



# Cloud Computing Due Diligence - WTF?

Jimmy Blake  
@jimmyblake



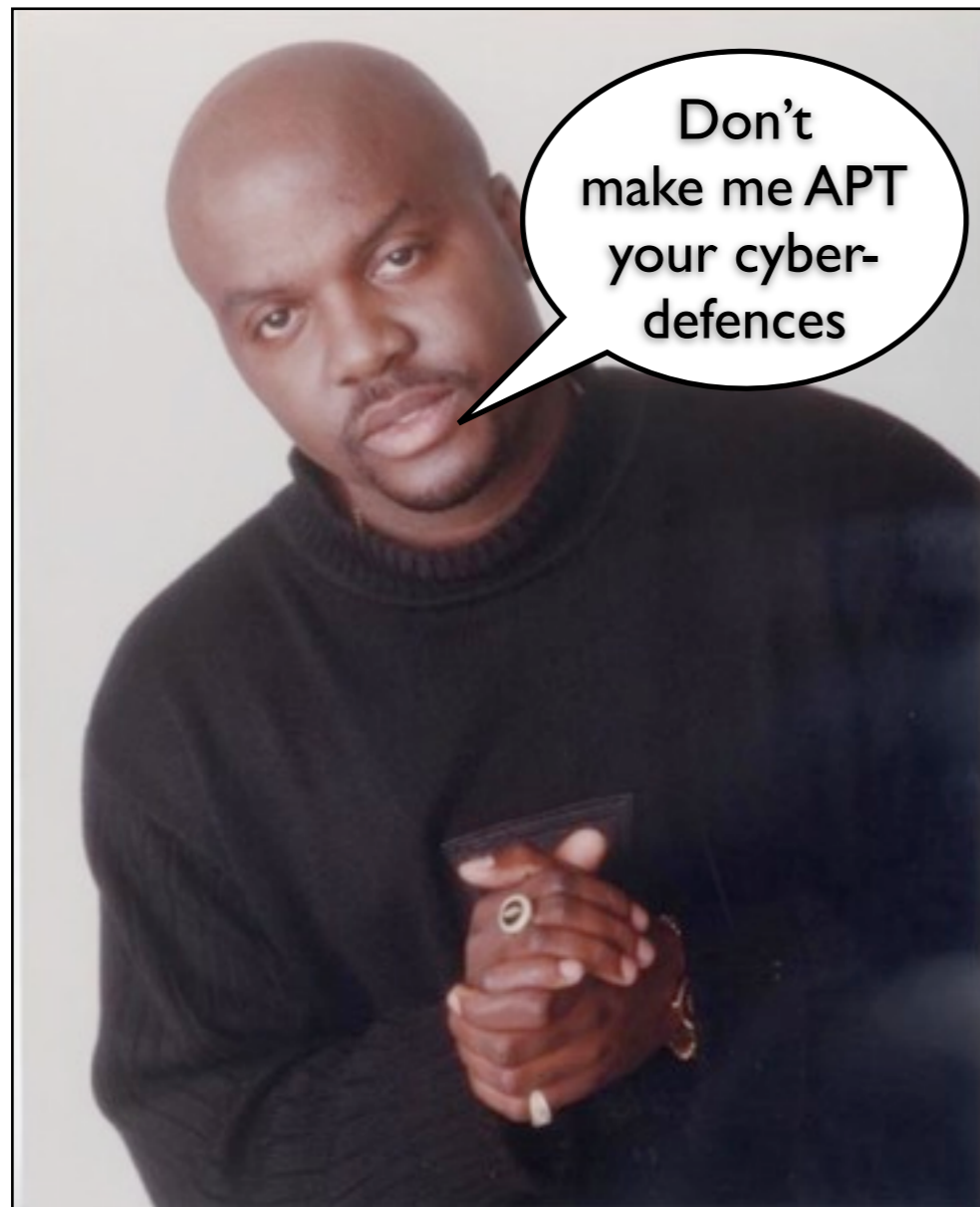
Security B-Sides London: Cloud Computing - WTF?

# Jimmy Who?

- CSO for one of the UK's largest SaaS providers
- Talking mainly from a SaaS perspective
- Dozens of client risk assessments a month
- ISO 27001 Lead Auditor
- These are my opinions, not necessarily those of my employer



# Cloud Computing



Essential Characteristics

Service Model

Deployment Model

...blah blah blah



# Businesses Are Moving to the Cloud



Well governed organisations  
make decisions after  
consideration of risk



# Businesses Are Moving to the Cloud



Well governed organisations make decisions after consideration of risk

...and we all know how many well governed organisations there are out there.



# Who Does the Due Diligence??

- Understands security, not risk
- Knows on-premise, not cloud
- Still thinks he has a secure perimeter
- Likes to be able to hug servers
- He, and his toys, may be displaced by the solution



# The Cost of Due Diligence: Do The Math

Average Due Diligence Questionnaire = 2 hours

Average Audit = 6 man hours

4,000 customers = 3,000 working days per annum

...and you want cost savings???



# Certification: ISO:IEC 27001:2005

- Scope?
  - Very few scopes include production platforms
- Is your acceptable risk < or > then the provider's?



ISO 27001:2005  
IS 512032

IS 245035  
ISO 27001:2005



# ISO 27001: What They Really Mean



**Our On-Premise  
27002 controls**



**Cloud  
Provider's  
27002 controls**



# Certification: SAS-70 (soon SSAE I 6)

- Control Statements
- Great for auditing against SOX 404 controls



# Getting Real

How do you ensure physical access to your data centres is restricted to those who need it for a job function?

By not having 100 customers a day walking through on audits...



# Getting Real

The IT Manager backs up to tape and leaves the tapes in the back of his car overnight.

So I hope that answers your question on how we handle key rotation on our distributed filing system utilising AES 256-bit encryption? Can I ask how you do it at the moment?

The tapes are encrypted of course?

....

Please tell me the car isn't left on his driveway overnight?

....



# Turning the Tables

RFP responses contain a lot of sensitive information

How do you classify completed RFP responses?

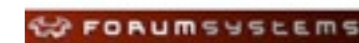
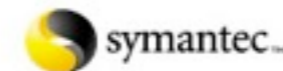
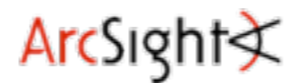
How many people have access to completed RFP responses?

How do you ensure access control and prevent leakage of completed RFP responses?

How do you dispose of printed copies of RFP responses?



# Industry Representation or Prospects?



Security B-Sides London: Cloud Computing - WTF?

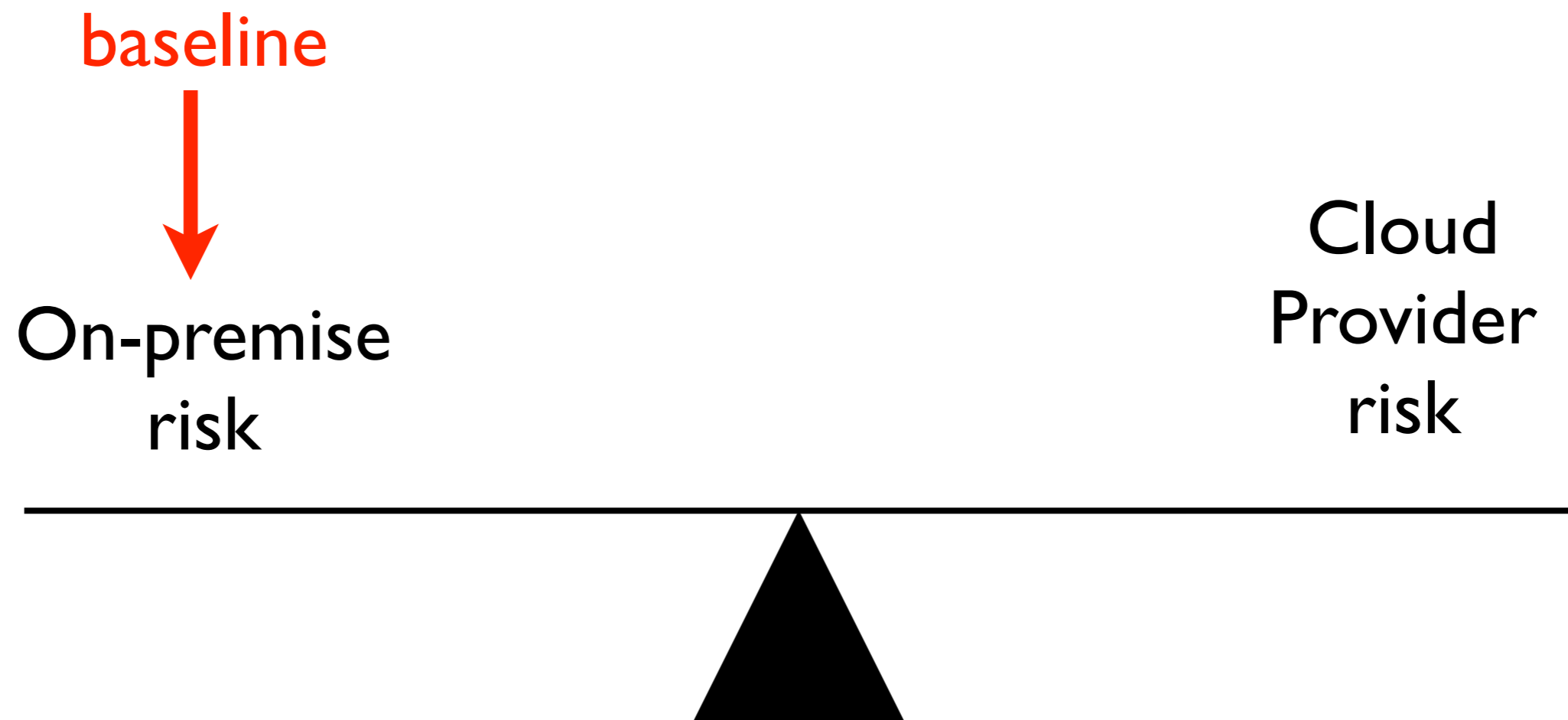
# What We Need

Software-as-a-Service is often about replacing specific on-premise solutions within the business

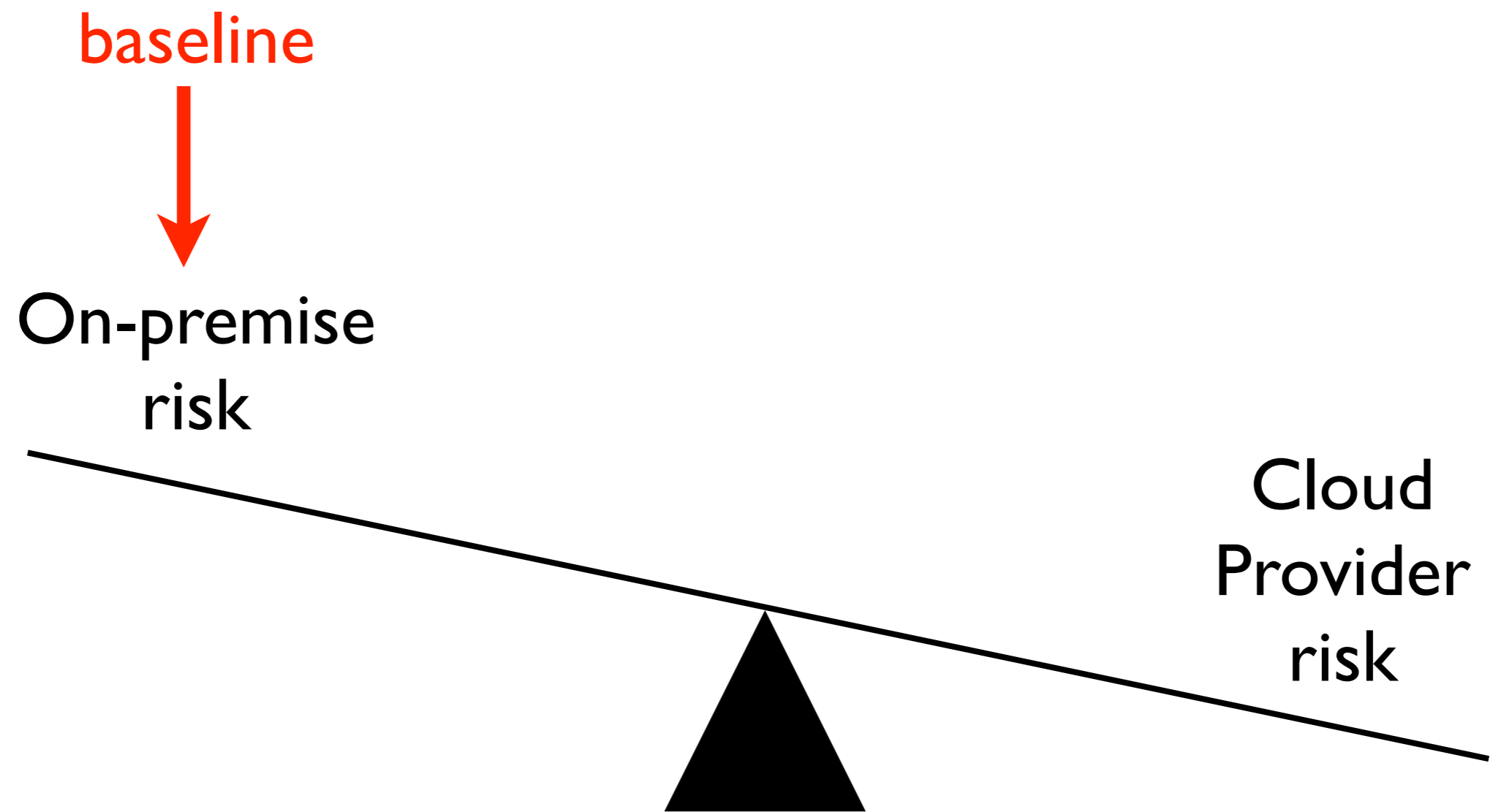


# What We Need

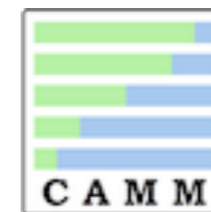
Software-as-a-Service is often about replacing specific on-premise solutions within the business



# What We Need



# What We're Getting



Great, now I've got 6 lots of audit and certification...



Security B-Sides London: Cloud Computing - WTF?

# A Final Plea

## **Customers:**

Baseline on your current risk exposure

Due your due diligence, but make it proportionate

If you want champagne, expect to pay for it

## **Industry Bodies:**

Come together for a unified standard of audit and assessment

Represent cloud customers and the service provider, not infrastructure vendors

## **Cloud Providers:**

Embrace transparency





# Cloud Computing Due Diligence - WTF?

Jimmy Blake  
@jimmyblake

<http://jimmyblake.com>



Security B-Sides London: Cloud Computing - WTF?