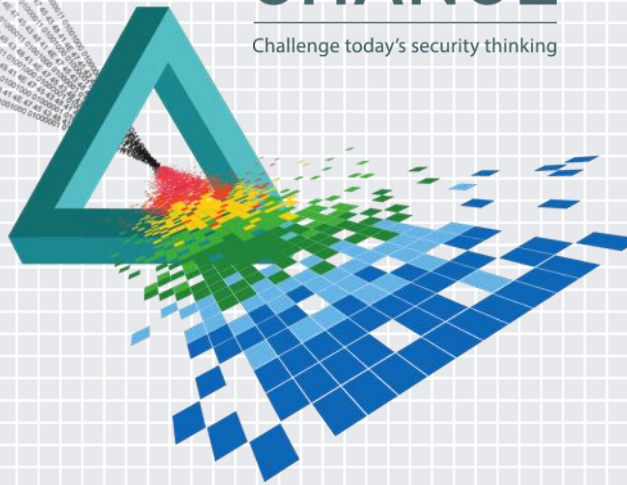
RSAConference2015
San Francisco | April 20-24 | Moscone Center

CHANGE
Challenge today's security thinking

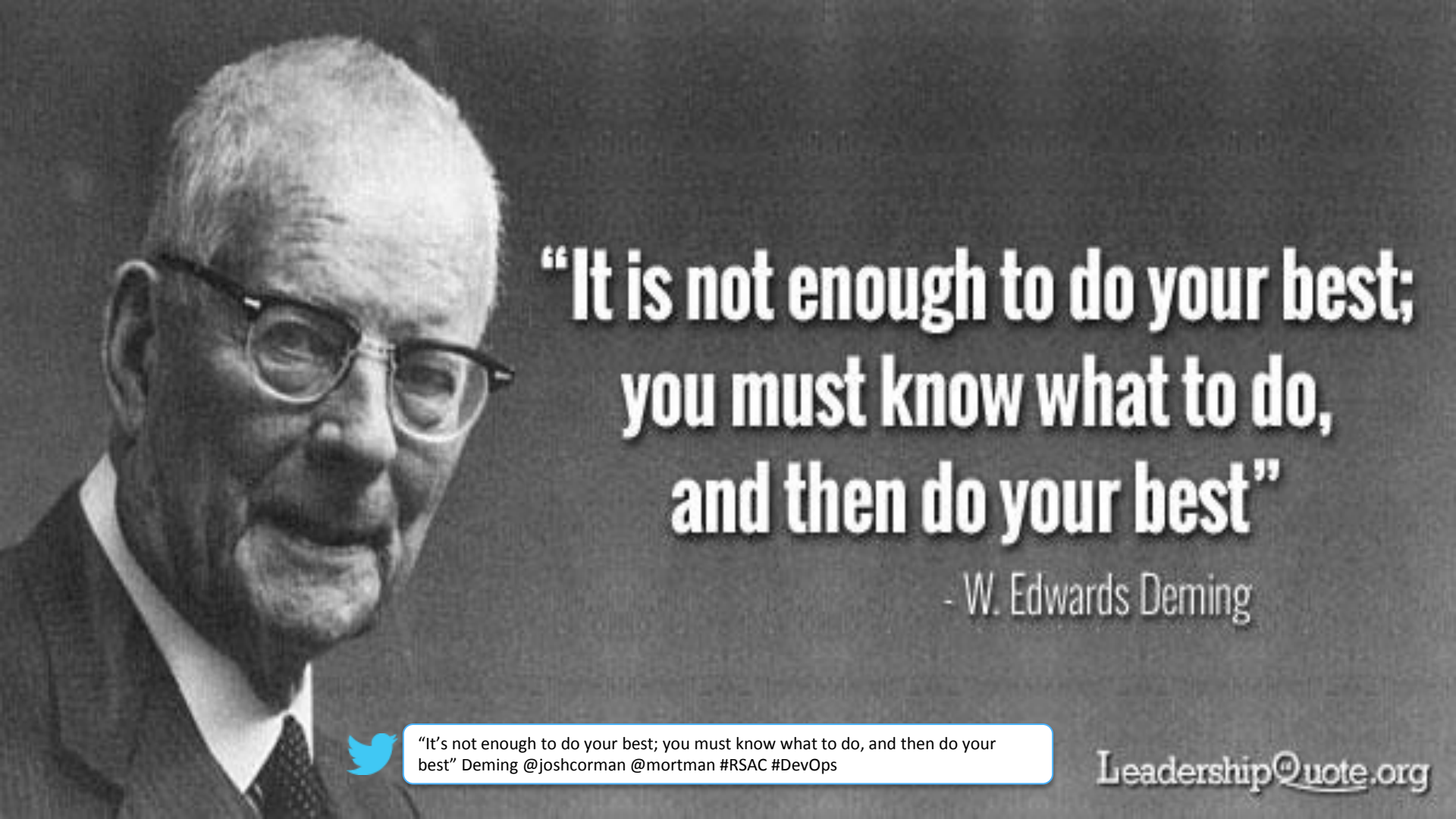


SESSION ID: **ASD-T07R**

Continuous Security: 5 Ways DevOps *Improves* Security

David Mortman
Chief Security Architect & Distinguished Engineer
Dell Software
@mortman

Joshua Corman
CTO
Sonatype
@joshcorman


"It is not enough to do your best;
you must know what to do,
and then do your best"
- W. Edwards Deming
"It's not enough to do your best; you must know what to do, and then do your best" Deming @joshcorman @mortman #RSAC #DevOps
LeadershipQuote.org

ON TIME	ON BUDGET	ACCEPTABLE QUALITY/RISK

Dev's core motivations are to be OnTime, OnBudget, w/ Acceptable Quality/Risk
@joshcorman @mortman #RSAC #DevOps


“Don’t Go Chasin’ Waterfalls” Dev started w/ Waterfall, but modern demands require us to go faster @joshcorman @mortman #RSAC #DevOps

ON TIME. Faster builds. Fewer interruptions. More innovation. 	ON BUDGET. More efficient. More profitable. More competitive. 	ACCEPTABLE QUALITY/RISK. Easier compliance. Higher quality. Built-in audit protection. 

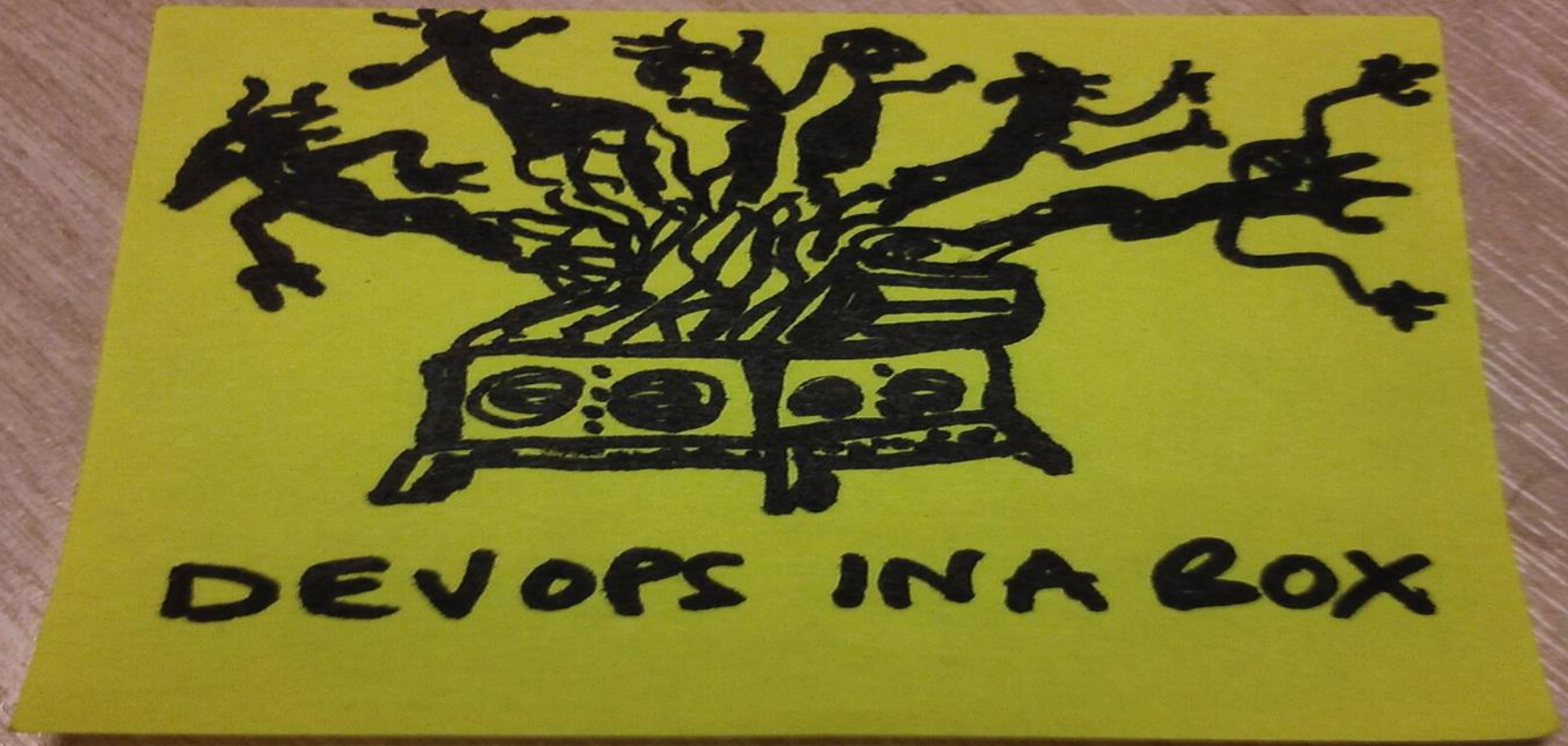
Waterfall's Design -> Dev -> Test -> Deploy may go 1.5-3yrs b/w releases.
@joshcorman @mortman #RSAC #DevOps

Agile goats; not goat rodeo. “We need to be agile, but not fragile.” @RuggedSoftware @joshcorman @mortman #RSAC #DevOps

ON TIME. Faster builds. Fewer interruptions. More innovation. 	ON BUDGET. More efficient. More profitable. More competitive. 	ACCEPTABLE QUALITY/RISK. Easier compliance. Higher quality. Built-in audit protection. 
Agile / CI		

#RSAC
@mortman
@joshcorman

Agile & Lean tightened Design -> Build -> Test cycle releasing 6-12+ smaller batches/yr @joshcorman @mortman #RSAC #DevOps



It may feel like DevOps is Pandora's Box, but it's open… and hope remains. ;)
@joshcorman @mortman #RSAC #DevOps

ON TIME. Faster builds. Fewer interruptions. More innovation.	ON BUDGET. More efficient. More profitable. More competitive.	ACCEPTABLE QUALITY/RISK. Easier compliance. Higher quality. Built-in audit protection.
Agile / CI DevOps / CD		

#RSAC
@mortman
@joshcorman

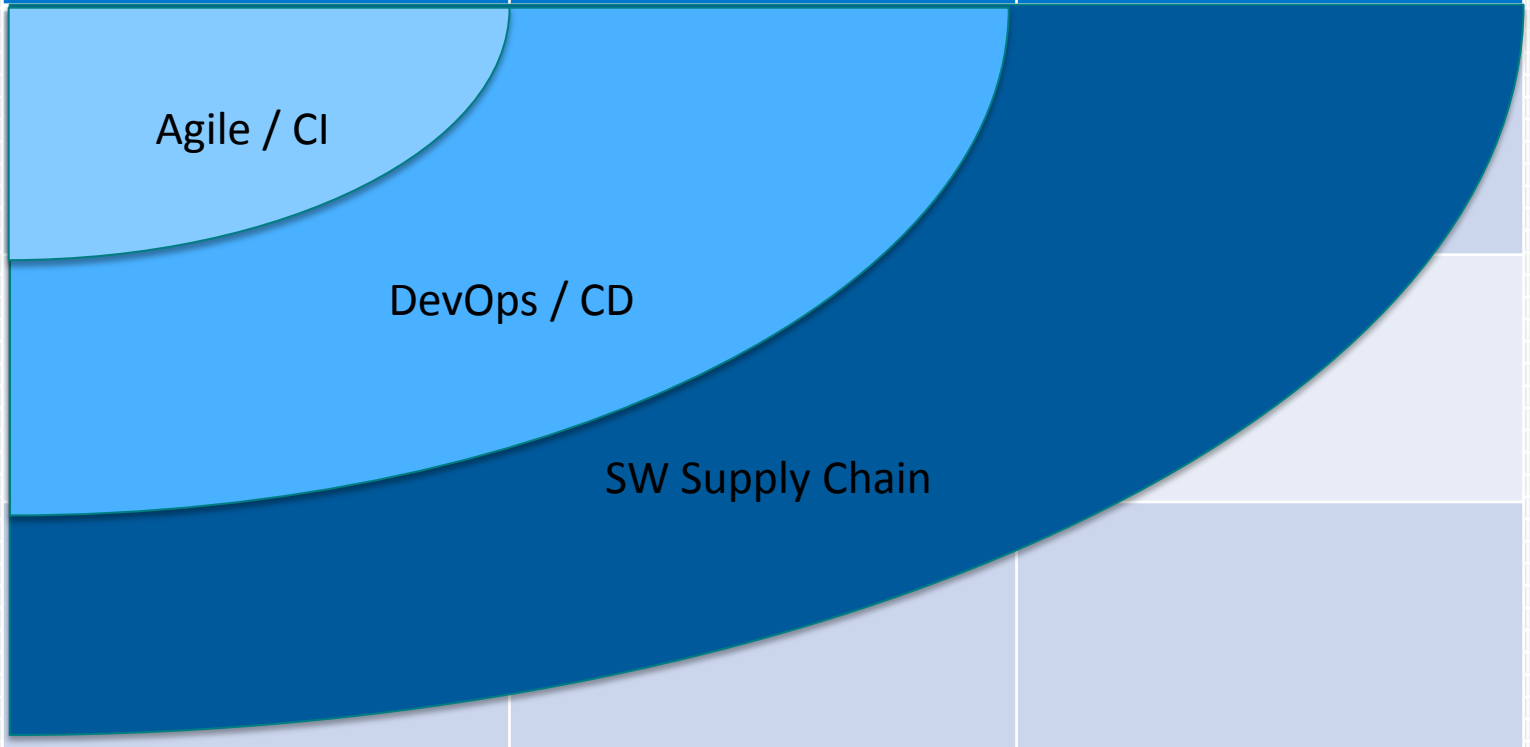
Agile made dev faster but wasn't enough. DevOps extends patterns to Ops 4 mutual gains @joshcorman @mortman #RSAC #DevOps

Deming drove Toyota Supply Chains. We can EXTEND DevOps w/ his quality/safety patterns @joshcorman @mortman #RSAC #DevOps

ON TIME.
Faster builds.
Fewer interruptions.
More innovation.

ON BUDGET.
More efficient.
More profitable.
More competitive.

ACCEPTABLE QUALITY/RISK.
Easier compliance.
Higher quality.
Built-in audit protection.



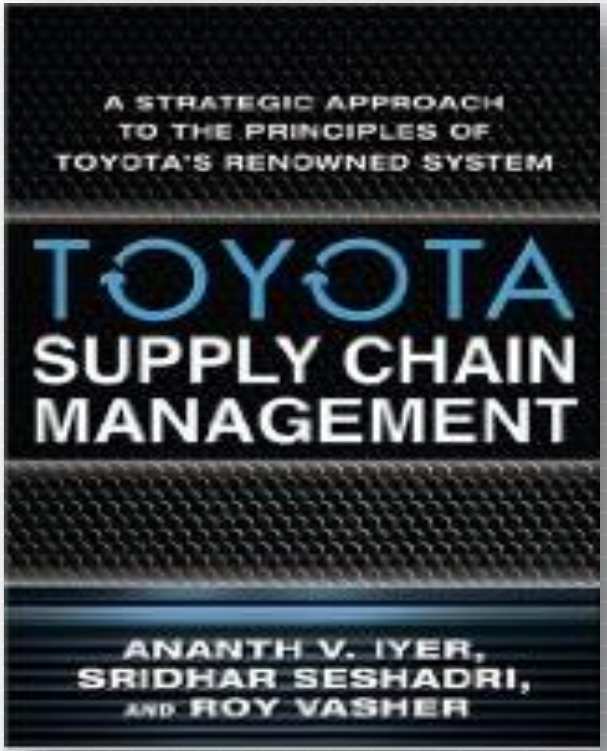
#RSAC
@mortman
@joshcorman

SW SupplyChains enable faster, more efficient dev by reducing elective complexity/risk++ @joshcorman @mortman #RSAC #DevOps

Our SW Supply Chain is only as strong as its weakest link. Can you say #OpenSSL? @joshcorman @mortman #RSAC #DevOps

Comparing the Prius and the Volt

	Toyota Prius	Chevy Volt
Cost	$24,200	$39,900
Units	23,294	1,788
Plant Suppliers	125	800
In-House Production	27%	54%
Firm-Wide Suppliers	*224*	*5,500*

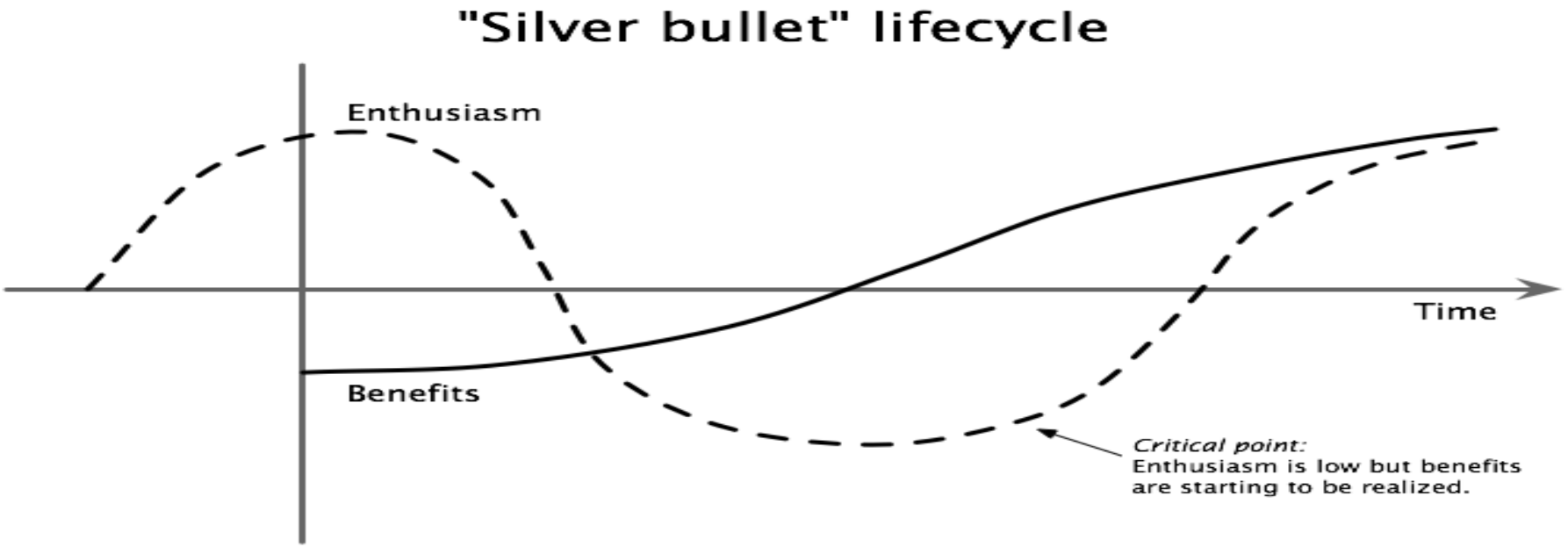


Toyota Prius (v Volt) used 1/6th suppliers, better leveraged, for 60% price & 12x sales @joshcorman @mortman #RSAC #DevOps


DELL
Sonatype
Is #DevOps a Culture? A Process? A Toochain? YES; but the greatest of these is Culture/Empathy @joshcorman @mortman #RSAC
RSAConference2015


B N
S F
TOOL CAR
Messy


FACTS
NOT OPINIONS

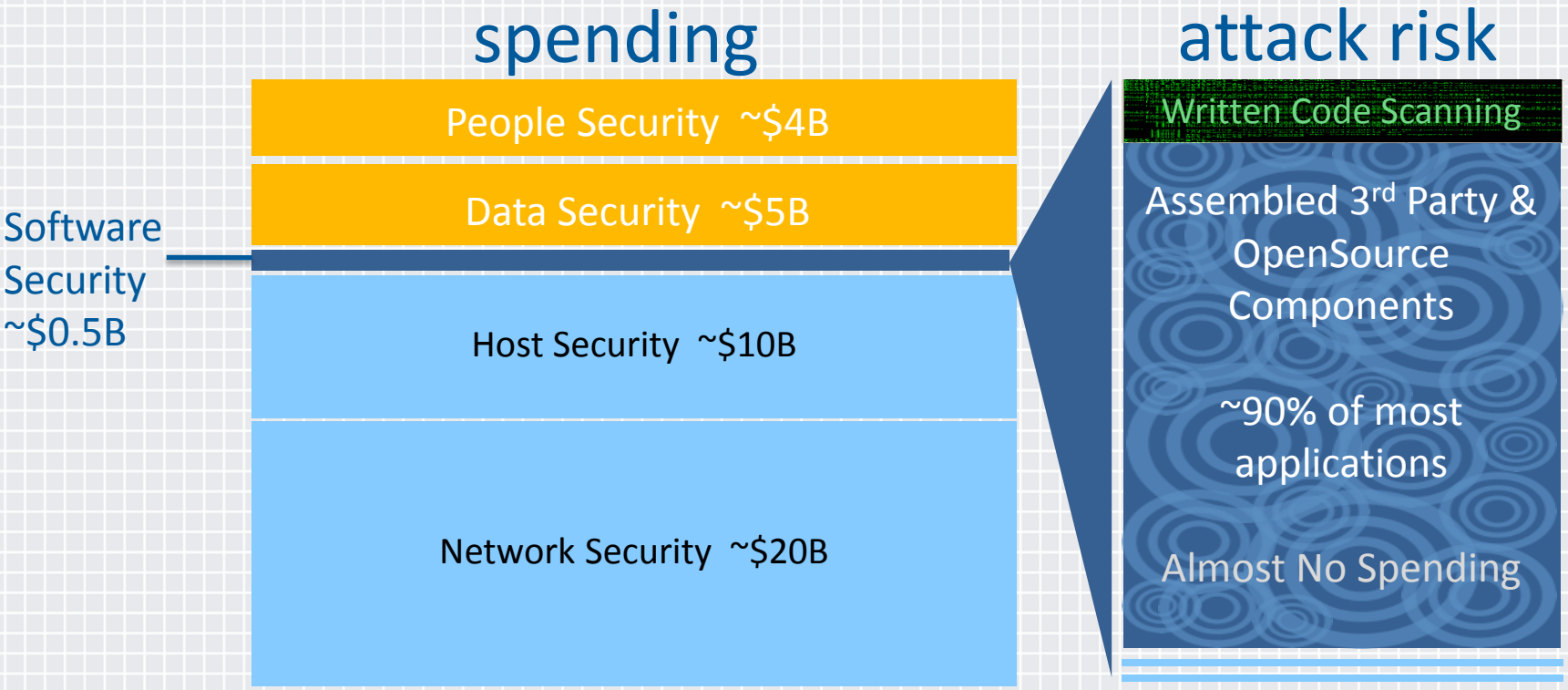


Reference: Taylor, Sharon, and Ivor Macfarlane. *ITIL Small-scale Implementation*. London: TSO, 2005.


magical
unicorn
poops
C. Stovall

SW Status Quo: Most attacked; least spend

Worse, w/in Software, existing dollars go to the <= 10% written



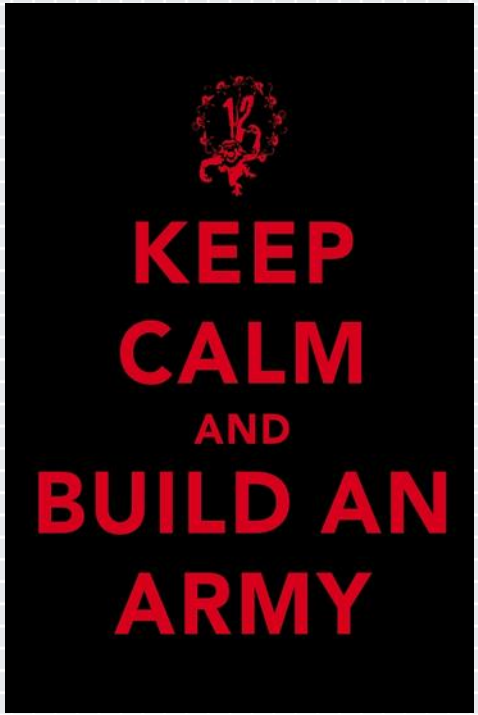
StatusQuo: SW is MOST attacked & gets LEAST SecSpend; most on 10% of code we write @joshcorman @mortman #RSAC #DevOps

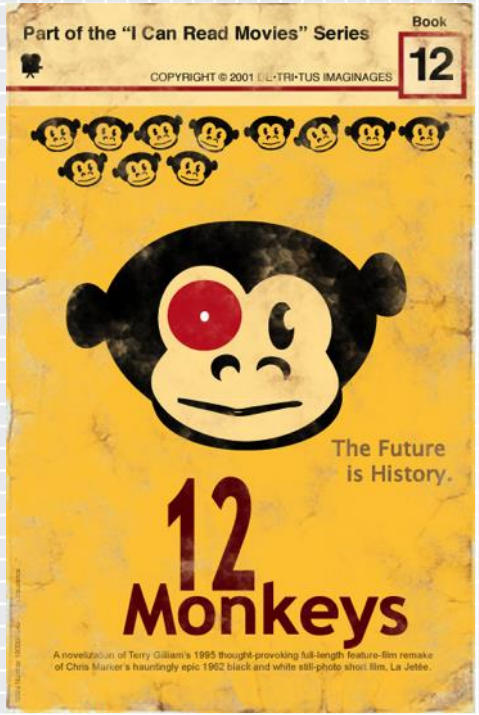
Source: Normalized CObIT spending across IDC, Gartner, The 451 Group; since groupings vary

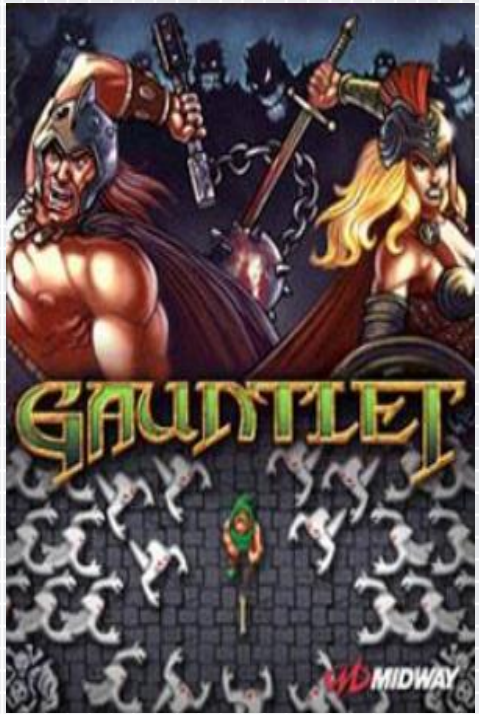

LOST
FOUND

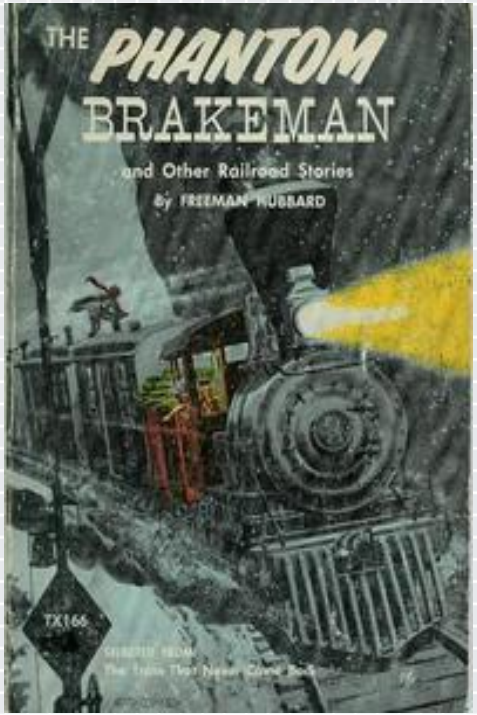
This was added b/c the Red Hat in the “Lost & Found” made @mortman giggle & he forced it upon @joshcorman #RSAC #DevOps

2) Be Mean To Your Code!



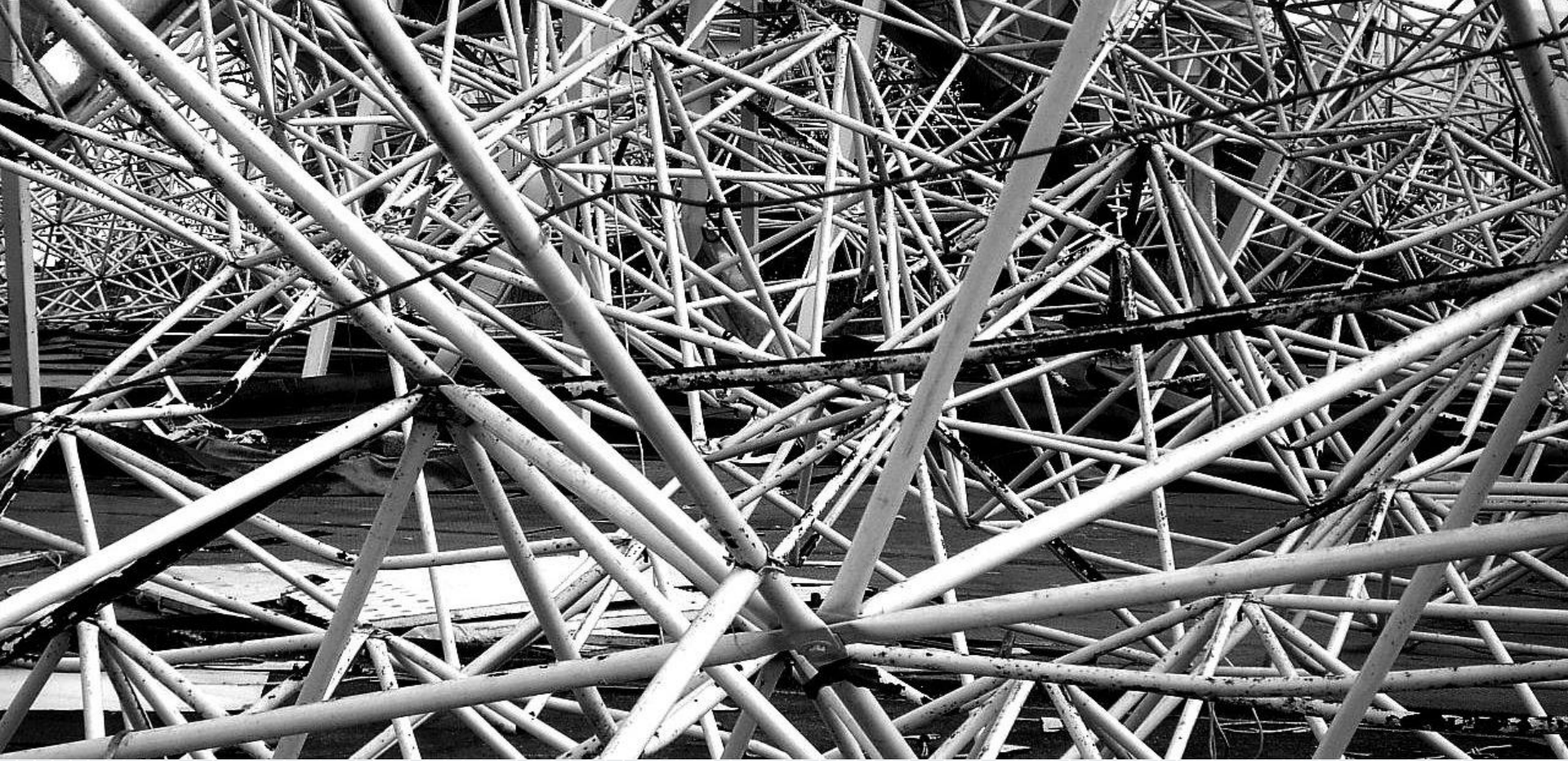






DELL Sonatype

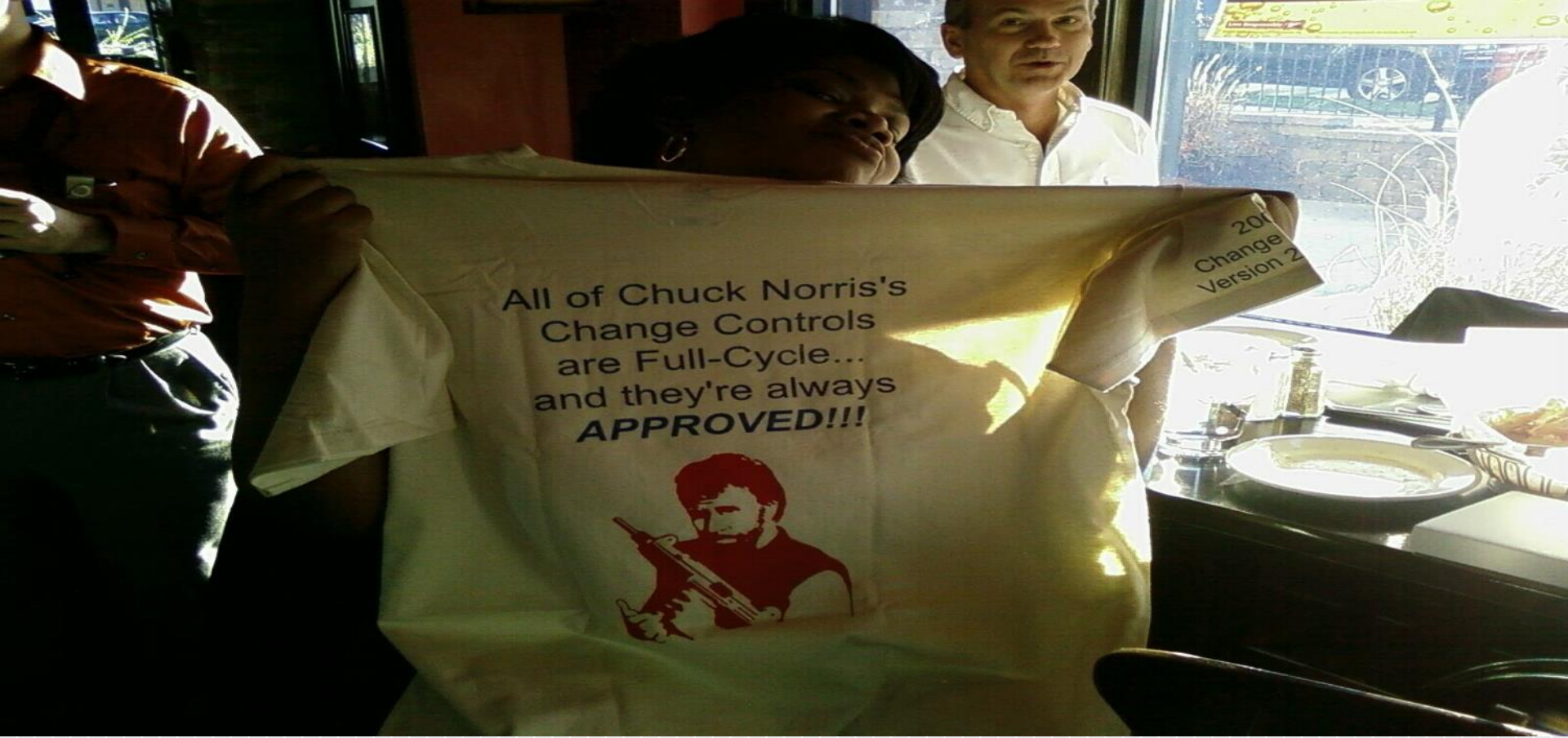
2) Be Mean To Your Code! To avoid failure; fail all the time #ChaosMonkey #GauntIt #BrakeMan @joshcorman @mortman #RSAC #DevOps



Decomposition lowers complexity adds security and reliability @mortman @joshcorman #RSAC #DevOps

Simple > Complex. Simple != Easy though. There is no easy button, but there is an easiER one. @joshcorman @mortman #RSAC #DevOps


change is good.
look hard

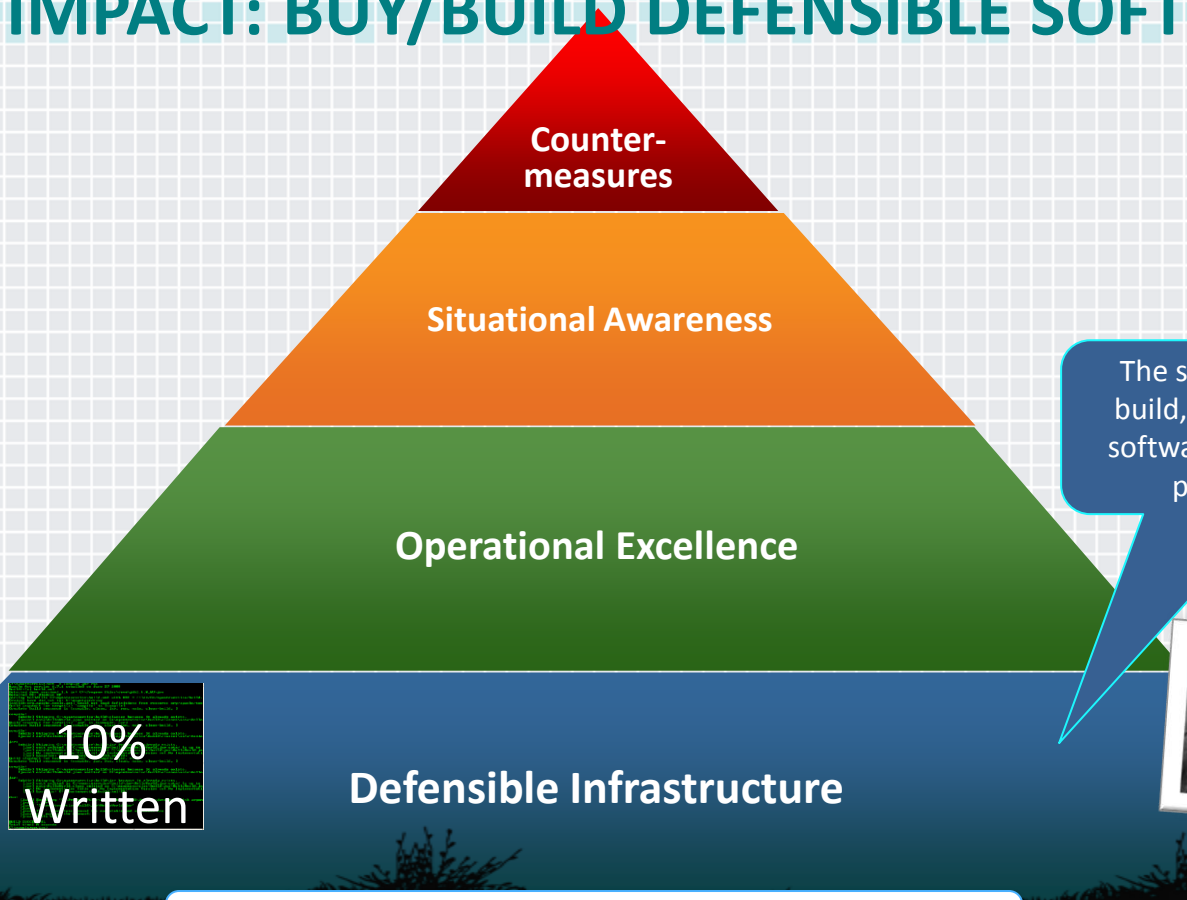


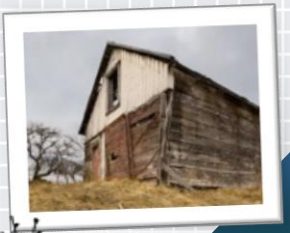
All of Chuck Norris's Change Controls are Full Cycle and they're always approved!
@joshcorman @mortman #RSAC #DevOps

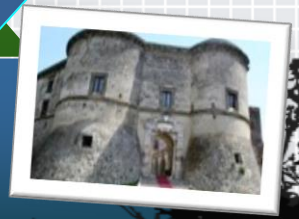
5) Empathy is the killer app! Silos prohibit sharing and empathy…. #RSAC #DevOps @mortman @joshcorman

MOST IMPACT: BUY/BUILD DEFENSIBLE SOFTWARE

#RSAC
@mortman
@joshcorman







DefensibleIT & OpsExcellence have MOST Security impact, but elude CISO influence
BUT... @joshcorman @mortman #RSAC #DevOps

#RSAC
@mortman
@joshcorman

Counter-measures

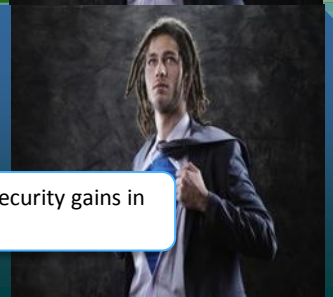
Situational Awareness

DevOps

Operational Excellence

DevOps

Defensible Infrastructure



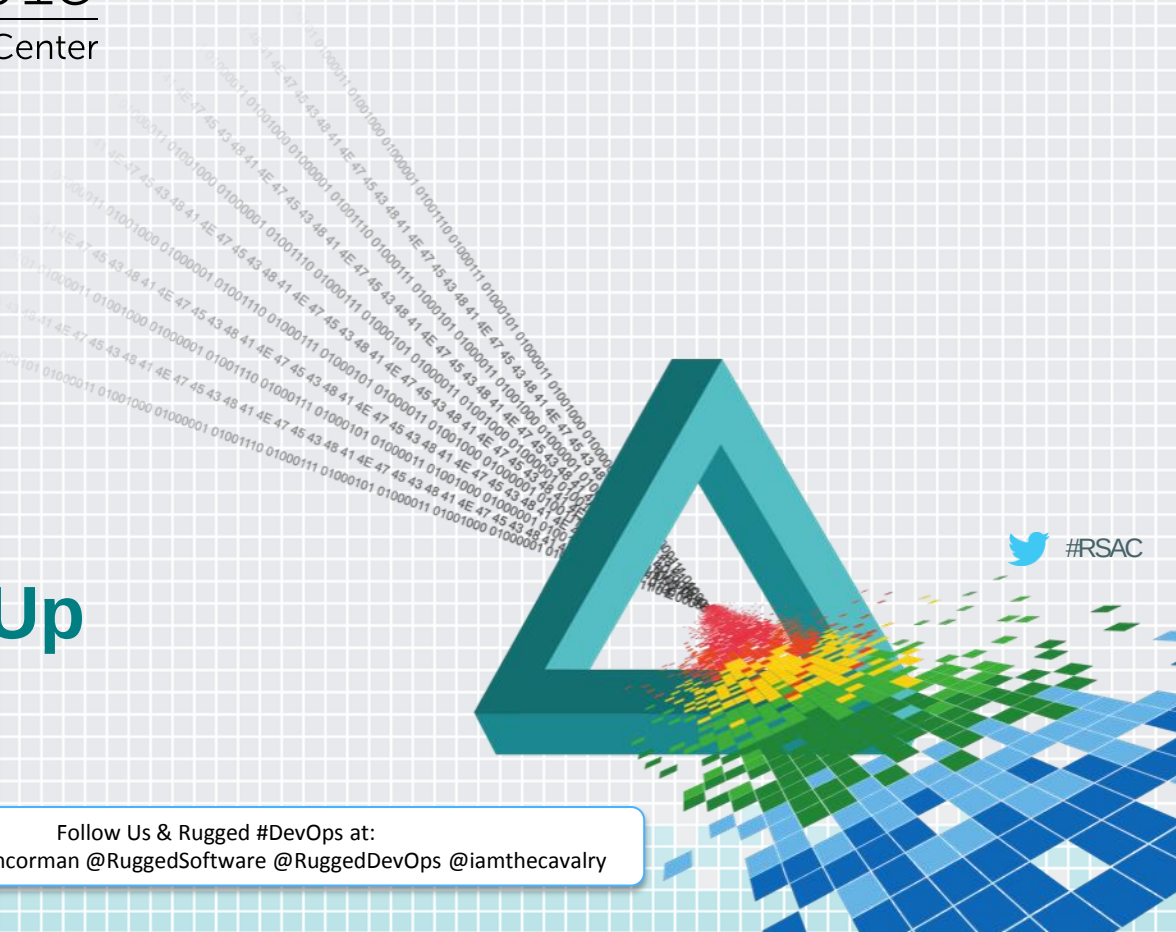
DevOps

[cont] #DevOps smashes silos & finally enables the MUCH LARGER Security gains in both @joshcorman @mortman #RSAC #DevOps

Apply!

- Stop resisting… “Survival isn’t mandatory” – Deming
  - Josh’s RSAC EU Keynote http://youtu.be/m4Y_K7MXQxQ
- Read “The Phoenix Project” by Gene Kim
  - http://itrevolution.com/books/phoenix-project-devops-book/
- Watch videos from RSAC “DevOps Connect” Rugged DevOps Day
  - http://www.sonatype.org/nexus/2015/04/13/devops-connect-secops-editon-at-rsac-2015-speakers-and-schedule/
- Grab tooling:
  - Gauntlt, BrakeMan, Chaos Monkey, and the Simian Army
- Start small, start anywhere, start TODAY!

Get on the train before the train gets on you! Don’t delay, start today!
@joshcorman @mortman #RSAC #DevOps



Conclusion/Wrap-Up

Follow Us & Rugged #DevOps at:
@mortman @joshcorman @RuggedSoftware @RuggedDevOps @iamthecavalry