Security in knowledge

Control Quotient: Adaptive Strategies For Gracefully Losing Control

David Etue (@djetue)

SafeNet

Joshua Corman (@joshcorman)

Akamai

RSA CONFERENCE 2013

Session ID: GRC-F41

Session Classification: Intermediate

Agenda

- Context
- The Control Quotient
- Today's Reality
- Making it Personal
- Examples
- Transcending "Control"
- Apply

Context

Security in knowledge

Forces of Security Change

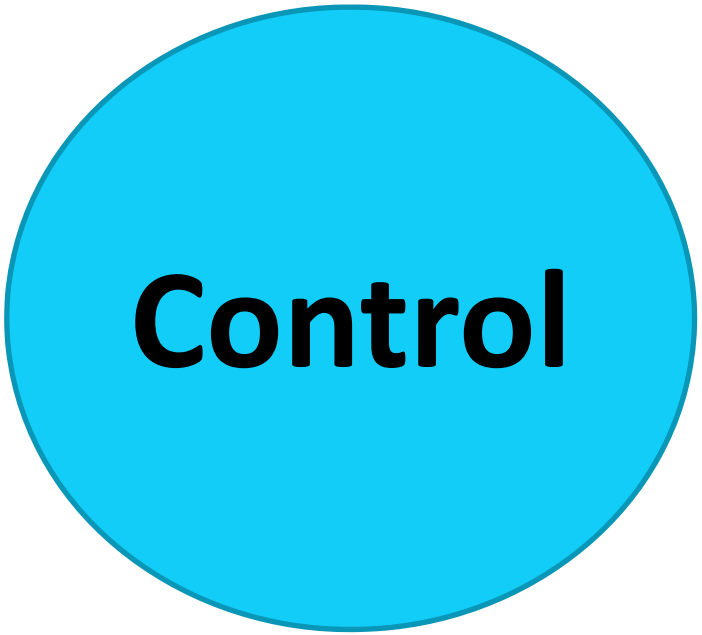
The IT Drunken Bender

The Control Continuum

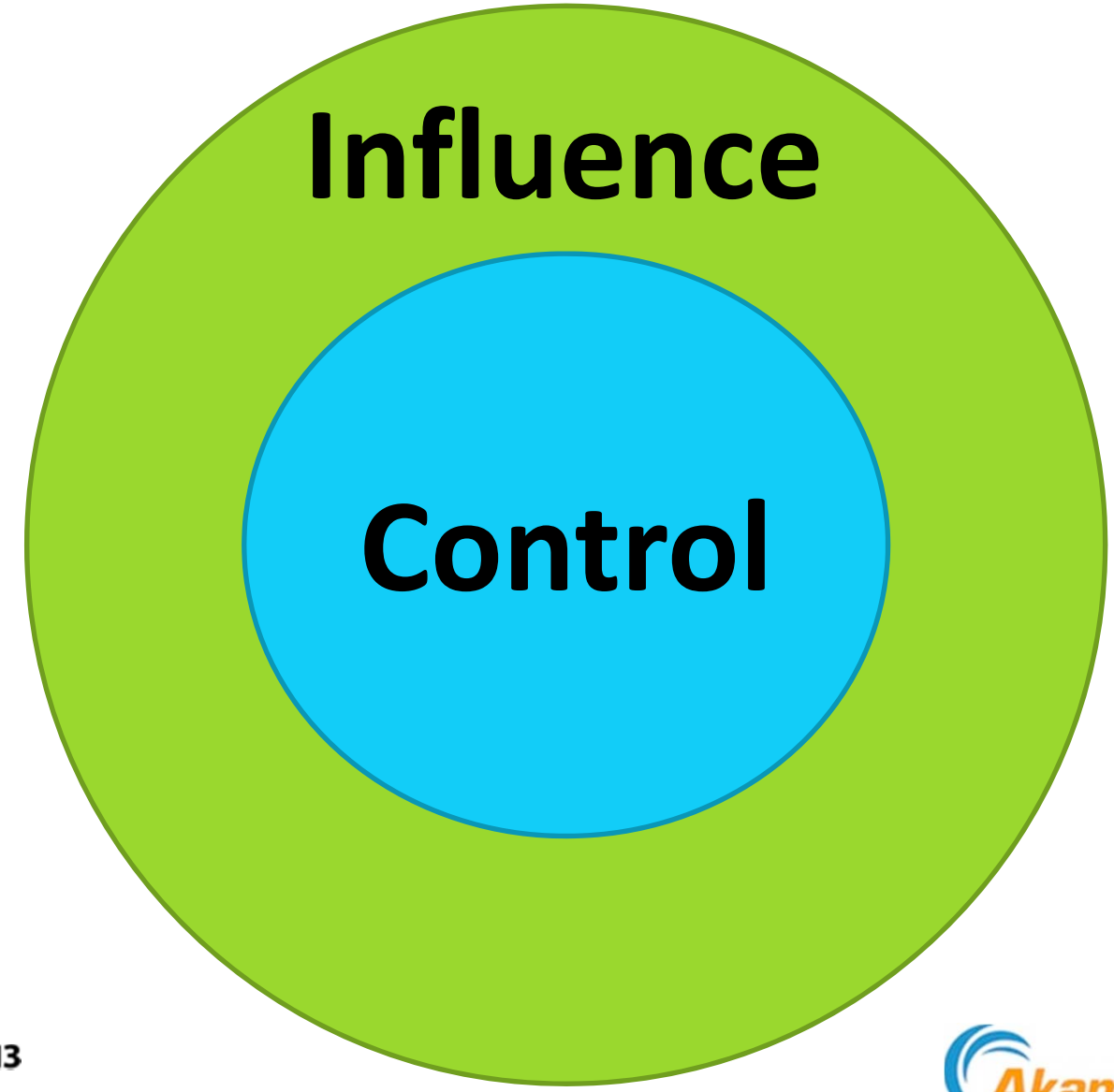
Dictator

Surrender

Sphere of Control



Sphere of Influence vs. Control



InfoSec Serenity Prayer

Grant me the Serenity to accept the things I cannot change;

Transparency to the things I cannot control;

Relevant controls for the things I can;

And the Wisdom (and influence) to mitigate risk appropriately.

The Control Quotient

Security in knowledge

The Control Quotient Definition

- **Quotient:** (from http://www.merriam-webster.com/dictionary/quotient)
  - the number resulting from the division of one number by another
  - the numerical ratio usually multiplied by 100 between a test score and a standard value
  - quota, share
  - **the magnitude of a specified characteristic or quality**

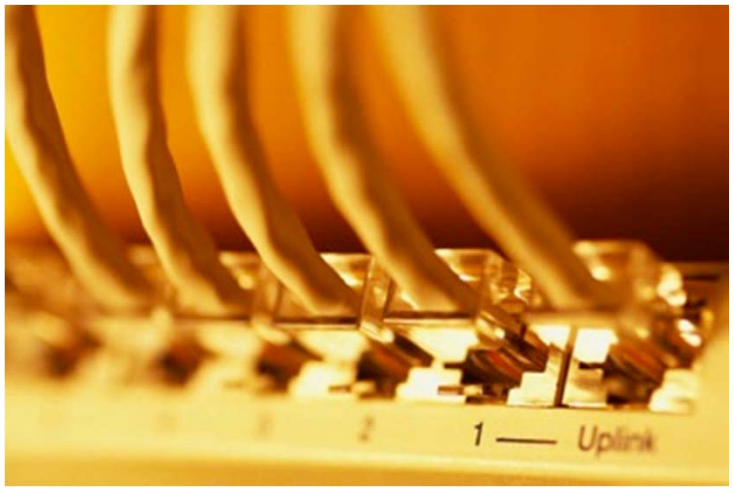
- **Control Quotient: optimization of a security control based on the maximum efficacy within sphere of control (or influence or trust) of the underlying infrastructure***

- *unless there is an independent variable…

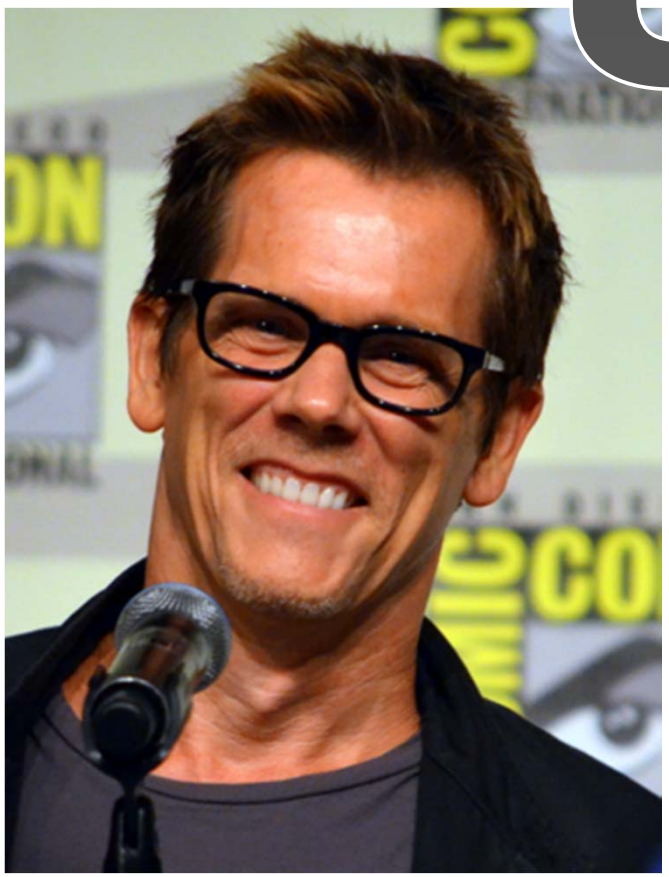
History

- RSA Conference US 2009 P2P
  - An endpoint has a comprehensive, but suspect, view
  - The network has a trustworthy, but incomplete, view

VS.



In Theory There Is An Optimal Place to Deploy a Control…



But Degrees Of Separation Happen….

Avoiding the Proverbial…

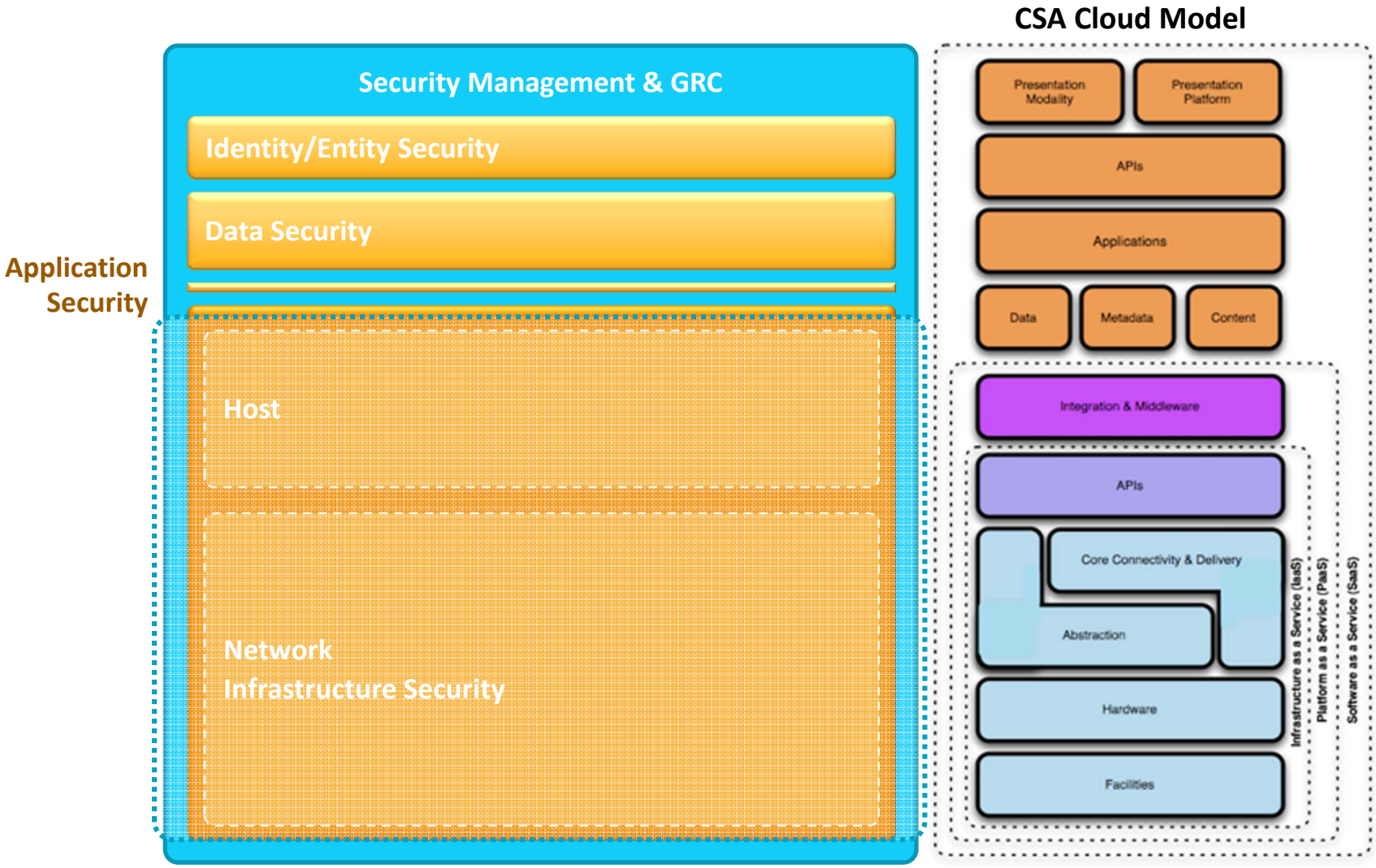
Today's Reality

Security in knowledge

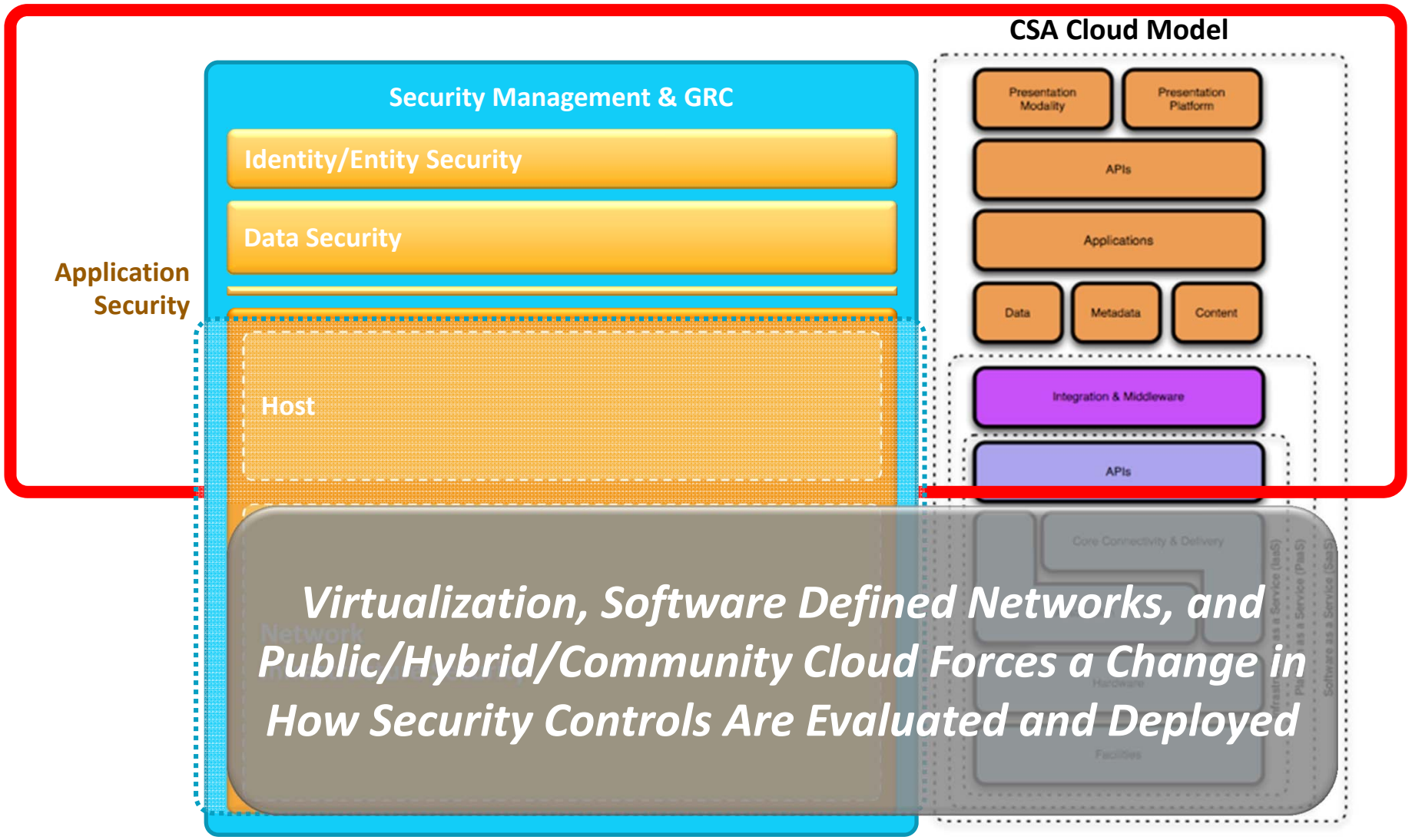
Today's Reality

- Administrative control of entire system is lost
- Increased attack surface
- Abstraction has made systems difficult to assess
- Expectation of anytime-anywhere access from any device

The Control Quotient and the SPI Stack



The Control Quotient and the SPI Stack



Half Full or Half Empty?

To Be Successful, We Must Focus on the Control Kept (or Gained!), NOT the Control Lost…

Controls Gained!!!

- Virtualization and Cloud
  - Asset, Configuration and Change Management
  - Snapshot
  - Rollback
  - Pause
- VDI
  - Asset, Configuration and Change Management
- Mobility
  - Encryption (with containers)
- Software-As-A-Service
  - Logging!

Making It Personal

Security in knowledge

A Parent's Most Valuable Asset?

A Parent's Most Valuable Asset?

Most Valuable Asset?

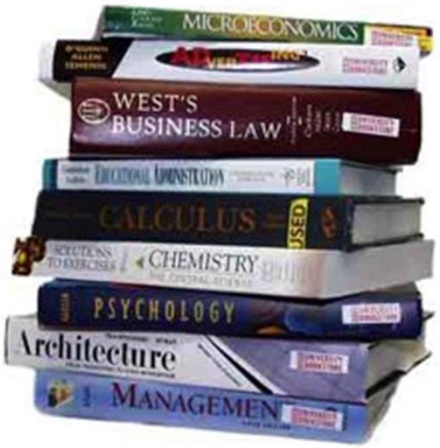
. . . Yet Most Parents Allow Their Kids to Leave Their Control

Choosing Child Care?

naeyc

National Association for the Education of Young Children

American Red Cross



BEST HIGH SCHOOLS U.S.News & WORLD REPORT RANKINGS

SAFE SITTER

Akamai SafeNet

Examples

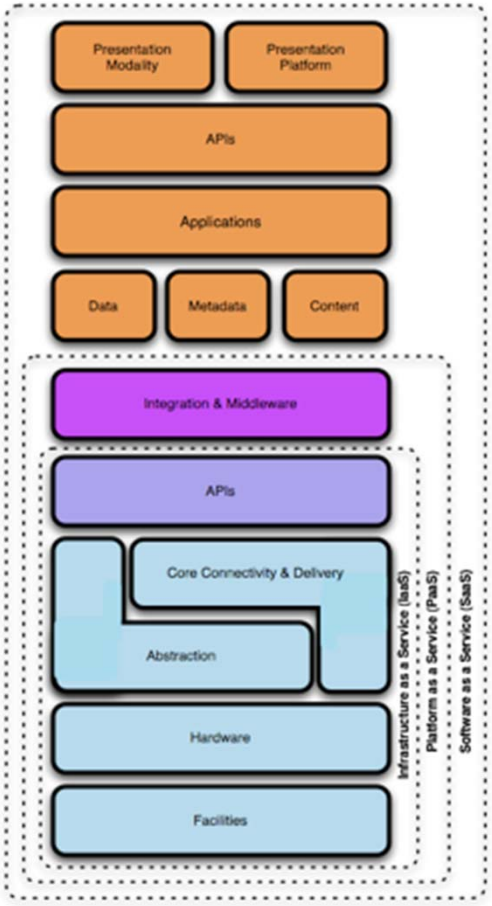
Security in knowledge

Virtualization and Cloud Created An Entire New Definition of Privilege

The Control Quotient and the SPI Stack

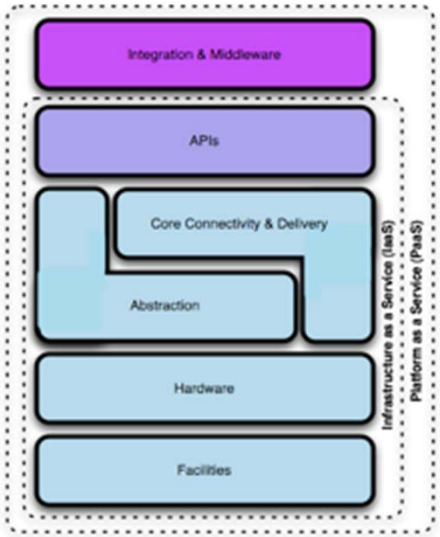
Stack by Chris Hoff -> CSA

Salesforce - SaaS

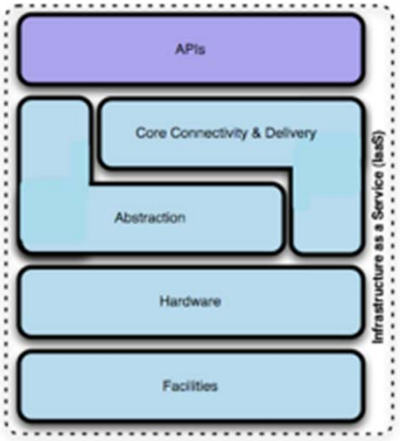


The lower down the stack the Cloud provider stops, the more security **you** are tactically responsible for implementing & managing yourself.

Google AppEngine - PaaS



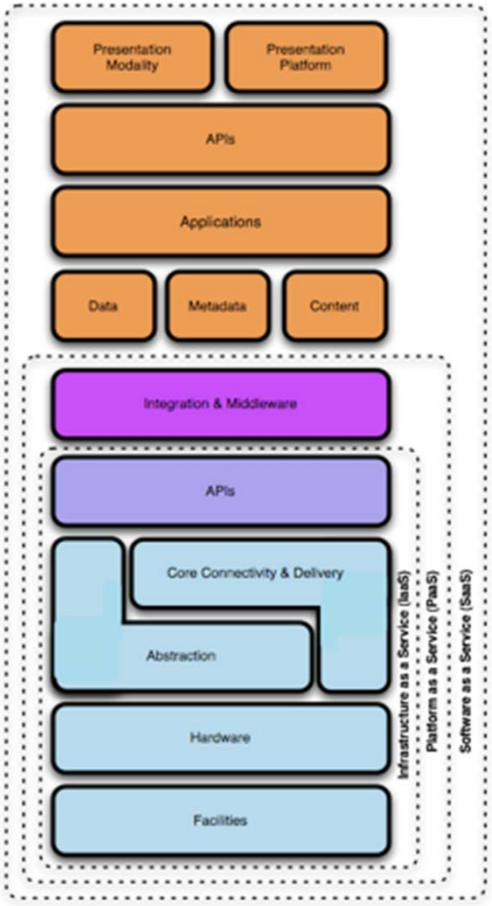
Amazon EC2 - IaaS



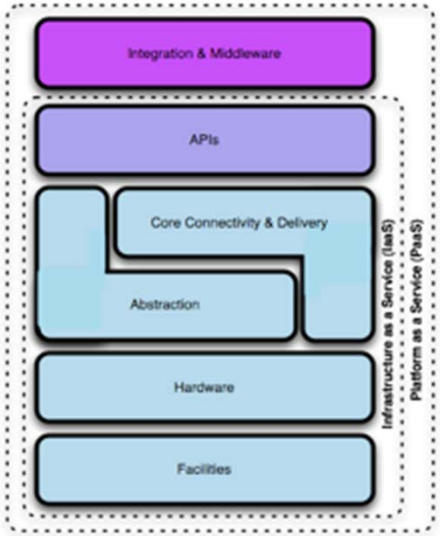
The Control Quotient and the SPI Stack

Stack by Chris Hoff -> CSA

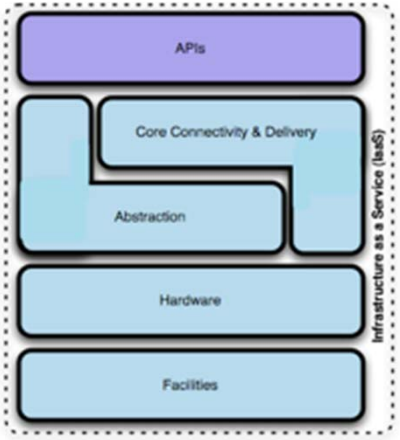
Salesforce - SaaS



Google AppEngine - PaaS



Amazon EC2 - IaaS



Cloud: Who Has Control?

Model	Private Cloud	IaaS in Hybrid / Community / Public Cloud	PaaS/SaaS
Who's Privilege Users?	Customer	**Provider**	**Provider**
Who's Infrastructure?	Customer	**Provider**	**Provider**
Who's VM / Instance?	Customer	Customer	**Provider**
Who's Application?	Customer	Customer	**Provider**
Law Enforcement Contact?	Customer	**Provider**	**Provider**

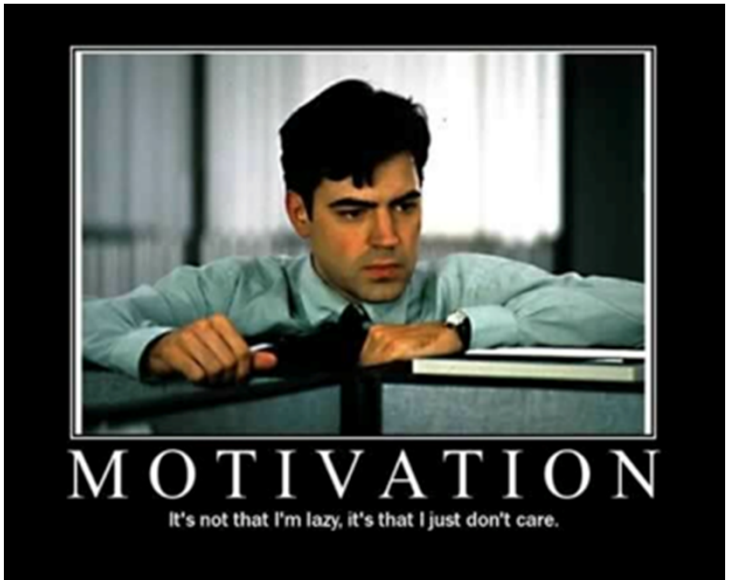
More Than Just Technology…

http://www.flickr.com/photos/markhillary/6342705495

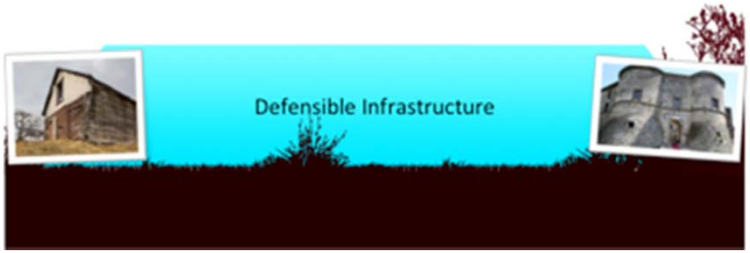
>

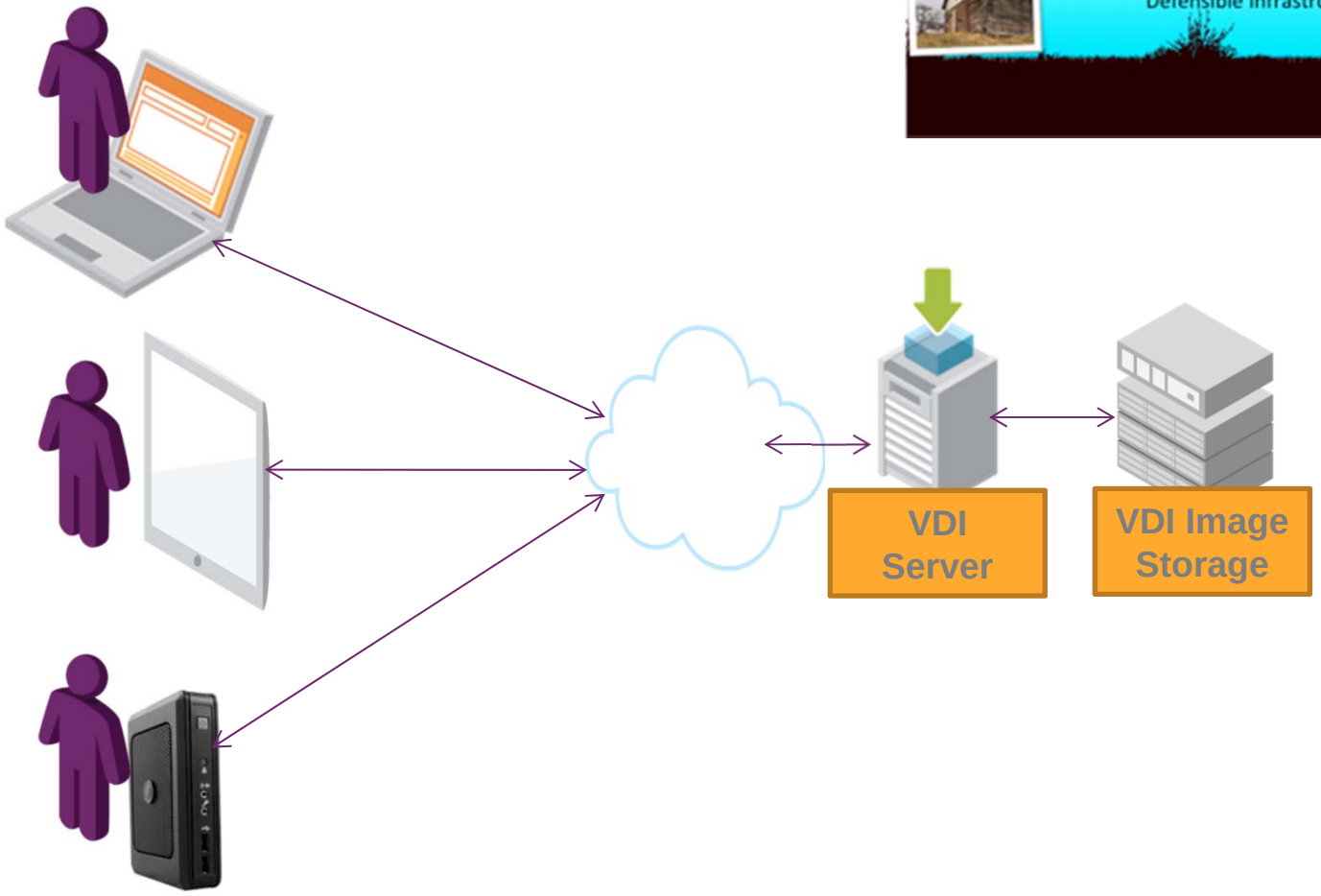
http://www.flickr.com/photos/tallentshow/2399373550

Human Capital



VDI: Centralizing the Desktop?





Mobile

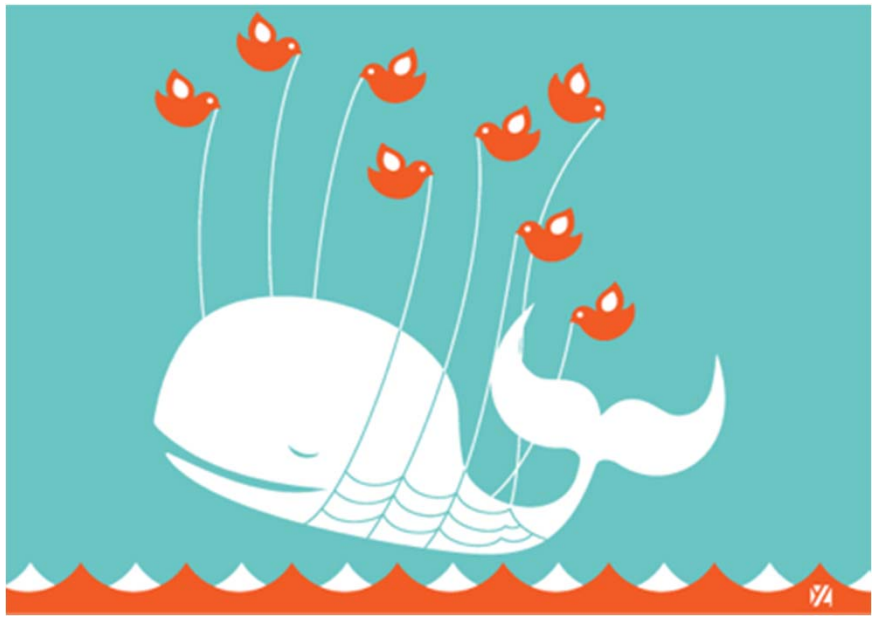
http://www.flickr.com/photos/patrick-allen/4318787860/

Embedded Devices

http://www.sodahead.com/fun/eight...blue-screen.../question-2038989/CachedYou/?slide=2&page=4

Service Providers

Old Ways Don't Work in New World…

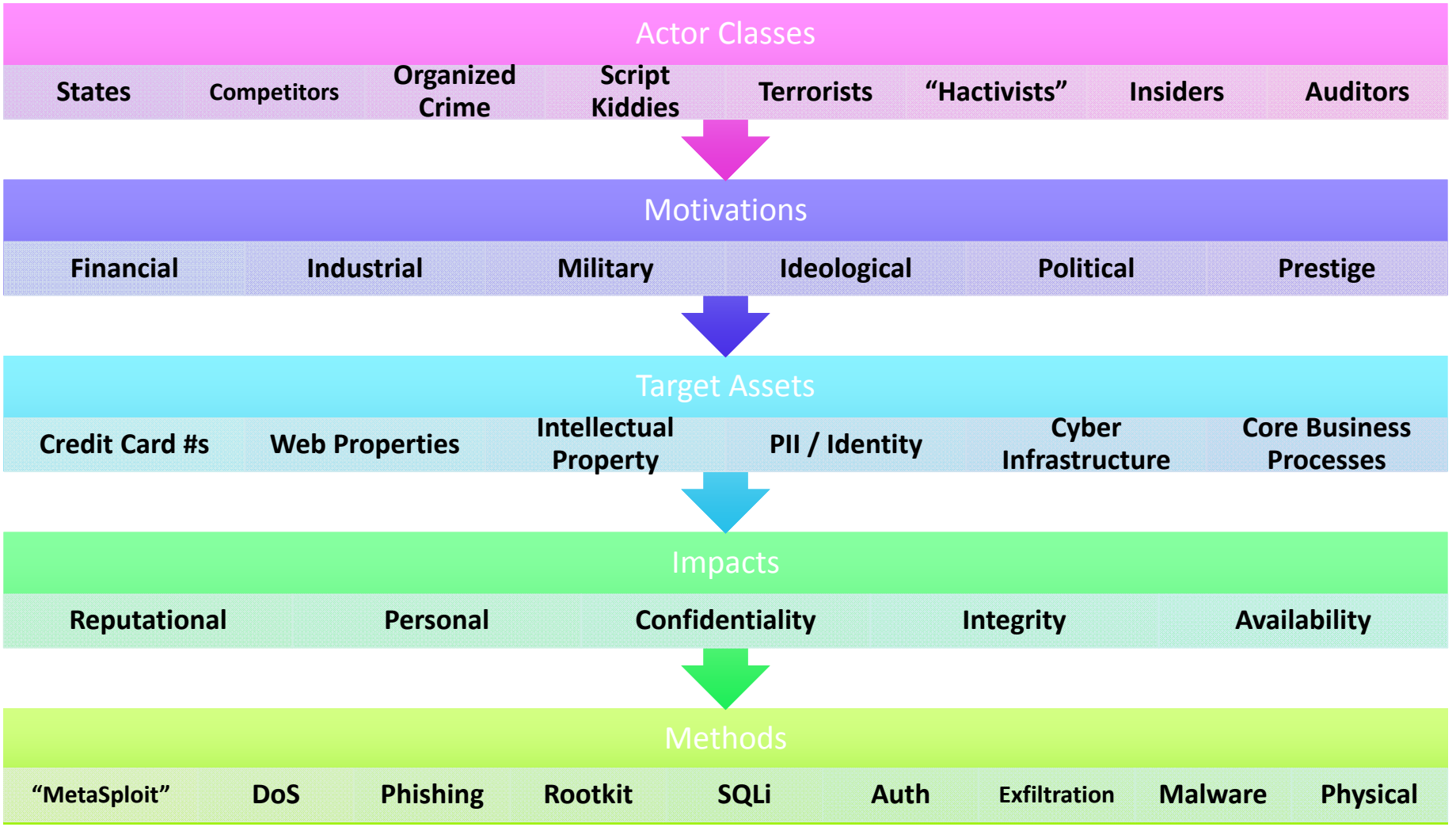


Most organizations are trying to deploy "traditional" security controls in cloud and virtual environments…but were the controls even effective then?

Transcending "Control"

Security in knowledge

A Modern Pantheon of Adversary Classes

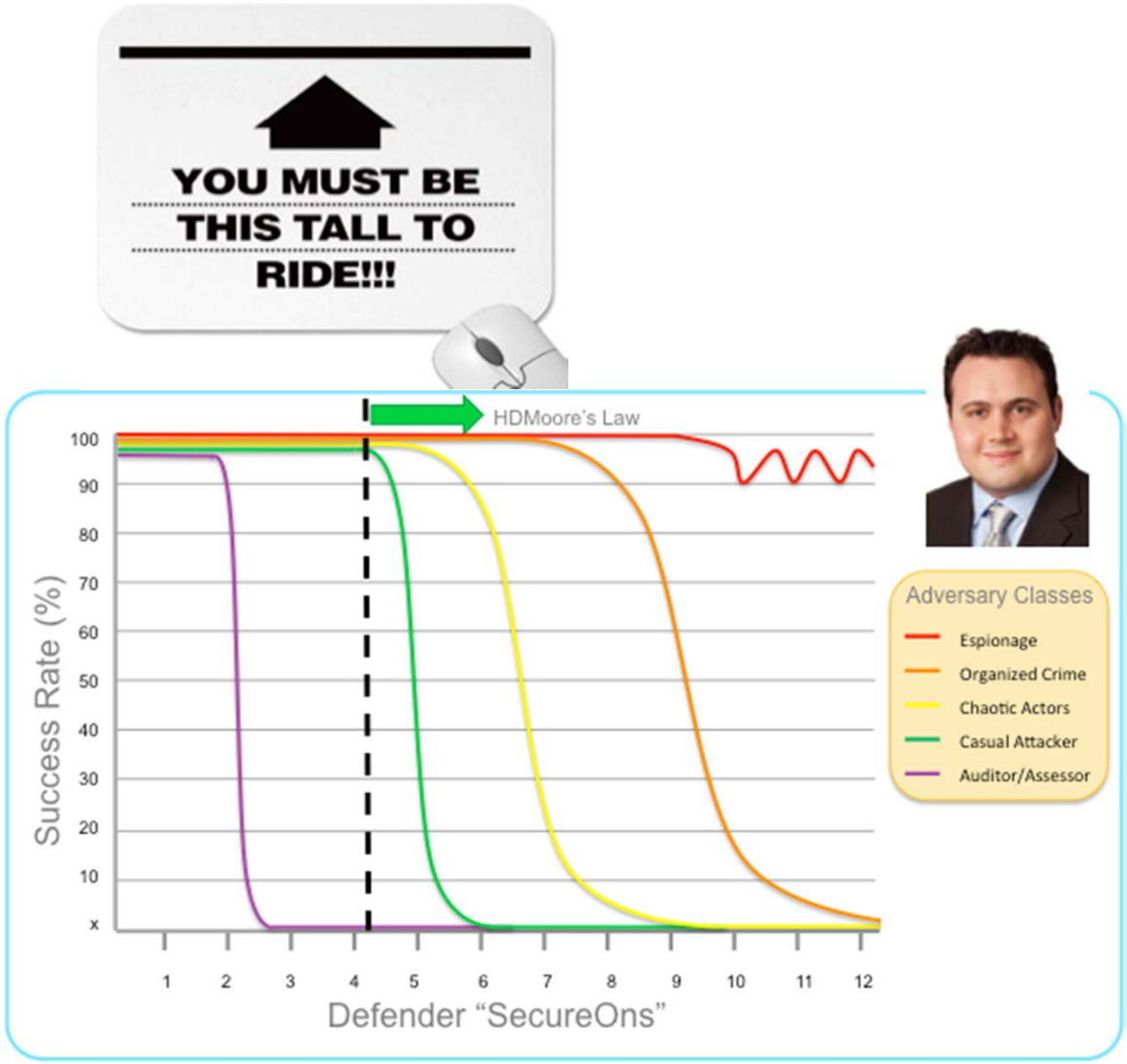


http://www.slideshare.net/DavidEtue/adversary-roi-evaluating-security-from-the-threat-actors-perspective

Akamai SafeNet

HD Moore's Law and Attacker Power

- **Moore's Law:** Compute power doubles every 18 months
- **HDMoore's Law:** Casual Attacker Strength grows at the rate of MetaSploit



http://blog.cognitivedissidents.com/2011/11/01/intro-to-hdmoores-law/

Akamai SafeNet

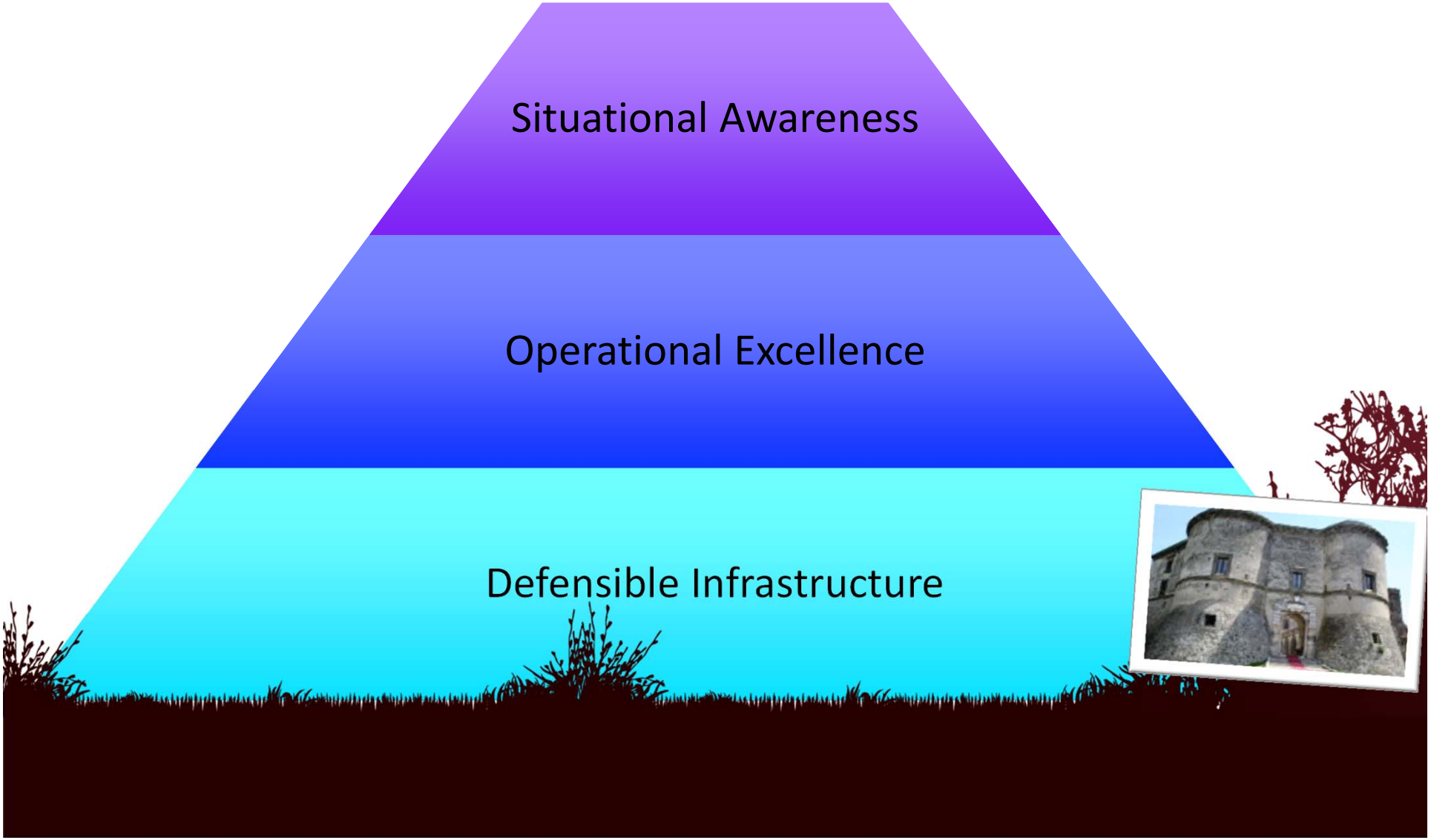
Defensible Infrastructure

Gene Kim

MULTIPLE AWARD-WINNING CTO, RESEARCHER, VISIBLE OPS CO-AUTHOR, ENTREPRENEUR & FOUNDER OF TRIPWIRE

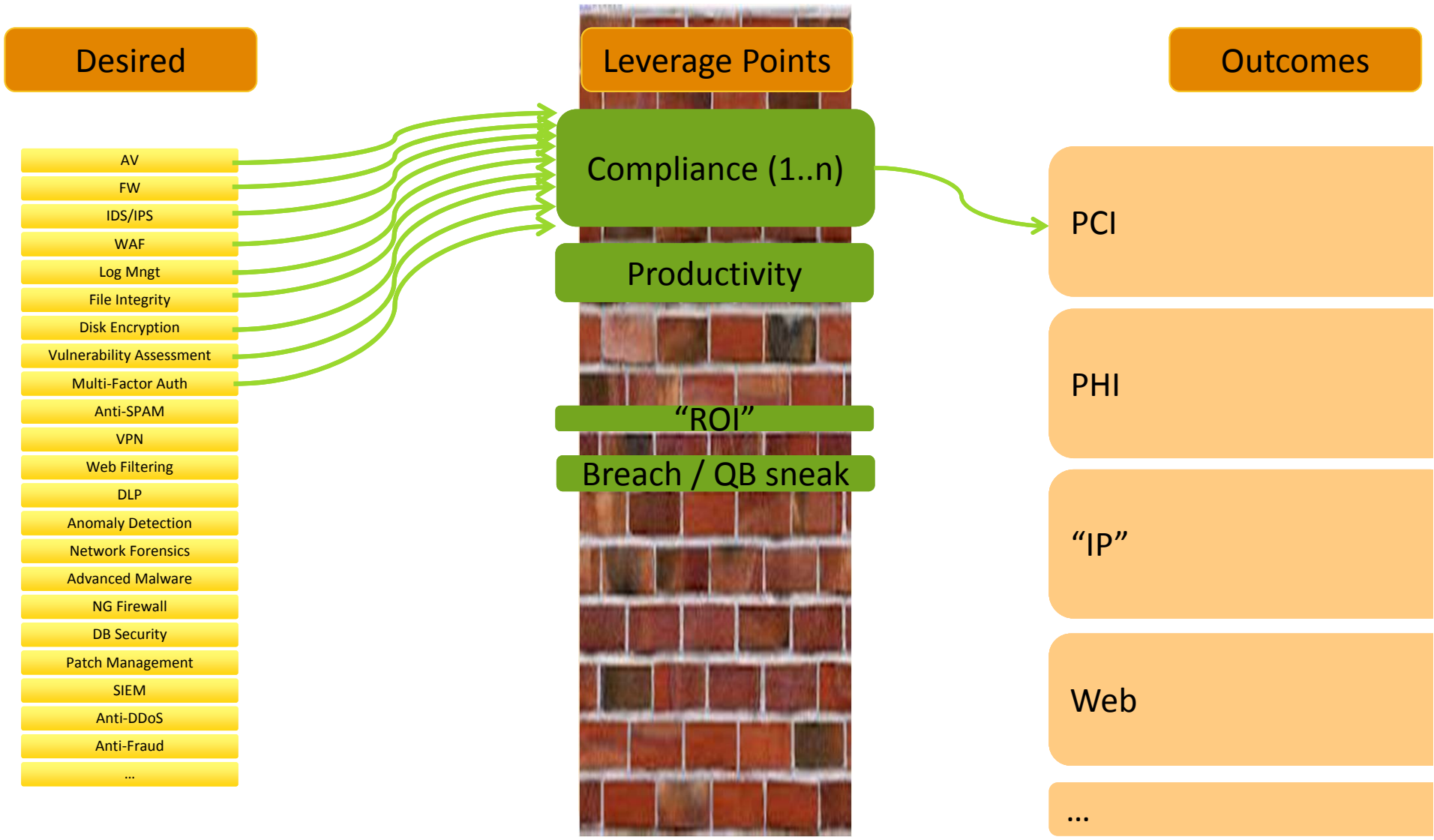
Operational Excellence

Defensible Infrastructure

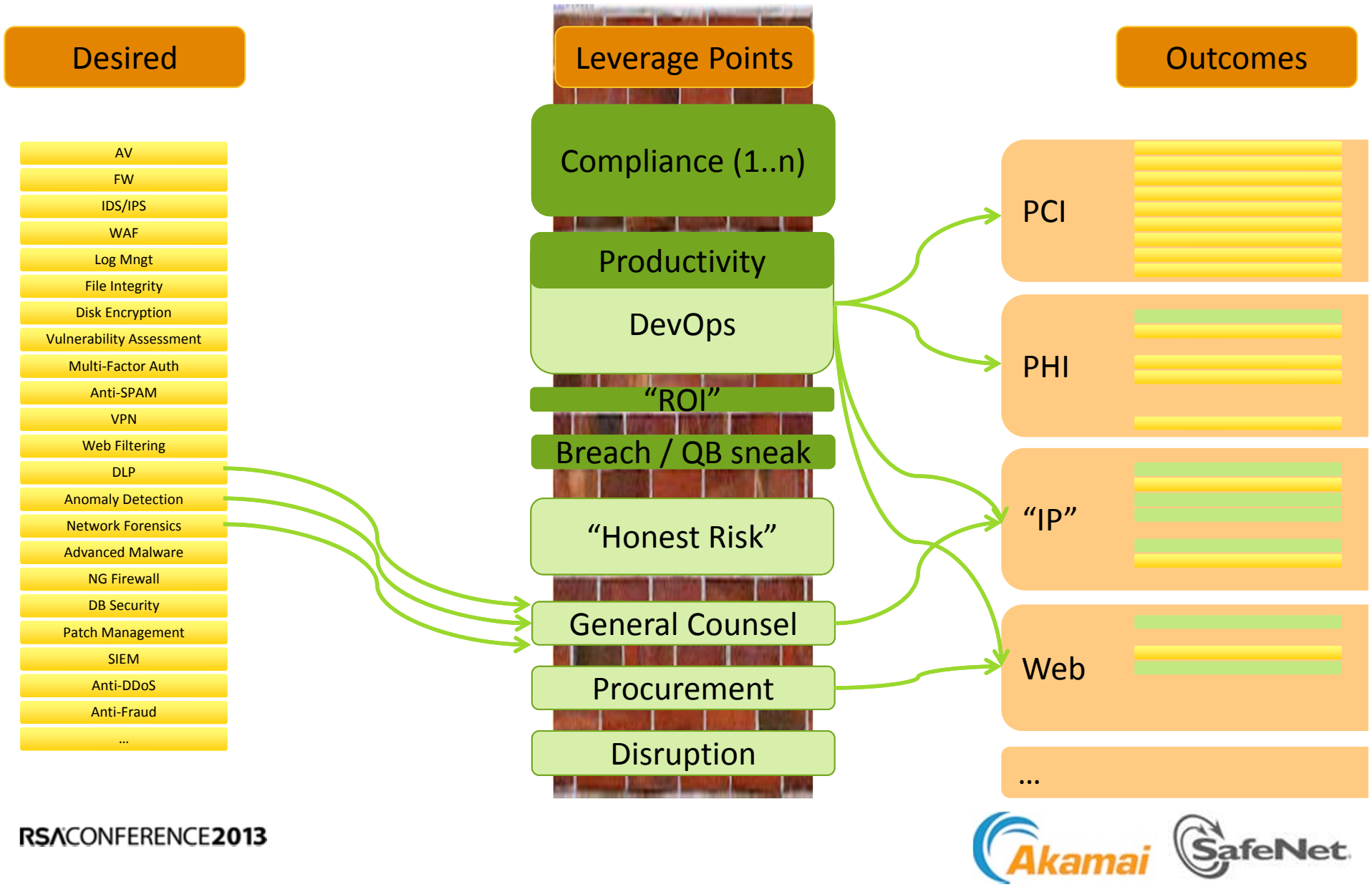

Situational Awareness
Operational Excellence
Defensible Infrastructure


Countermeasures
Situational Awareness
Operational Excellence
Defensible Infrastructure

Control "Swim Lanes"



Control & Influence "Swim Lanes"



Under-tapped Researcher Influence

Desired

- AV
- FW
- IDS/IPS
- WAF
- Log Mngt
- File Integrity
- Disk Encryption
- Vulnerability Assessment
- Multi-Factor Auth
- Anti-SPAM
- VPN
- Web Filtering
- DLP
- Anomaly Detection
- Network Forensics
- Advanced Malware
- NG Firewall
- DB Security
- Patch Management
- SIEM
- Anti-DDoS
- Anti-Fraud
- …

- Litigation
- Legislation
- Open Source
- Hearts & Minds
- Academia

Leverage Points

- Compliance (1..n)
- Productivity
- DevOps
- "ROI"
- Breach / QB sneak
- "Honest Risk"
- General Counsel
- Procurement
- Disruption

Outcomes

- PCI
- PHI
- "IP"
- Web
- …

Potential Independent Variables

Encryption

- with good key management…

Rootkits

- well, rootkits for good…

Intermediary Clouds

- Anti-DDoS, WAF, Message/Content, Identity, etc…

Identity and Access Management

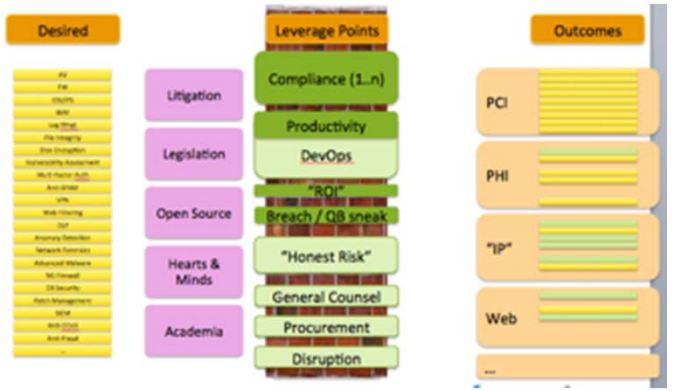
- with proper integration and process support

Software-As-A-Service (SaaS)

- *if* the provider harnesses the opportunity

APPLY!

- Identify at least one opportunity to leverage a new swim lane



- Identify one opportunity this year to influence each layer of the Pyramid

- Leverage a control gained!
- Leverage the Rugged Handbook (ruggedsoftware.org)

Security in knowledge

Thank You!

David Etue (@djetue)

SafeNet

Joshua Corman (@joshcorman)

Akamai

RSA CONFERENCE 2013

Session ID: GRC-F41

Session Classification: Intermediate

About Joshua Corman @joshcorman

- Director of Security Intelligence for Akamai Technologies
  - Former Research Director, Enterprise Security [The 451 Group]
  - Former Principal Security Strategist [IBM ISS]

- Industry:
  - Faculty: The Institute for Applied Network Security (IANS)
  - 2009 NetworkWorld Top 10 Tech People to Know
  - Co-Founder of "Rugged Software" www.ruggedsoftware.org
  - BLOG: www.cognitivedissidents.com

- Things I've been researching:
  - Compliance vs Security
  - Disruptive Security for Disruptive Innovations
  - Chaotic Actors
  - Espionage
  - Security Metrics

Akamai SafeNet

About David Etue @djetue

- VP, Corporate Development Strategy at SafeNet
  - Former Cyber Security Practice Lead [PRTM Management Consultants] (now PwC)
  - Former VP Products and Markets [Fidelis Security Systems]
  - Former Manager, Information Security [General Electric Company]

- Industry:
  - Faculty: The Institute for Applied Network Security (IANS)
  - Leads Washington Relations for Cyber Security Forum Initiative
  - Certified Information Privacy Professional (CIPP/G)

- Cyber things that interest me:
  - Adversary innovation
  - Social media security
  - Applying intelligence cycle / OODA loop in cyber
  - Supply chain security