# Doing the Unstuck

## How Rugged Cultures Drive Biz & AppSec Value

# 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

EXCLUSIVE! THE INTIMATE, INSIDE PHOTOS OF THE VANITY FAIR OSCAR PARTY!
VANITY FAIR
Special TV Issu
Admit it… you love
more than u
FRIENDS

# A Personal Bit…

Passionate

Purposeful

Principled

Protector

Provider

Honest

Courageous

Consequential

# Unreasonable

# A Fool

# Are We Getting Better…

No

*Is it getting better?*

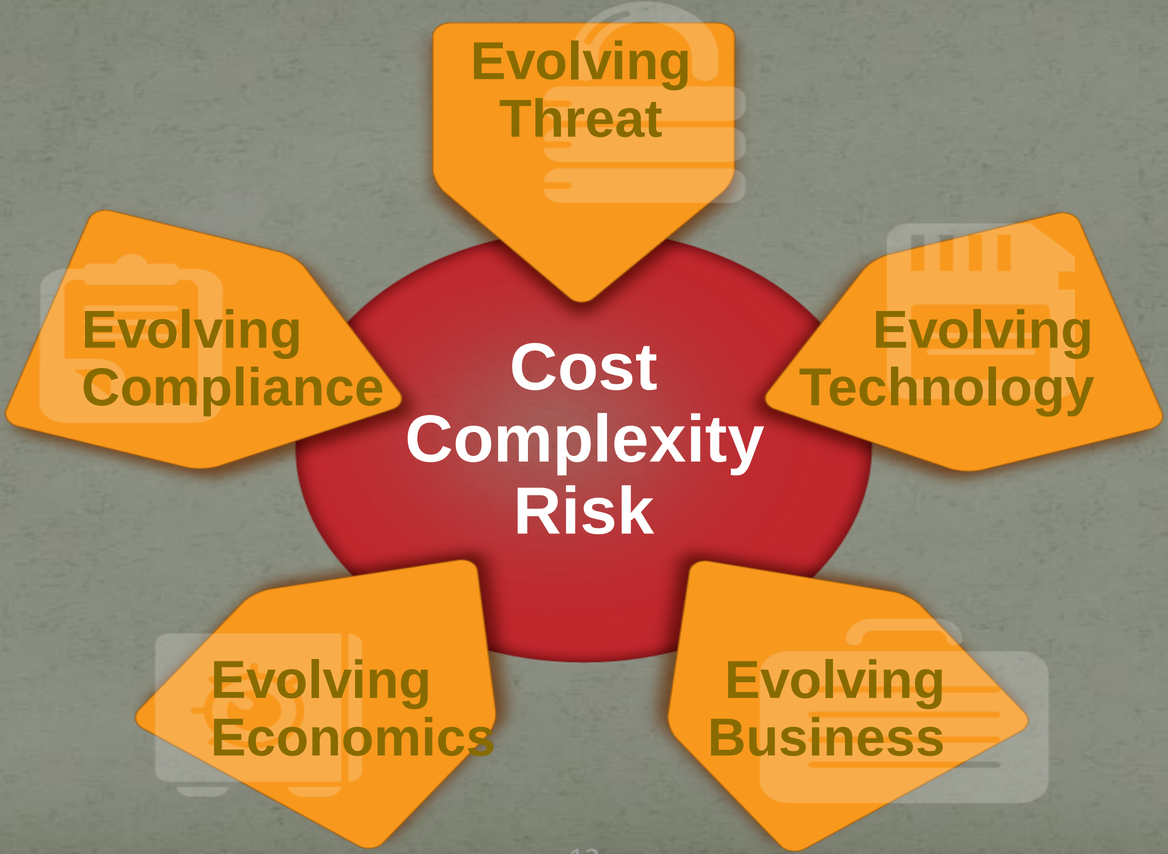
*Or do you feel the same?*

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

How would you know?

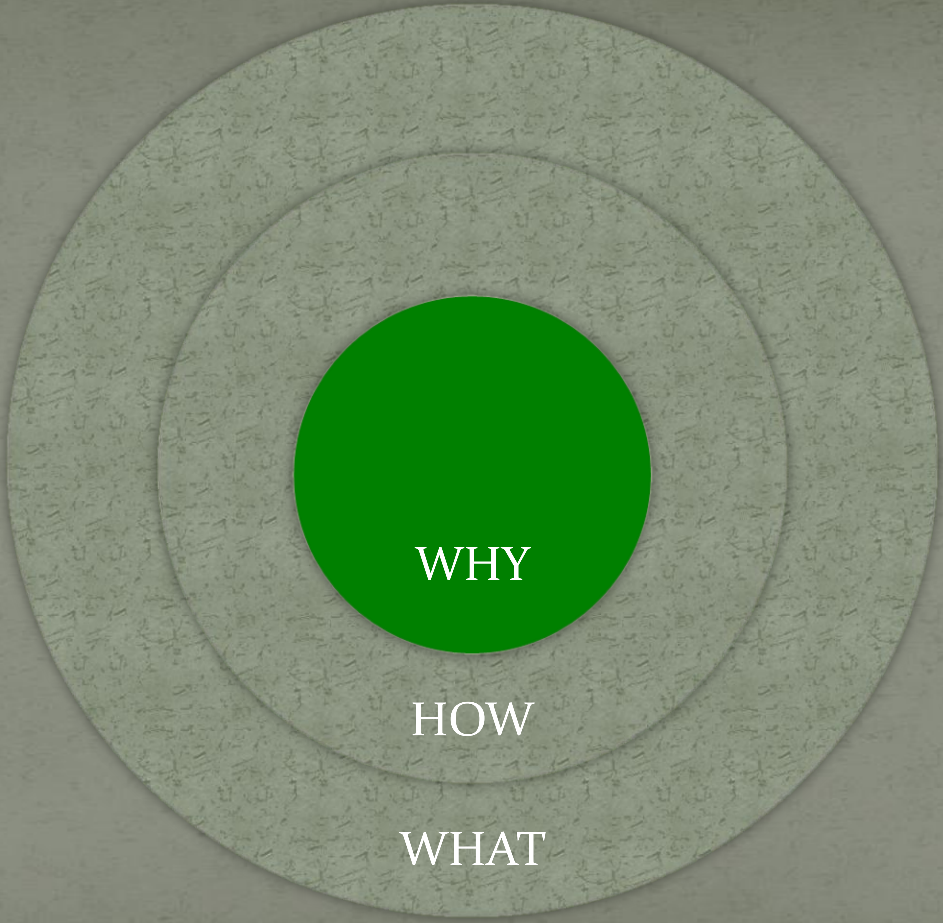
By which criteria?

# Constant Change



SECBURNOUT.ORG

# Why It Matters…



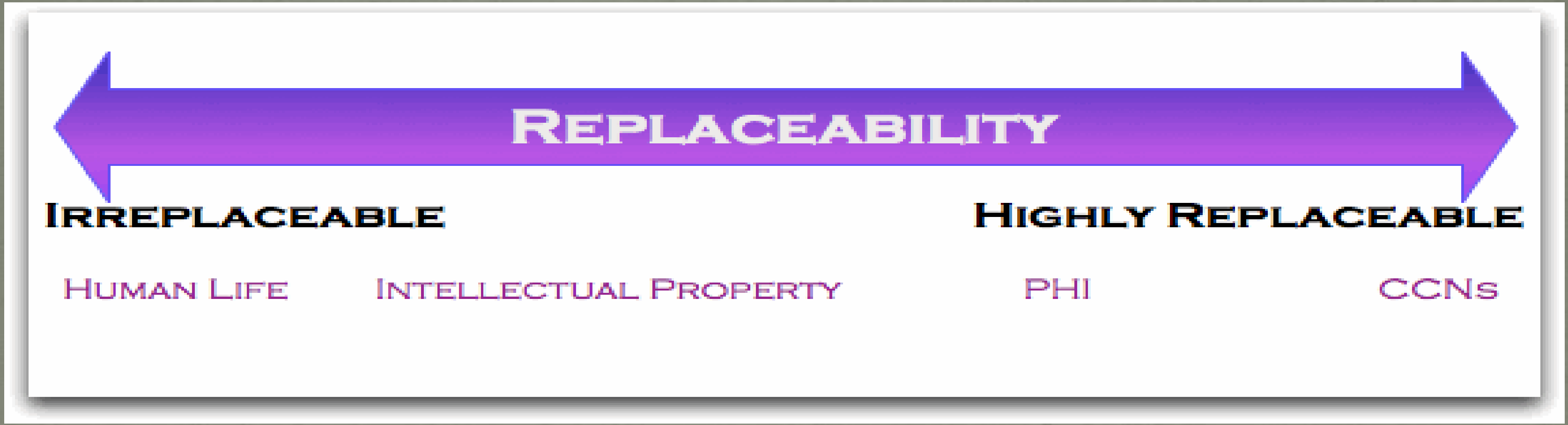
WHY

HOW

WHAT

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

# Consequences: Value & Replaceability



Replaceability

Irreplaceable

Highly Replaceable

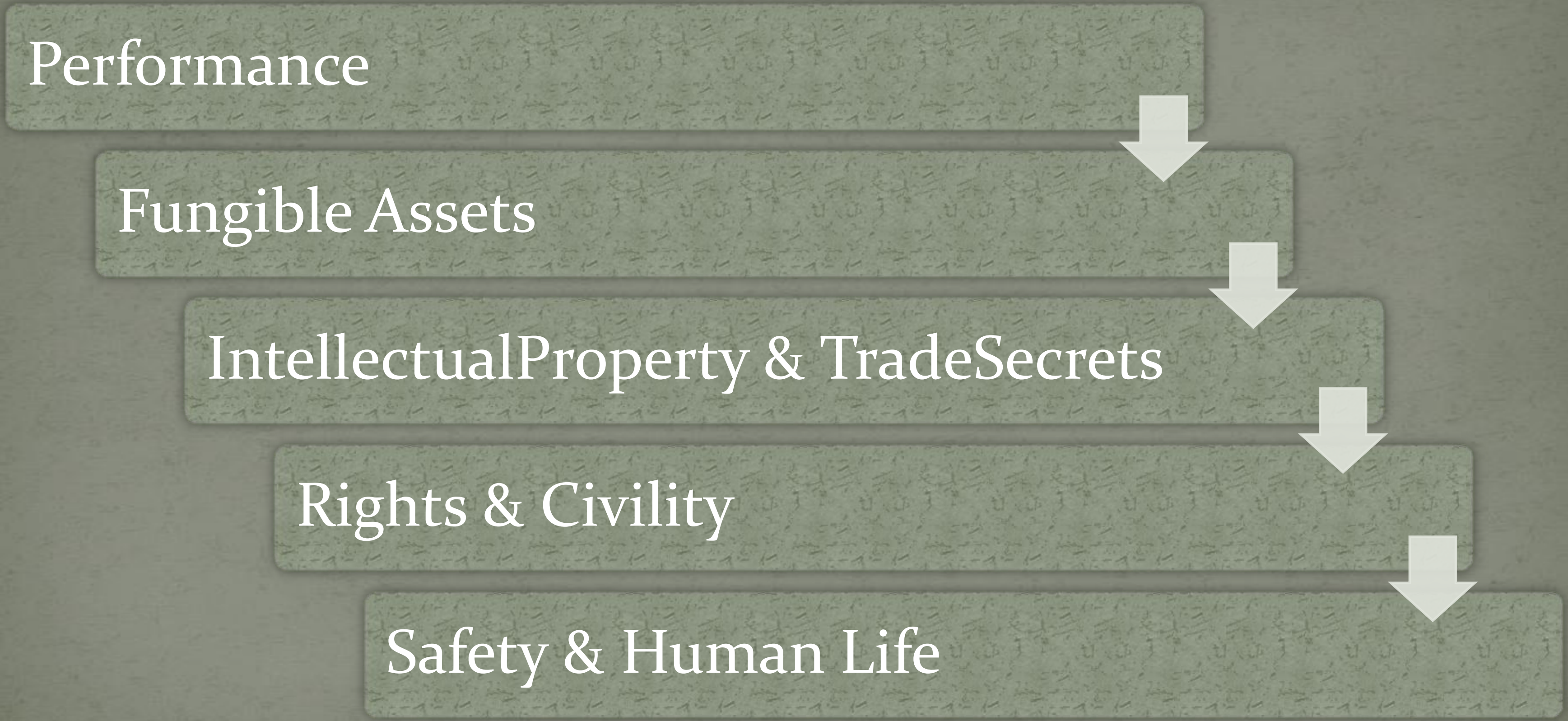
Human Life

Intellectual Property

PHI

CCNs

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



Performance

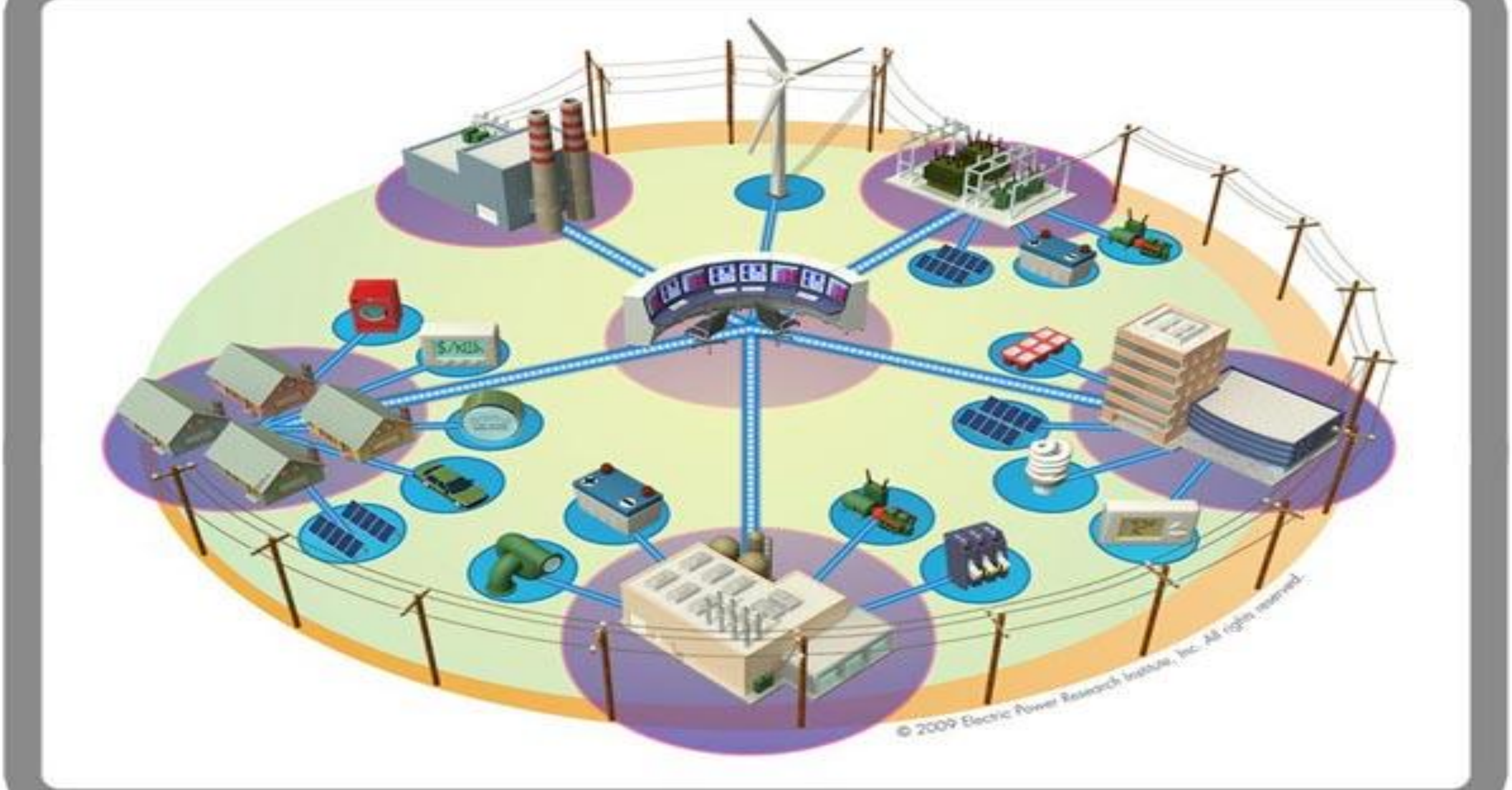
Fungible Assets

IntellectualProperty & TradeSecrets

Rights & Civility

Safety & Human Life

# Dependence


$/kWh

Ford
20
40
60
80
100
120
140
P
R
N
D
M
Entertainment
21 Alt Nation
Rock
Blazing Lazer
72°
Auto
70°

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

# OWASP Top 1~~0~~

*“We can eliminate SQLi in our lifetime”*

# Activity

Effect

# Symptoms

# Root Causes

# Easy

# Important

80/20

# Best Practices

# aren’t

# Good Enough

# isn’t

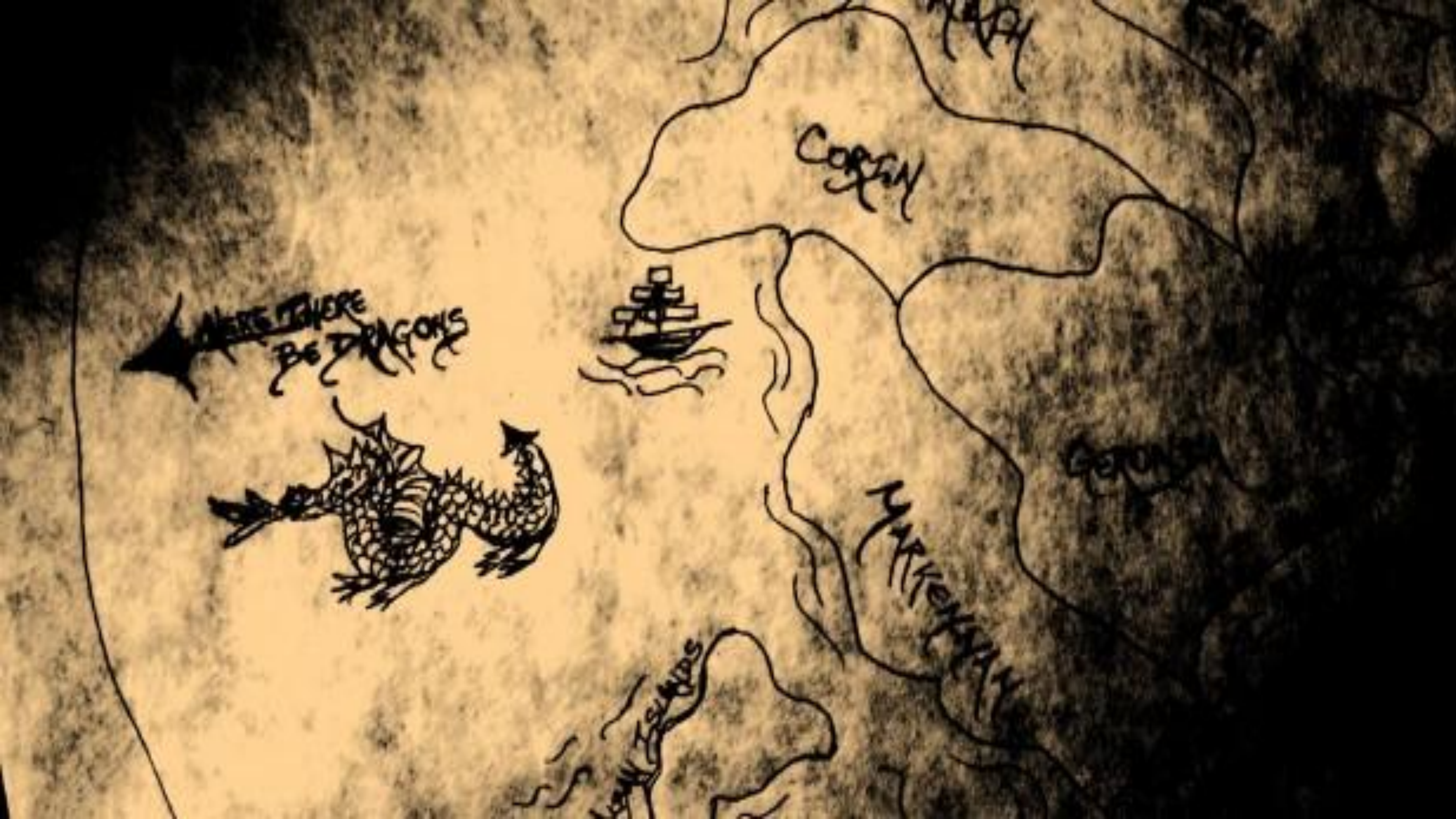
# Incentives

# What you can do about it…

# Pick one:

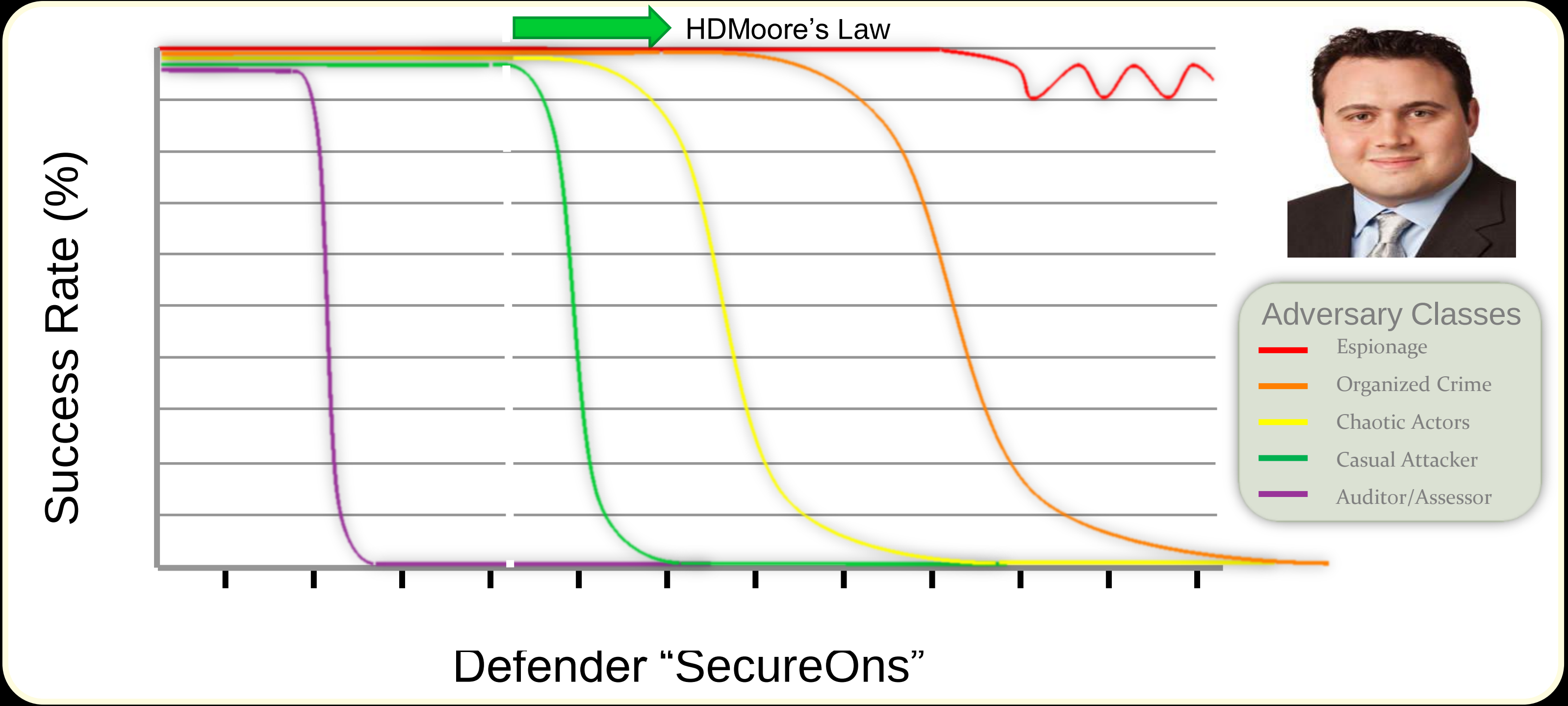
□ Make Excuses

□ Make Progress


HERE THERE BE DRAGONS
CORGIN
MARKENWAN
GERONSA
ISLANDS

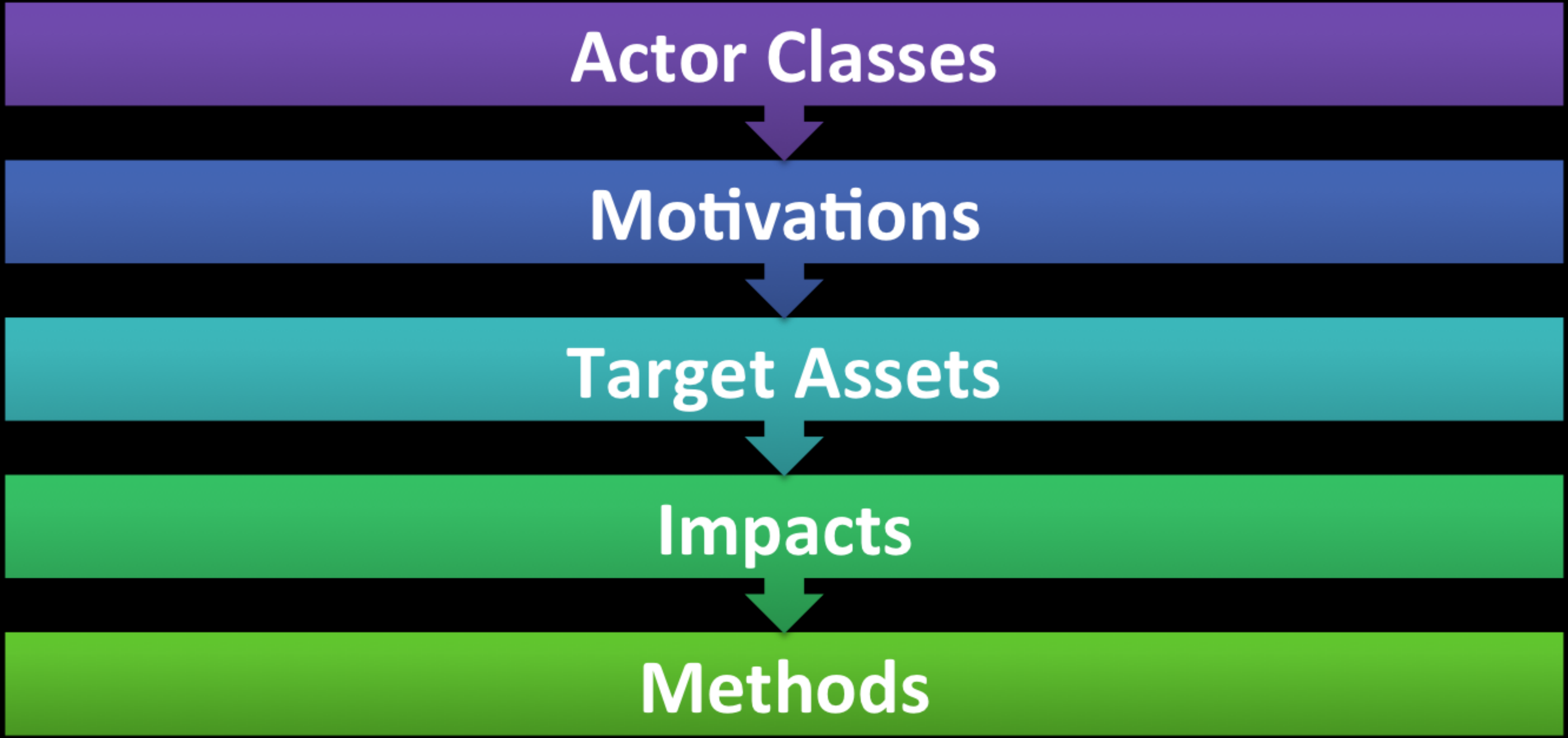
-MAR-

# HDMoore's Law



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

# Adversary Centric



Actor Classes

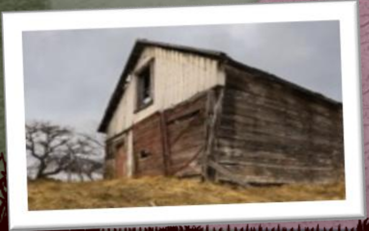
Motivations

Target Assets

Impacts

Methods

# Rugged DevOps: IT @ Ludicrous Speed!



# Defensible Infrastructure

Gene Kim

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

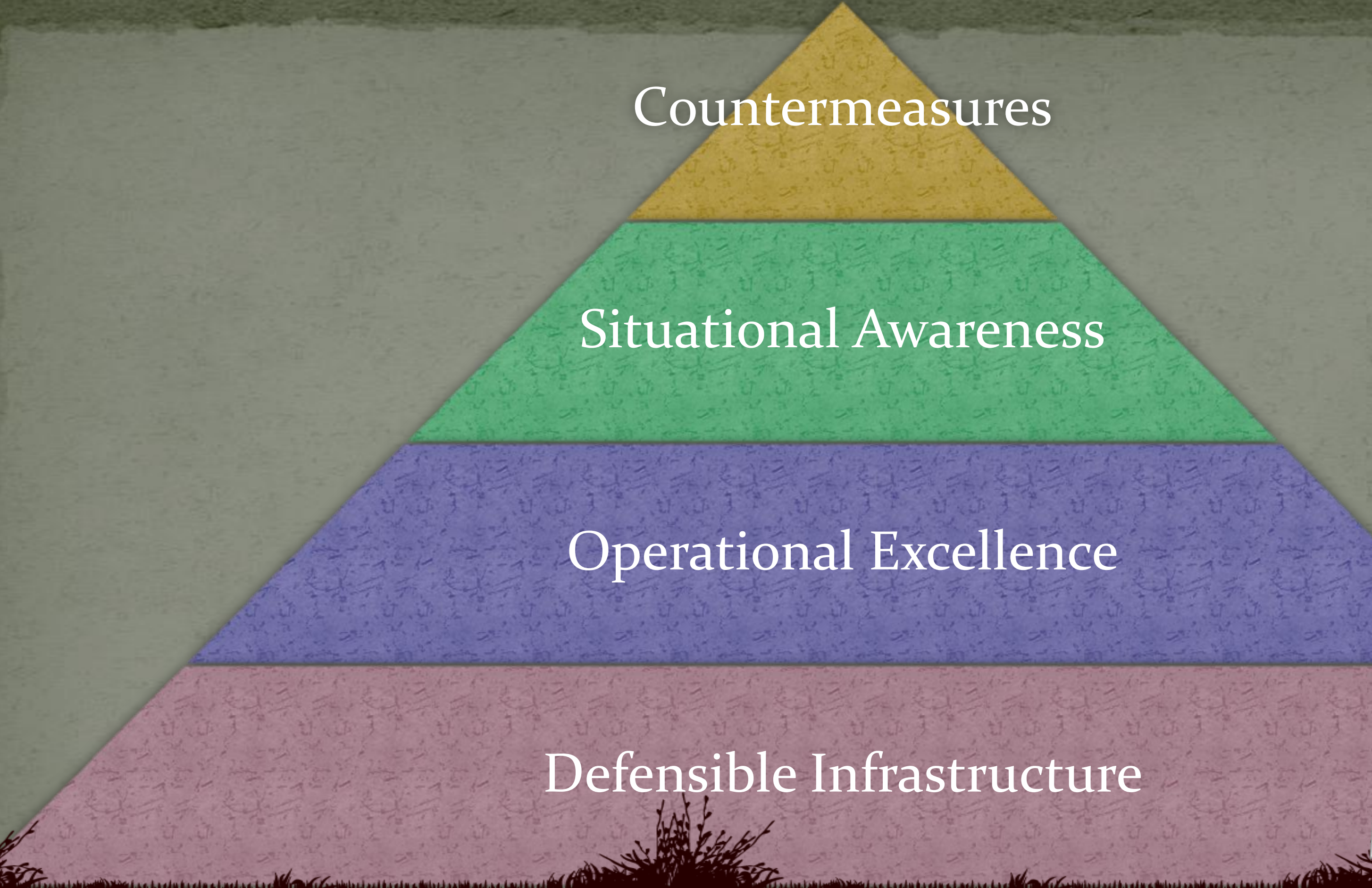
Operational Excellence

Defensible Infrastructure

Situational Awareness

Operational Excellence

Defensible Infrastructure



Countermeasures

Situational Awareness

Operational Excellence

Defensible Infrastructure

# Experimentation

An untested hypothesis is a wish

# RUGGED SOFTWARE

hydrolift
fly without wings
SIEMENS
SIEMENS
Koenigsegg
Koenigsegg
Radisson
Radisson
Coca-Cola
Color Line
NORWAY

# FAST

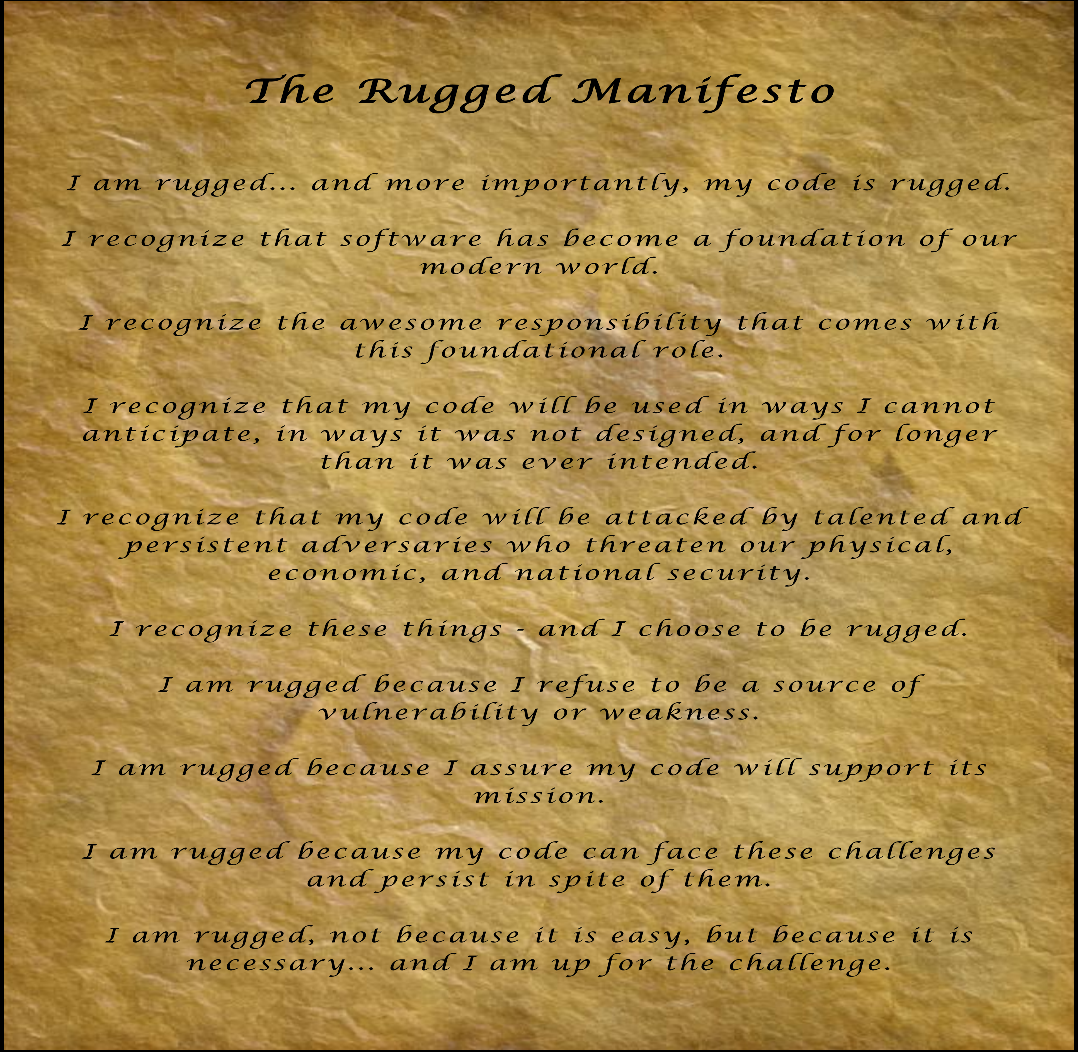
# AGILE

# Are You Rugged?

HARSH

UNFRIENDLY

# THE MANIFESTO



# The Rugged Manifesto

I am rugged... and more importantly, my code is rugged.

I recognize that software has become a foundation of our modern world.

I recognize the awesome responsibility that comes with this foundational role.

I recognize that my code will be used in ways I cannot anticipate, in ways it was not designed, and for longer than it was ever intended.

I recognize that my code will be attacked by talented and persistent adversaries who threaten our physical, economic, and national security.

I recognize these things - and I choose to be rugged.

I am rugged because I refuse to be a source of vulnerability or weakness.

I am rugged because I assure my code will support its mission.

I am rugged because my code can face these challenges and persist in spite of them.

I am rugged, not because it is easy, but because it is necessary... and I am up for the challenge.

I recognize that my code will be used in ways I cannot anticipate, in ways it was not designed, and for longer than it was ever intended.

# Rugged?

[www.ruggedsoftware.org](www.ruggedsoftware.org)

[https://www.ruggedsoftware.org/documents/](https://www.ruggedsoftware.org/documents/)

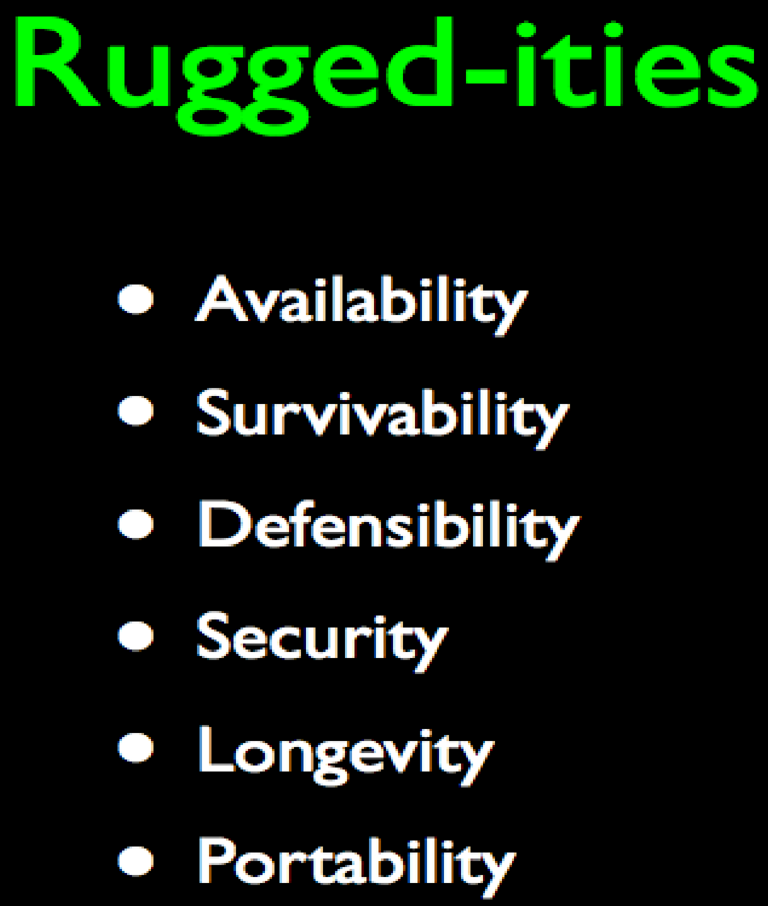
*CrossTalk*
*[http://www.crosstalkonline.org/issues/marchapril-2011.html](http://www.crosstalkonline.org/issues/marchapril-2011.html)*

CROSSTALK
The Journal of Defense Software Engineering
THE RUGGED SOFTWARE MANIFESTO

~~SECURITY~~

COST

INHIBITOR



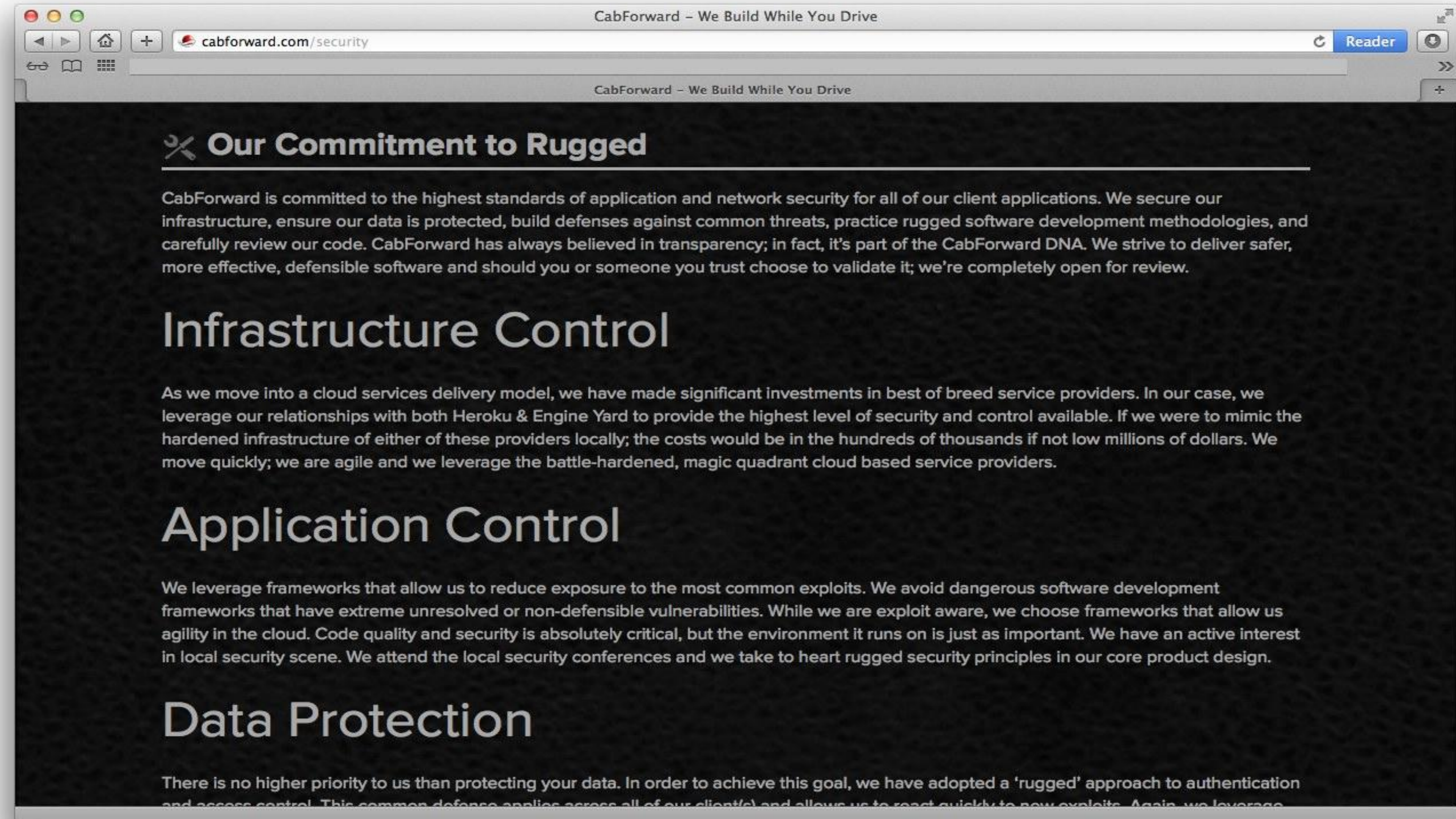
# Rugged-ities

- Availability
- Survivability
- Defensibility
- Security
- Longevity
- Portability

Source: Wendy Nather (at the time, a CISO)

# Rugged DevOps Success

- Vertical: Financial
- Business: Money management firm
- Implemented Rugged DevOps to quicken the change cycle and tighten the security
- Results:
  - Increased from quarterly change cycle, to daily changes, 46 average a month.
  - Reduced failed changes from 17% to 4%
  - Reduced IT audit exceptions to zero


CabForward – We Build While You Drive
cabforward.com/security
Reader
CabForward – We Build While You Drive

## Our Commitment to Rugged

CabForward is committed to the highest standards of application and network security for all of our client applications. We secure our infrastructure, ensure our data is protected, build defenses against common threats, practice rugged software development methodologies, and carefully review our code. CabForward has always believed in transparency; in fact, it's part of the CabForward DNA. We strive to deliver safer, more effective, defensible software and should you or someone you trust choose to validate it; we're completely open for review.

# Infrastructure Control

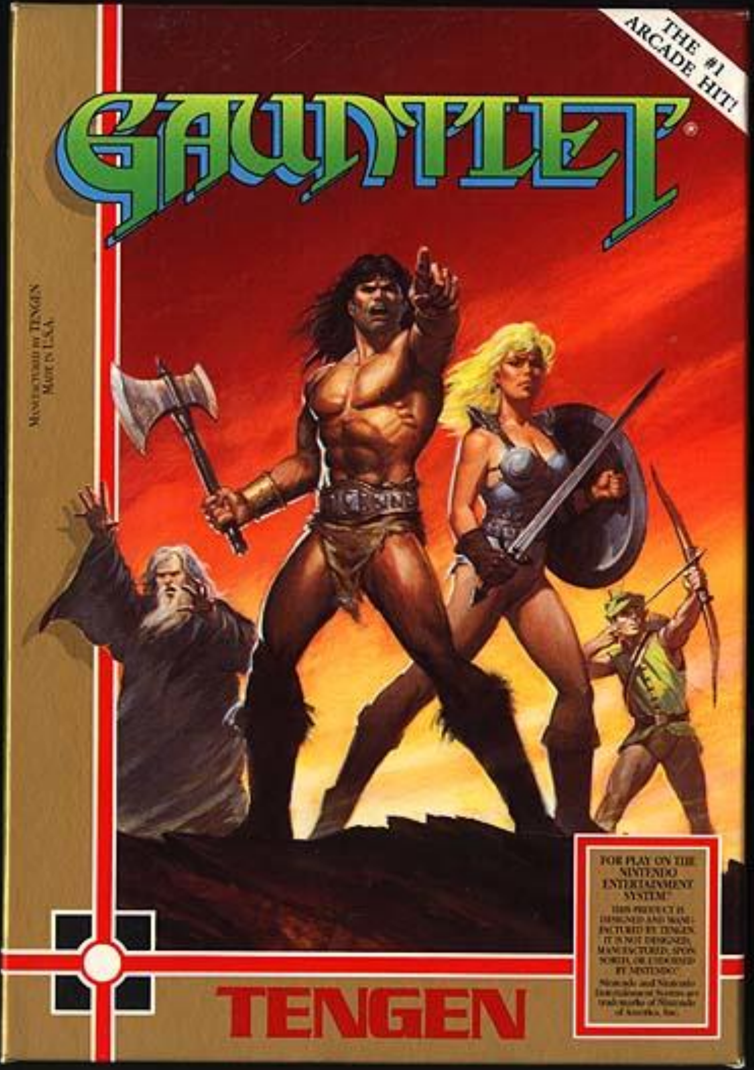
As we move into a cloud services delivery model, we have made significant investments in best of breed service providers. In our case, we leverage our relationships with both Heroku & Engine Yard to provide the highest level of security and control available. If we were to mimic the hardened infrastructure of either of these providers locally; the costs would be in the hundreds of thousands if not low millions of dollars. We move quickly; we are agile and we leverage the battle-hardened, magic quadrant cloud based service providers.

# Application Control

We leverage frameworks that allow us to reduce exposure to the most common exploits. We avoid dangerous software development frameworks that have extreme unresolved or non-defensible vulnerabilities. While we are exploit aware, we choose frameworks that allow us agility in the cloud. Code quality and security is absolutely critical, but the environment it runs on is just as important. We have an active interest in local security scene. We attend the local security conferences and we take to heart rugged security principles in our core product design.

# Data Protection

There is no higher priority to us than protecting your data. In order to achieve this goal, we have adopted a 'rugged' approach to authentication and access control. This common defense applies across all of our client(s) and allows us to react quickly to new exploits. Again, we leverage



THE #1 ARCADE HIT!
GAUNTLET®
MANUFACTURED BY TENGEN
MADE IN U.S.A.
FOR PLAY ON THE NINTENDO ENTERTAINMENT SYSTEM™
THIS PRODUCT IS DESIGNED AND MANUFACTURED BY TENGEN. IT IS NOT DESIGNED, MANUFACTURED, SPONSORED, OR ENDORSED BY NINTENDO®.
Nintendo and Nintendo Entertainment System are trademarks of Nintendo of America, Inc.
TENGEN

A declaration of intent & recognition…

# The Rugged Summit

# We don’t all agree

STRAW MAN ARGUMENT

Dorothy, why do some AppSec guru’s hate Rugged?

## The Rugged Bank Security Story

***Commitment**: Brick-and-mortar banks protect money with vaults, guards, and alarms. As we move these operations to cyberspace, everyone should expect even better protection of their money and financial information. RuggedBank is committed to the highest standards of application and network security for our RBOnline application. We secure our infrastructure, ensure data is always protected, build defenses against injection and other application attacks, practice rugged software development, and carefully verify our code. At the core of our security is a commitment to transparency – across our protections, processes, and even potential problems.*

### Infrastructure Control

RBOnline security depends on maintaining control of our physical and network infrastructure. We are hosted in a secure data center, managed by trusted staff, and our systems are kept hardened, patched, and up-to-date. Our network is defended and segmented by firewalls and we detect and block both network and application attacks.

Learn more... ▸

### Application Control

All our data protections depends on having software that is resistant to injection or other attacks that rob us of control of our systems. We have strict rules around data handling and interpreter use to prevent injection. In addition we ensure the application is always available and ready for use.

Learn more ... ▸

### Data Protection

Protecting your data is our highest priority. Our primary defense is universal authentication and access control. As a secondary defense, we also use strong encryption everywhere data is transmitted or stored. To ensure that these protections are not bypassed, we have established extensive protections against injection and other attacks.

Learn more ... ▸

### Rugged Development

To make sure that our application is designed and implemented securely, We follow a secure development lifecycle. All our developers are trained in using our standard security defenses. We have performed extensive threat modeling and minimized our attack

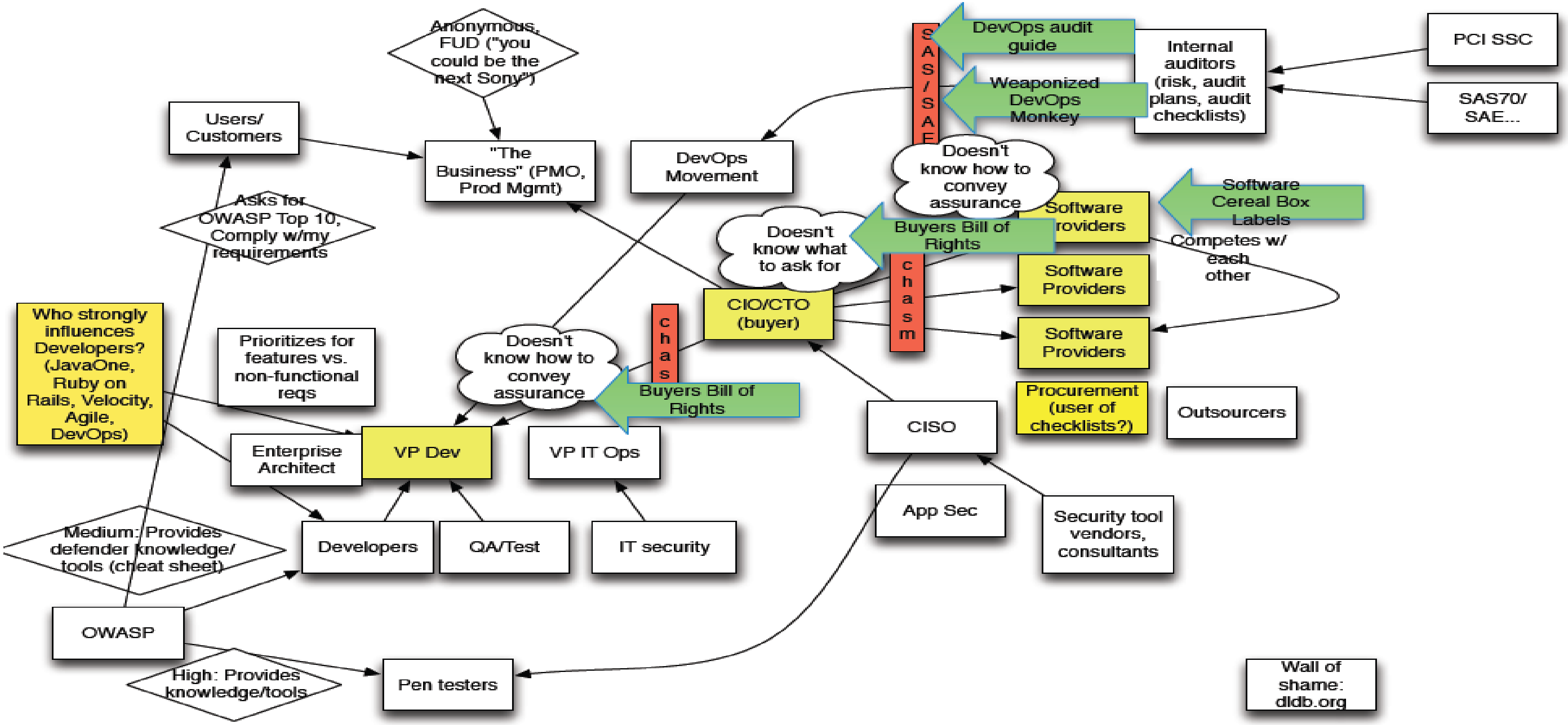
### Security Verification

An independent team performs architecture analysis, code review, and penetration testing on our application. We use a custom test suite and automated security tools to double-check for vulnerabilities. We are committed to finding and eliminating

### Transparent Security

Without information, good security decisions are impossible, so we are committed to ensure that you understand the protections that we have provided. We will notify you of any security issues that might affect your business. You can export your data from

# From the Rugged Handbook StrawMan



Anonymous, FUD ("you could be the next Sony")

Users/ Customers

"The Business" (PMO, Prod Mgmt)

DevOps Movement

SAS/SAE

DevOps audit guide

Weaponized DevOps Monkey

Internal auditors (risk, audit plans, audit checklists)

PCI SSC

SAS70/ SAE...

Doesn't know how to convey assurance

Software Cereal Box Labels

Software Providers

Asks for OWASP Top 10, Comply w/my requirements

Doesn't know what to ask for

Buyers Bill of Rights

chasm

Competes w/ each other

Software Providers

Software Providers

Who strongly influences Developers? (JavaOne, Ruby on Rails, Velocity, Agile, DevOps)

Prioritizes for features vs. non-functional reqs

Doesn't know how to convey assurance

chas

CIO/CTO (buyer)

Buyers Bill of Rights

Procurement (user of checklists?)

Outsourcers

Enterprise Architect

VP Dev

VP IT Ops

CISO

App Sec

Security tool vendors, consultants

Medium: Provides defender knowledge/ tools (cheat sheet)

Developers

QA/Test

IT security

OWASP

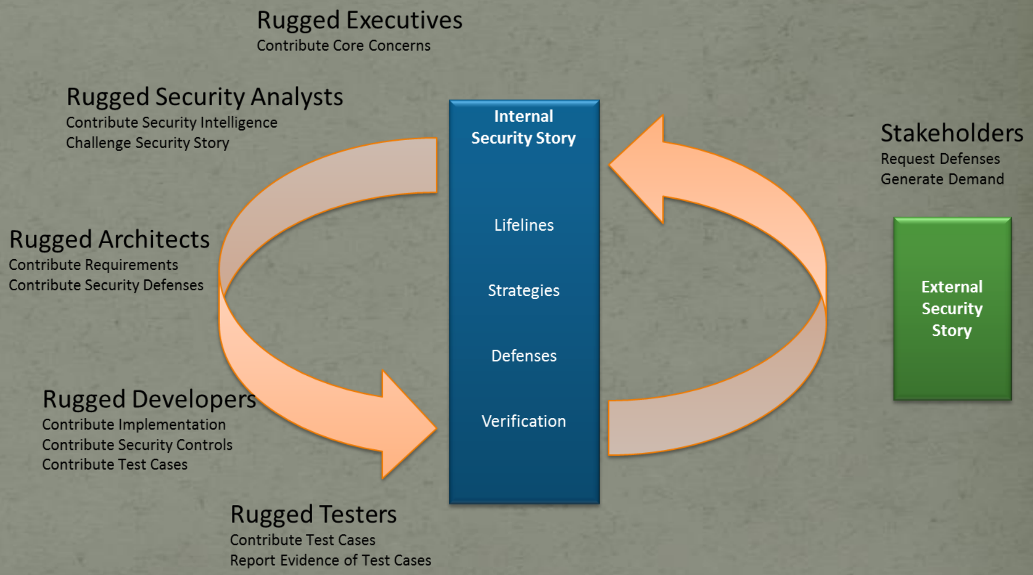
High: Provides knowledge/tools

Pen testers

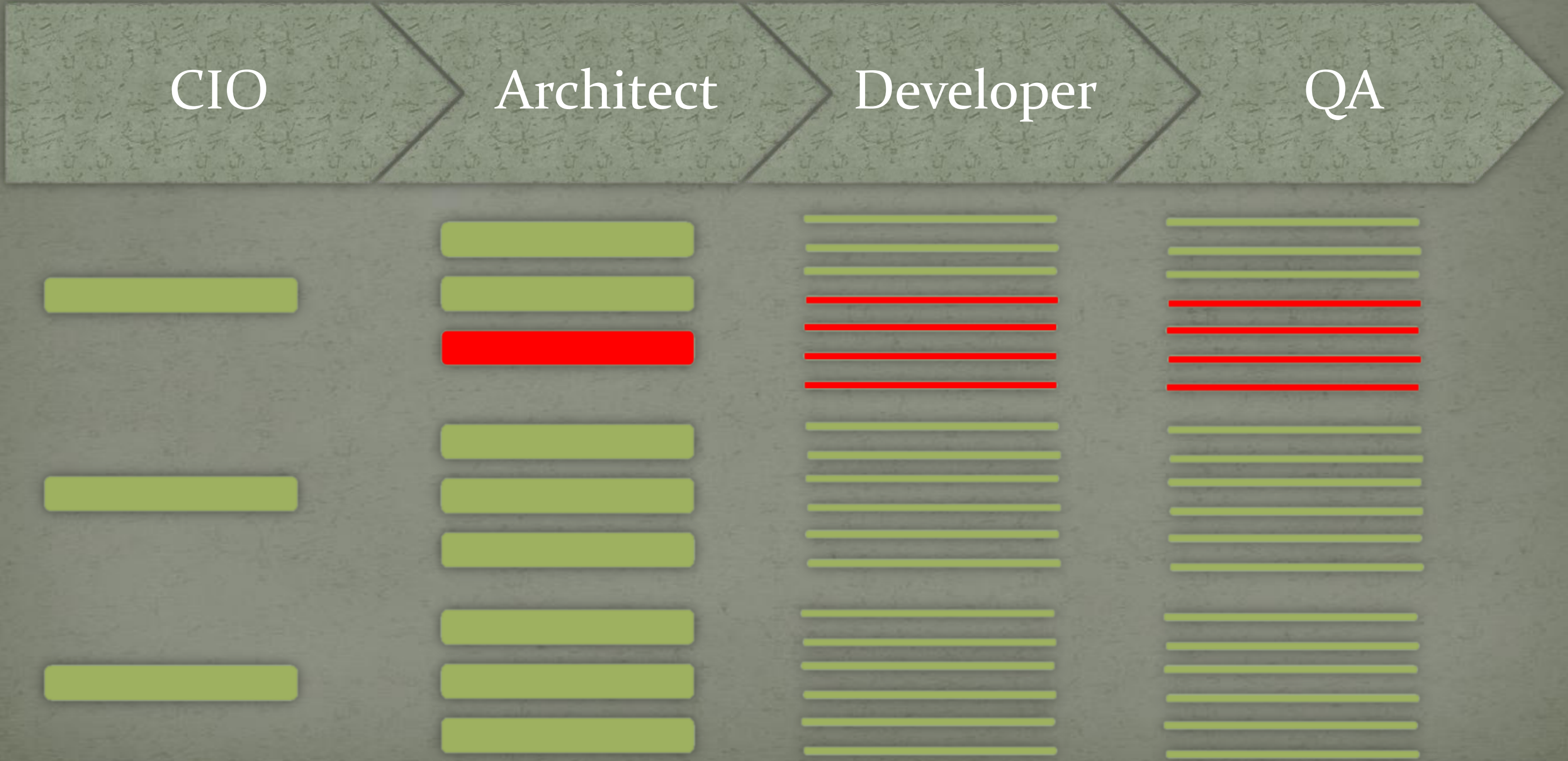
Wall of shame: dldb.org

# Rugged by Role

- Executives CIO/CTO
- Security "Analysts"
- Architects
- Developers
- Testers
- Program Managers

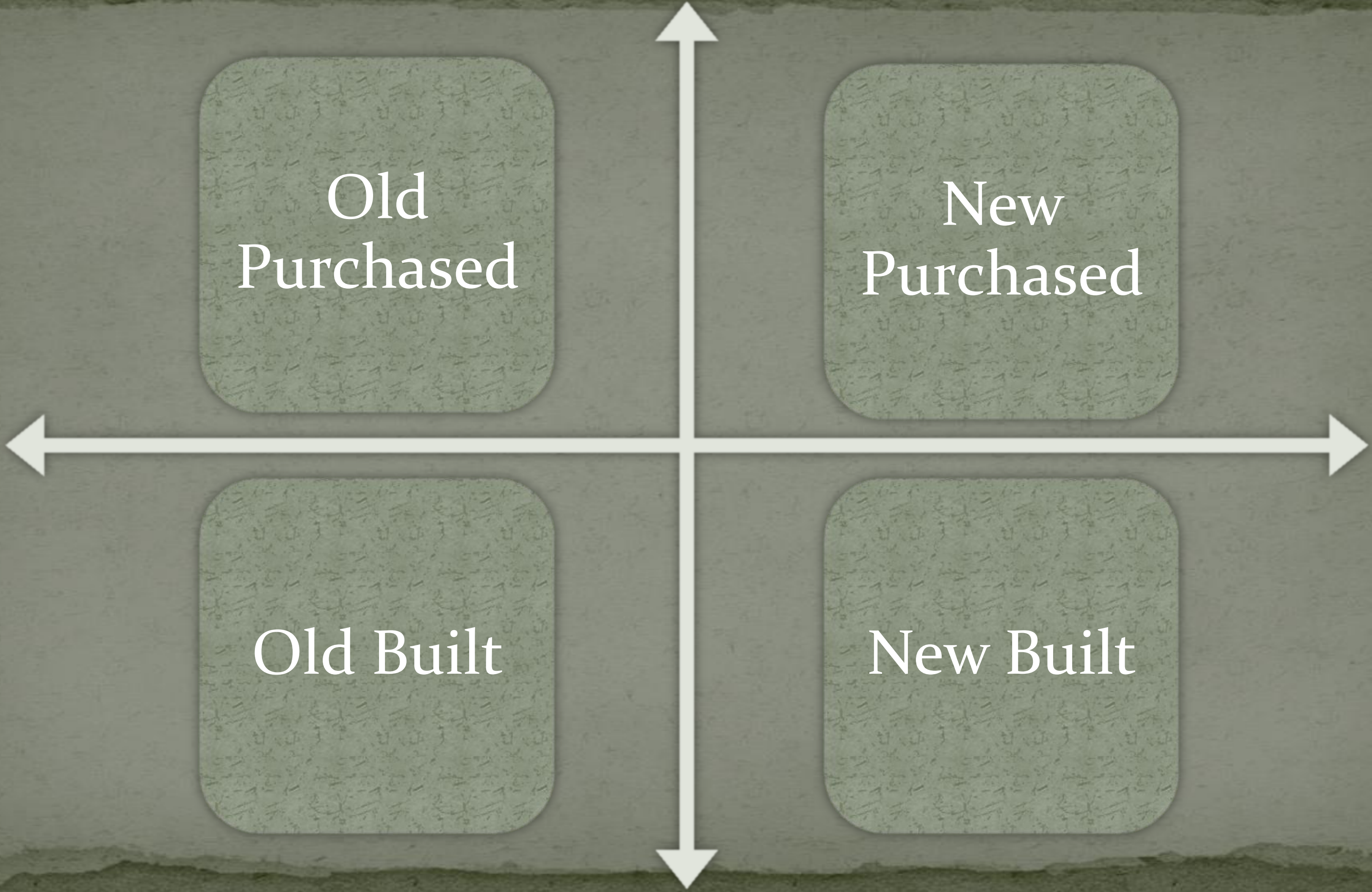


# Linkage and Efficiency



# To be added from the Rugged Summit

- Buying and selling software
- Understanding the entire software supply chain
- Network security, physical security, database security, etc…
- Other types of software projects, including legacy code, outsourced code, libraries, etc…
- Enterprise level security as opposed to individual projects



Old Purchased

New Purchased

Old Built

New Built

# Experimentation

An untested hypothesis is a wish

# Operational & Attitude

HONEY BADGER
DON'T CARE
memegenerator.net

HONEY BADGER
CARES

# Make it better

# THANK YOU
# My Collaborators

# Joshua Corman

[Knowledge Seeker | Zombie Killer]

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

@RuggedSoftware @RuggedDevOps
http://RuggedSoftware.org