- Technical Attacks



*'What do you mean I can't do X in the cloud'*

*SAYING  
GOODBYE TO  
FAMILIAR FACES*

---

*Things you  
(generally)  
should  
prepare to  
let go of*

- Full packet capture from passive network taps
- Full physical isolation
- Racks and Racks of awesome hardware from major security vendors
- Passive security bolt-on

With respect to NSM-fans, pure network infosec is going the way of the dodo.

*Smartly, not blindly*

# *RISK MITIGATIONS*

---

# *If All My Tools are Gone, How do I Work?*

- **SECURITY MUST BE PART OF THE ARCHITECTURE**
- Take advantage of new capabilities, and design for failure
- Learn from Zane Lackey

If we spent as much time looking at application sec as we did at PCAPs...


*I don't have to drive to the datacenter to do that?*

*SAYING HELLO  
TO NEW  
FRIENDS*

---

# *Things to Cozy Up to*


---

- APIs
  - Automation
  - APIs and Automation
  - Delegation and refocusing of resources
  - Encryption
- 




# *APIs and Automation*

---

- Nearly instant, definitive access to tons of information, built in for free to most CSP platforms
  - When was the last time you had a comprehensive inventory of hosts on your network?
  - E.g.: Heartbleed patching prioritization – instead of a mad scramble to get the patch every where **right now**, able to query CSP for list of instances and associated filtering rules and prioritize patching those that had a related port (25,443,993, etc.) exposed to the Internets.
- 

# *APIs and Automation (cont'd)*

---

- Many CSPs offer 'alert' or 'log trail' streams (or both in different fashions)
  - Active Defense
  - Traceable and enforceable CM
  - DFIR and Root Cause dream world
  - Copy and Playback
- 


# *Delegation and refocusing*

- Shared Responsibility – let the CSP handle physical/etc.
- Refocus your limited time/budget and personnel on your application security
  - Tool up for moving beyond packet captures and L2/L3 IDS/IPS
- Make sure your security / DFIR folks know how to work with the CSP (this is \*non obvious\* for many of them)

Assuming you followed vendor selection guidance...

---

# *Encryption*

- Do you encrypt in your own data center?
  - Did you do significant due diligence on your CSP?
  - Encryption is not a panacea, but can be a useful mitigation to leaks/breaches/spills
  - Encryption significantly complicates...basically everything at the moment, so be careful in it's use
- 
- 

*Tell me why I'm wrong and we gotta stick to passive sensors...*

*Q&A*

---