Are We Getting Better?

Why We Don't Know.
What We Can Do About It.

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

- Things I've been researching:
  - DevOps
  - Security Intelligence
  - Chaotic Actors
  - Espionage
  - Security Metrics

A Personal Bit…

Passionate
Purposeful
Principled
Protector
Provider

Honest

Courageous

Consequential

Unreasonable
A Fool

Are We Getting Better…

No

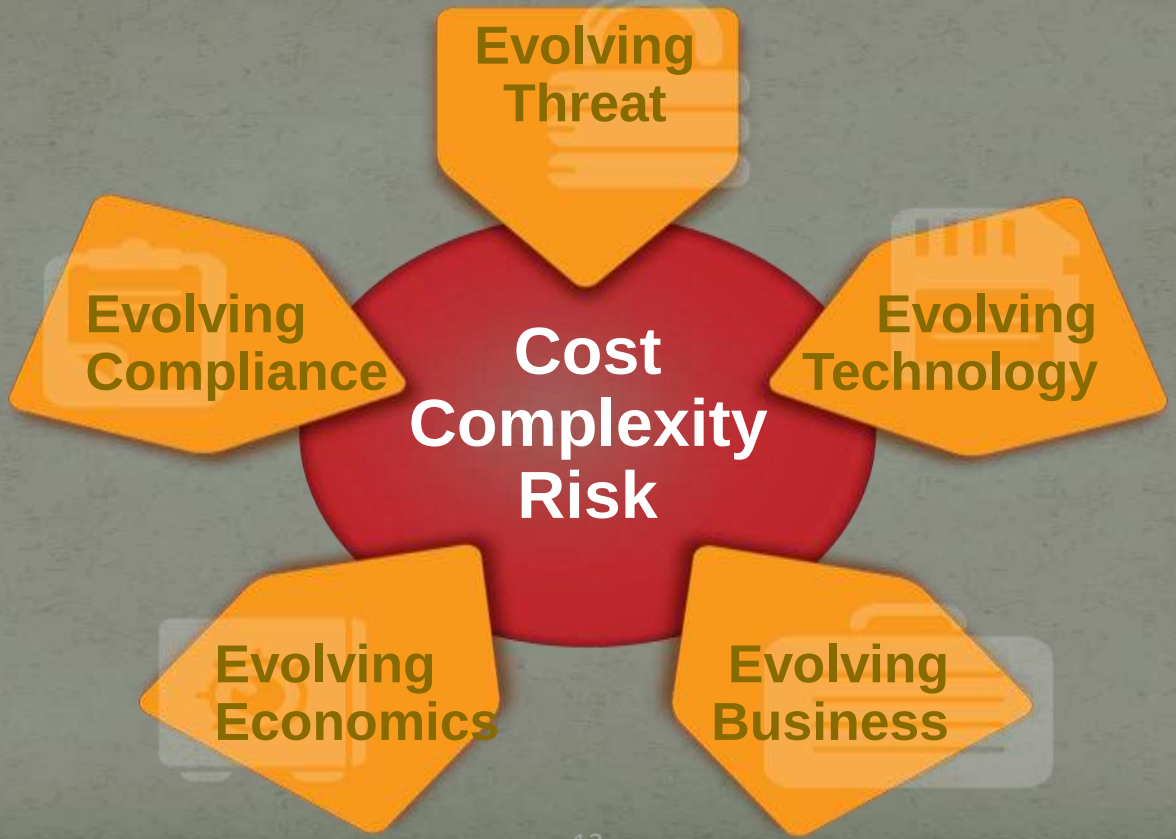
Is it getting better?

Or do you feel the same?

Will it make it easier
on you now?
You got someone to
blame...

How would you know?
By which criteria?

Constant Change



Why It Matters…

http://www.ted.com/talks/simon_sinek_how_great_leaders_inspire_action.html

Consequences: Value & Replaceability

http://blog.cognitivedissidents.com/2011/10/24/a-replaceability-continuum/

Performance

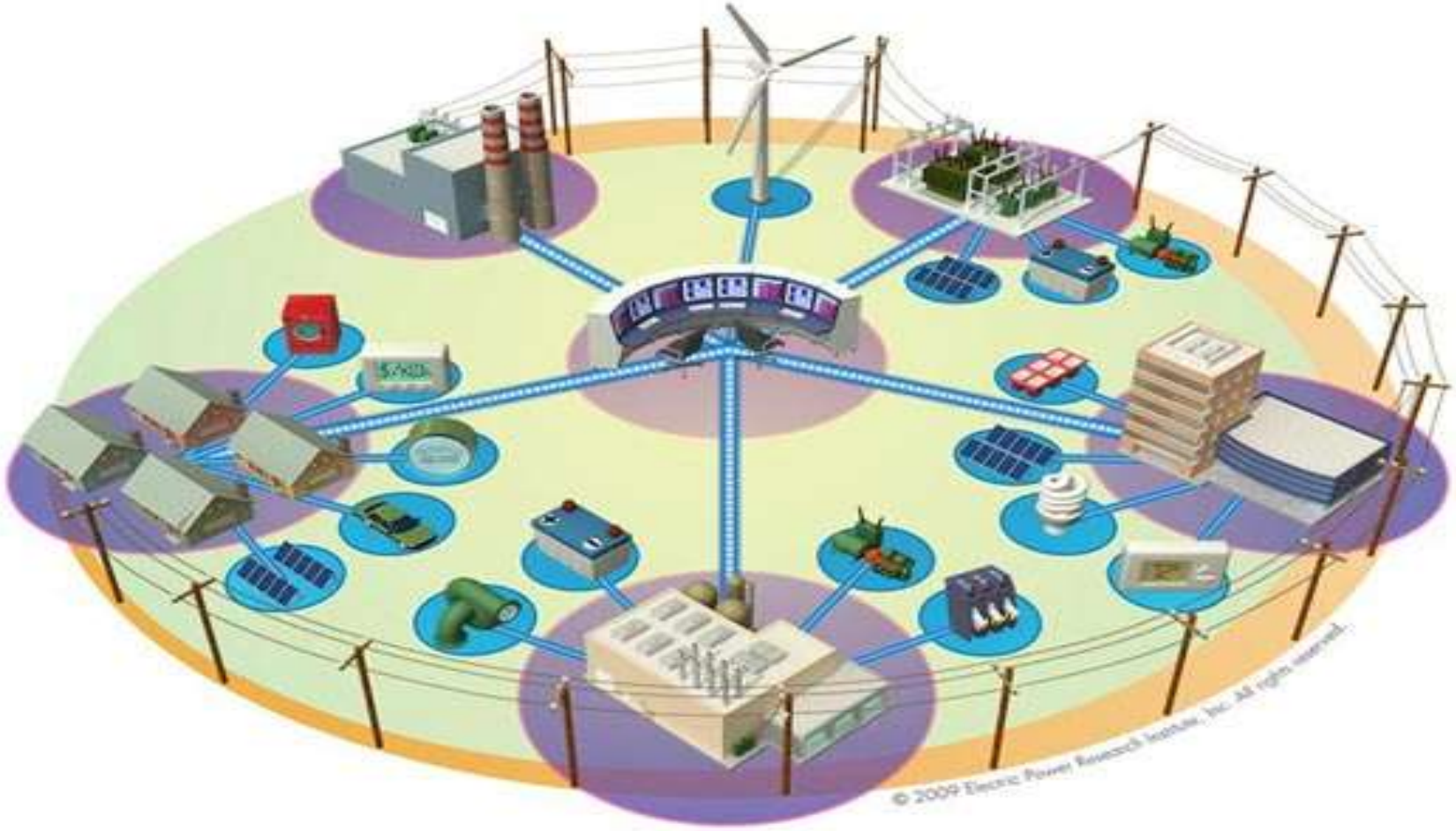
Fungible Assets

IntellectualProperty & TradeSecrets

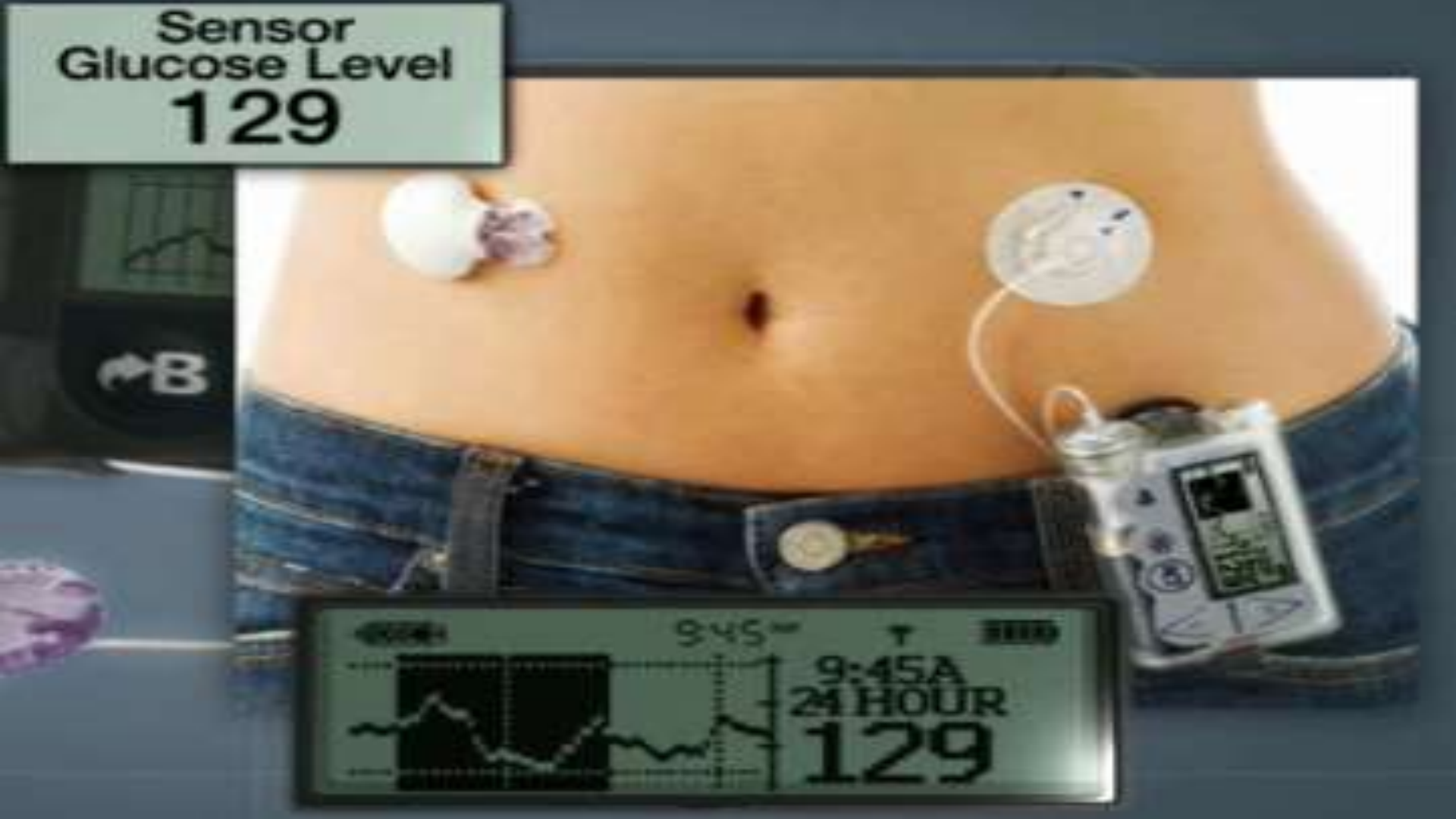
Rights & Civility

Safety & Human Life

Dependence


© 2009 Electric Power Research Institute, Inc. All rights reserved.

Ford
P R N D M
21 Alt Nation
Rock
Blazing Laze


Sensor
Glucose Level
129
B
9:45
9:45A
24 HOUR
129

Consider...

s/Software/Vulnerability/

Consider...

s/Connected/Exposed/

Consider…

Our challenges are not technical… but cultural

Activity Effect

Symptoms

Root Causes

Easy

Important

80/20

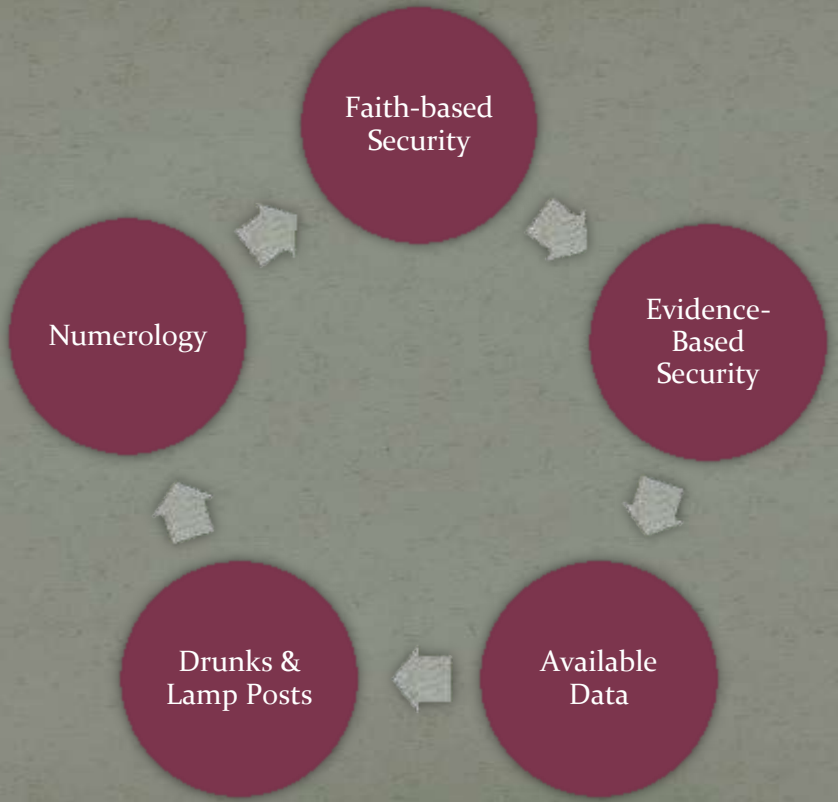
Best Practices

aren’t

Good Enough

isn’t

Why?


Faith-based Security
Evidence-Based Security
Available Data
Drunks & Lamp Posts
Numerology

Incentives

I still haven't found...

...what I'm looking for...

HERE BE DRAGONS

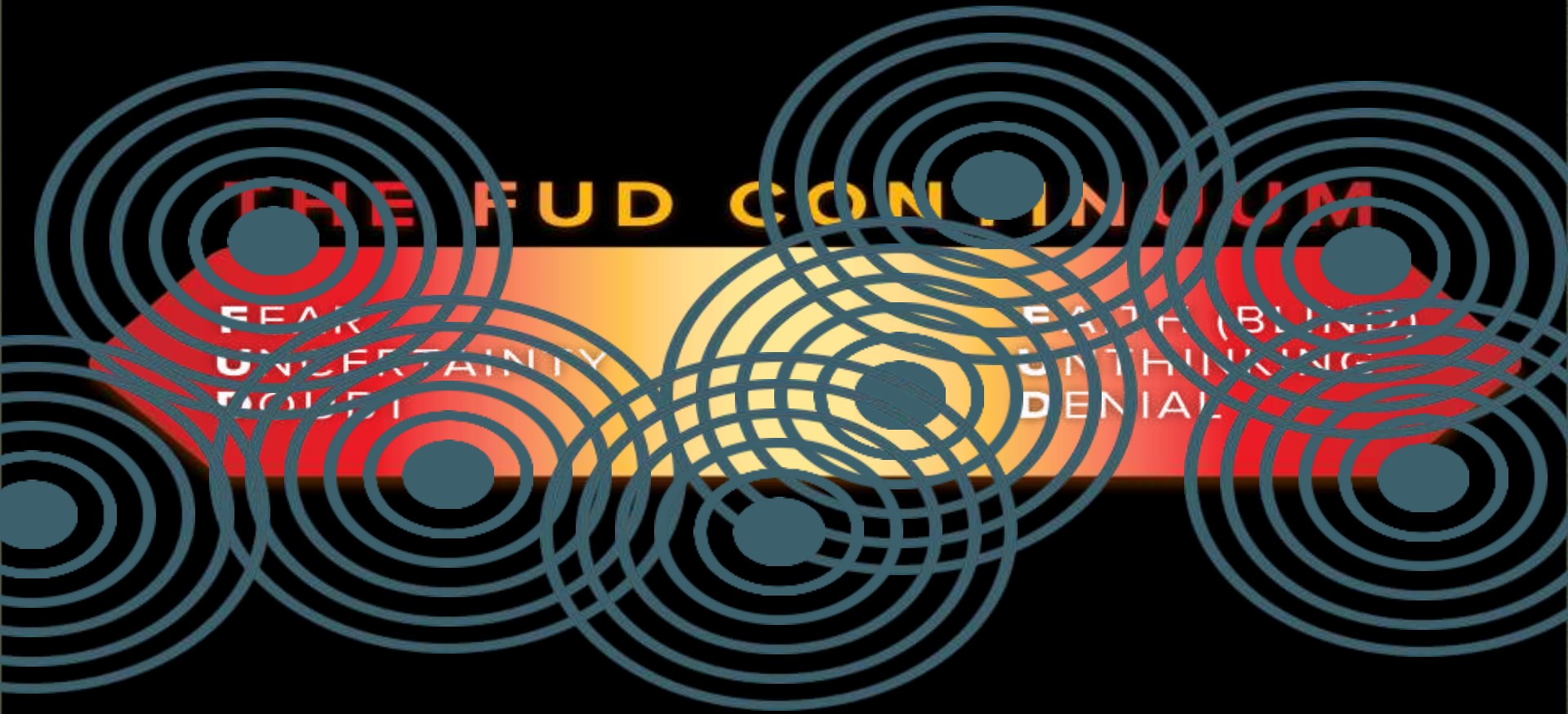
“7” Dirty Secrets of the Security Industry

0) *“Vendors don’t need to be Ahead of the Threat…*
…just Ahead of the Buyer”

1) AV Certification Omissions
2) There is no Perimeter… [nor Santa Claus]
3) Risk Management Threatens Vendors
4) Psst… There is more to Risk than Weak Software
5) Compliance Threatens Security…
6) Vendor Blind Spots Allowed for Storm++
7) Security has grown well past “Do it yourself”

RUGGED SOFTWARE

fsck the FUD & the Echo Chamber



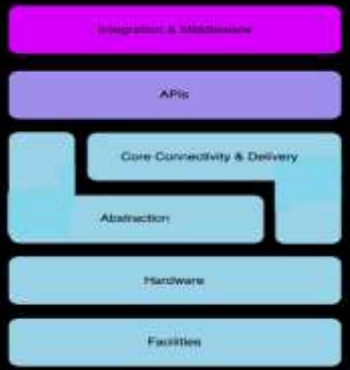
Game Changers: Virt/Cloud/Deperim...

Salesforce - SaaS

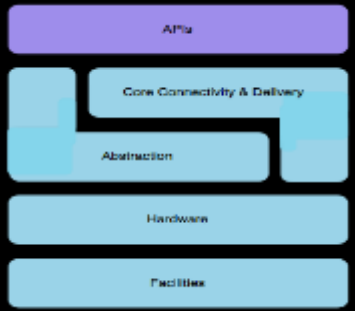
with Chris Hoff and solo talks

models by Chris Hoff

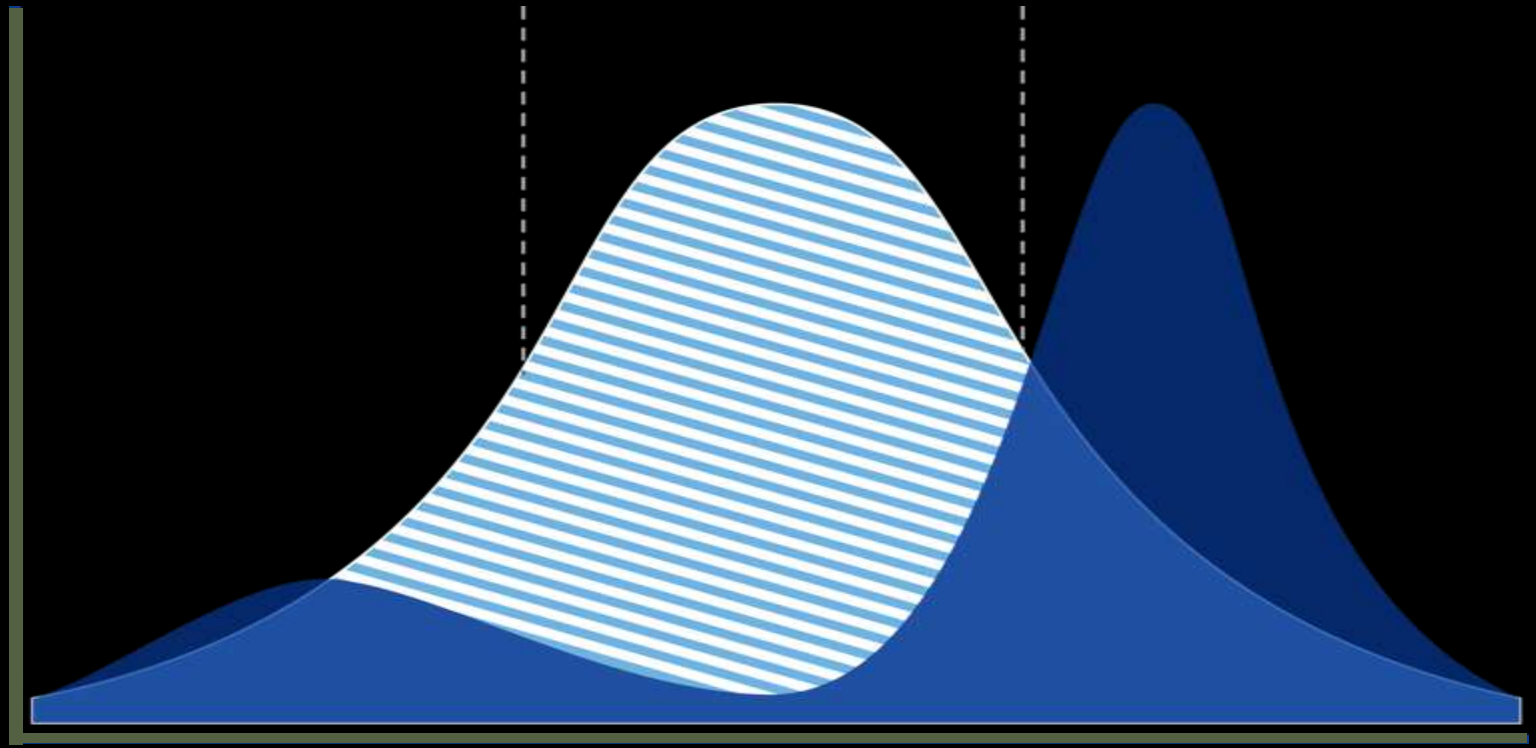
Google AppEngine - PaaS



Amazon EC2 - IaaS



Is PCI the No Child Left Behind Act

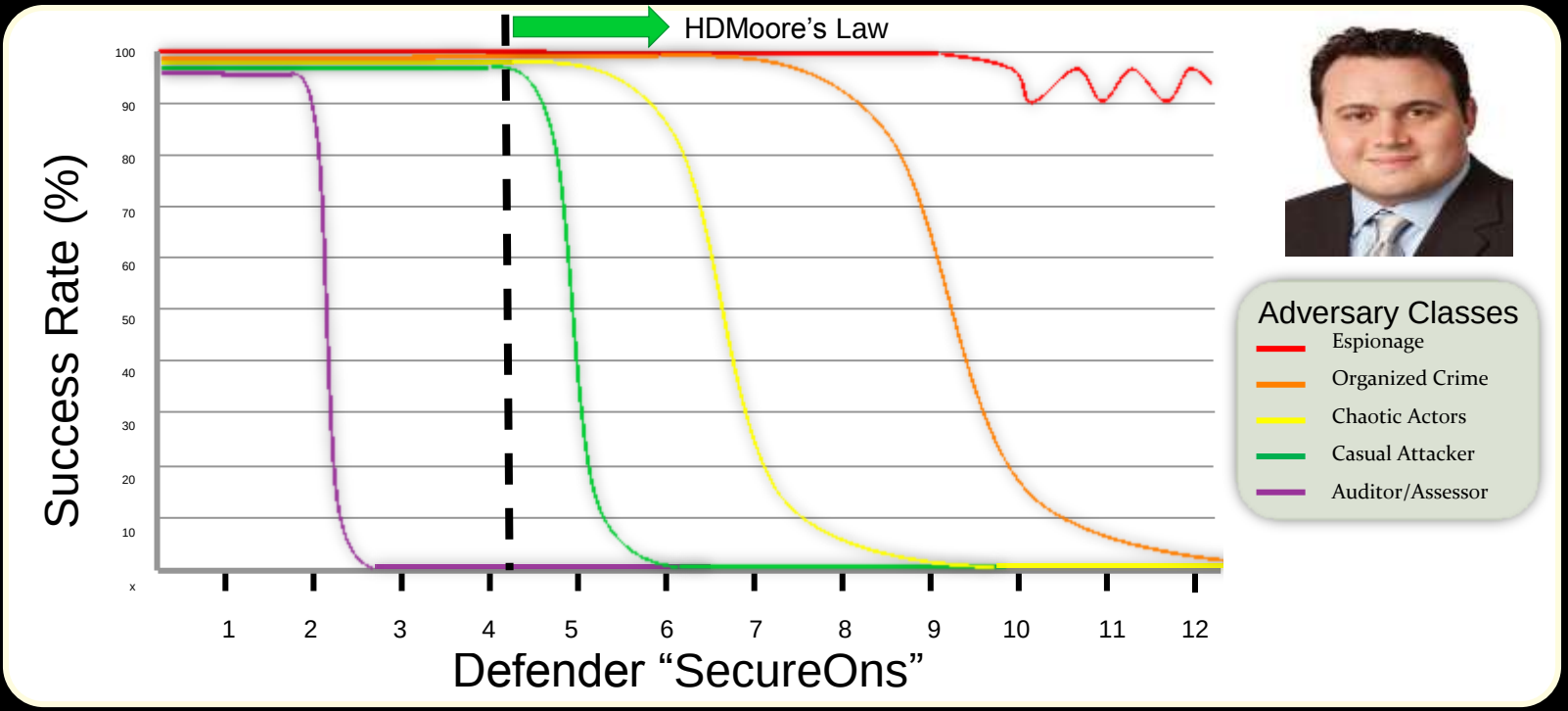


alice
&
bob

SECBURNOUT.ORG

—MAR—

HDMoore's Law



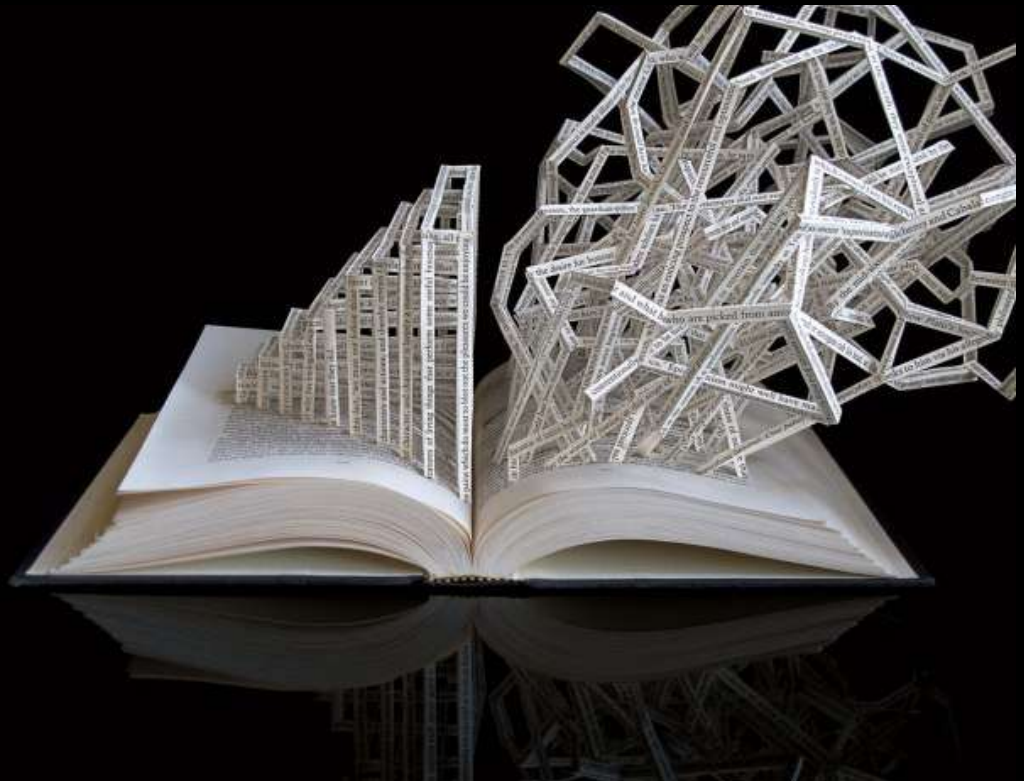
http://blog.cognitivedissidents.com/2011/11/01/intro-to-hdmoores-law/

Adversary Centric

Rugged DevOps: IT @ Ludicrous Speed!

Control and Chaos

"World War 3.0" by Michael Joseph Gross
Vanity Fair - May 2012



Josh Corman & Jericho

BruCON 2012

What you can do about it…

Pick one:

- Make Excuses
- Make Progress

Defensible Infrastructure

Operational Excellence

Defensible Infrastructure

Situational Awareness

Operational Excellence

Defensible Infrastructure

Countermeasures

Situational Awareness

Operational Excellence

Defensible Infrastructure

Knowledge Seeker
Zombie Killer

Experimentation

An untested hypothesis is a wish

FORTINET
Where The World Talks Security

YOU KIDS
GET OUT
OF MY INDUSTRY

Unreasonable Fool

THANK YOU
My Collaborators
My Teammates

Joshua Corman

[Knowledge Seeker | Zombie Killer]

Twitter: @joshcorman
BLOG: http://blog.cognitivedissidents.com