RSA Conference2015
San Francisco | April 20-24 | Moscone Center

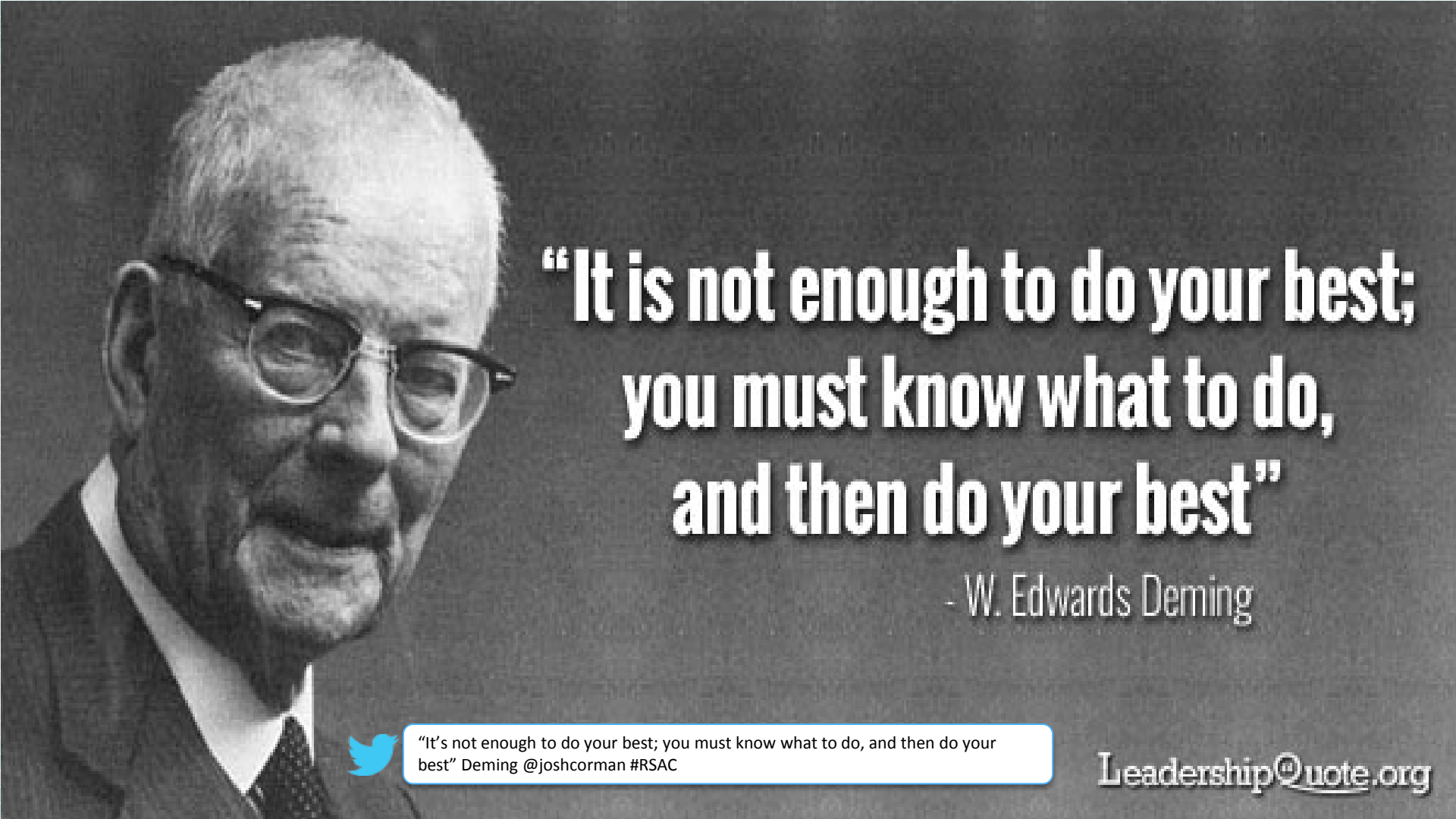
CHANGE
Challenge today's security thinking

SESSION ID: **FRM-R03**

CyberLegislation Is Upon Us… But Are *We* Ready?

Joshua Corman

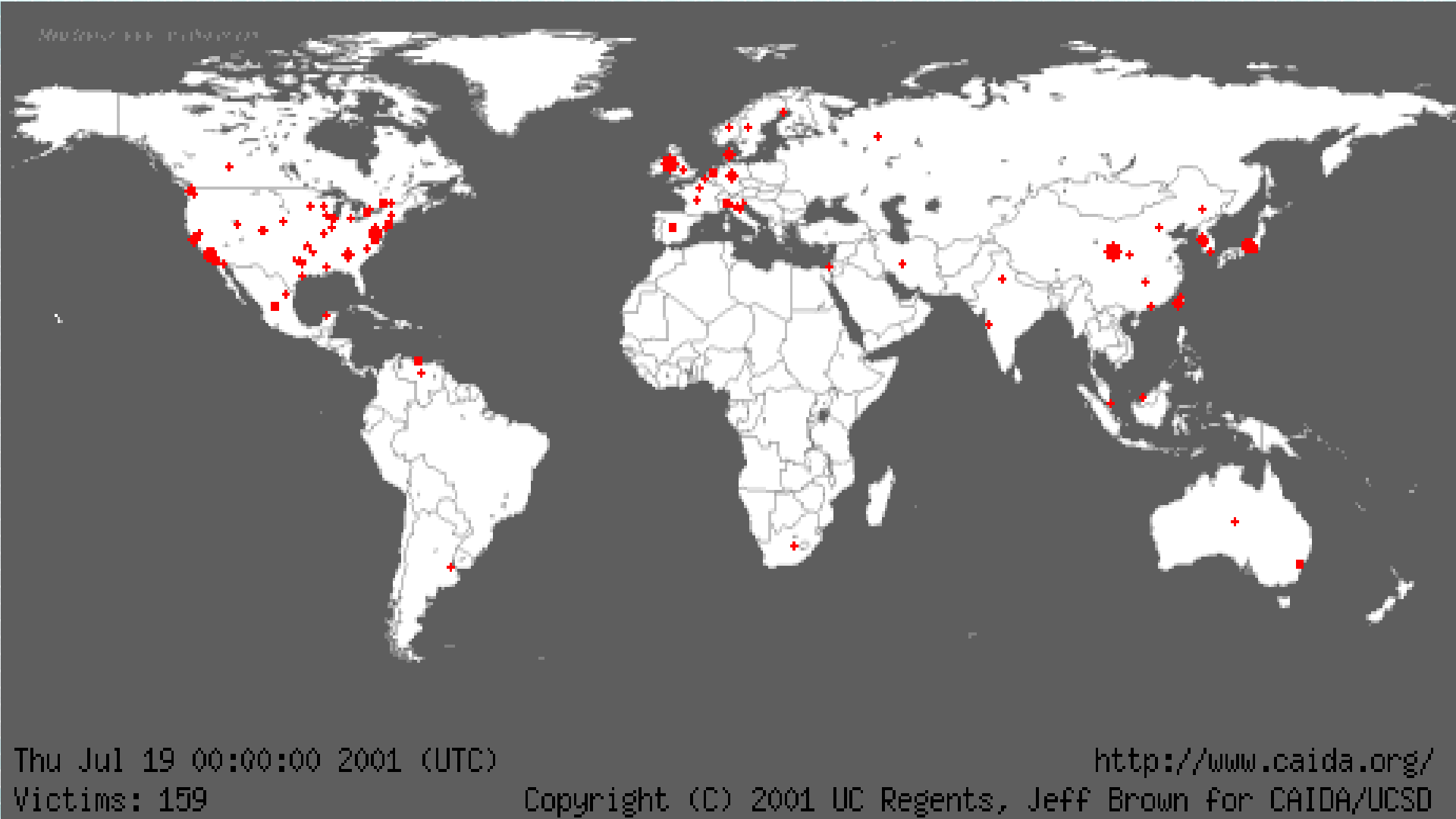
CTO, Sonatype
Founder, I am The Cavalry
@joshcorman @iamthecavalry


"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 #RSAC
LeadershipQuote.org

CYBER*

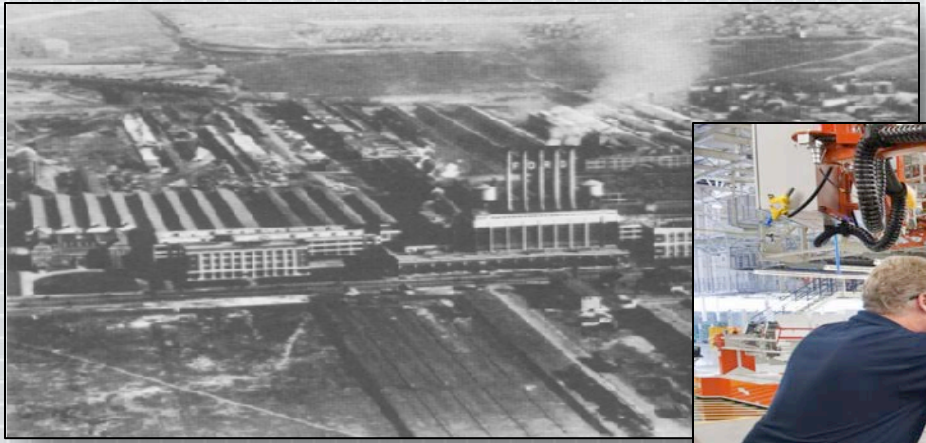
~ Marc Marc Andreessen 2011

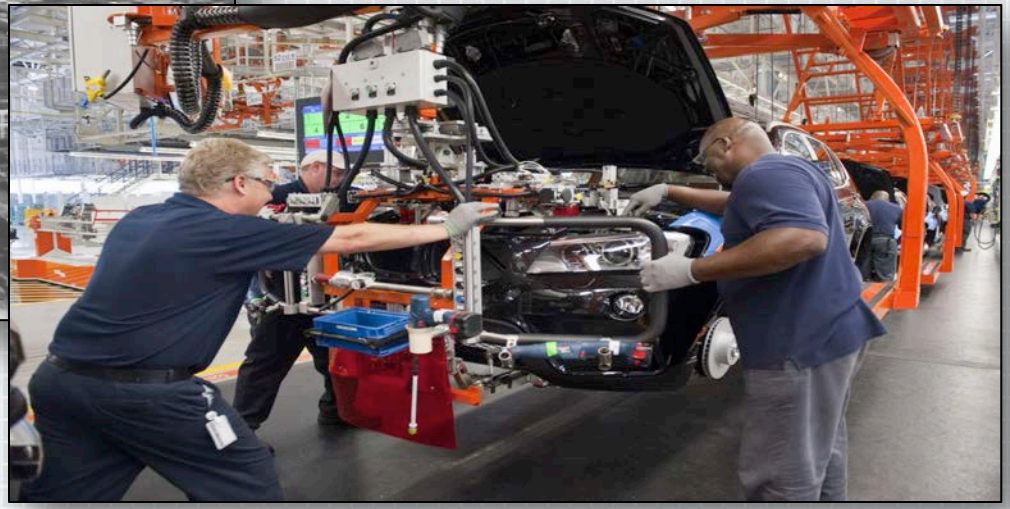
SOGETI


Thu Jul 19 00:00:00 2001 (UTC)
http://www.caida.org/
Victims: 159
Copyright (C) 2001 UC Regents, Jeff Brown for CAIDA/UCSD

Trade Offs
Costs & Benefits

Industrial Evolution





THE REAL IMPLICATIONS OF HEARTBLEED

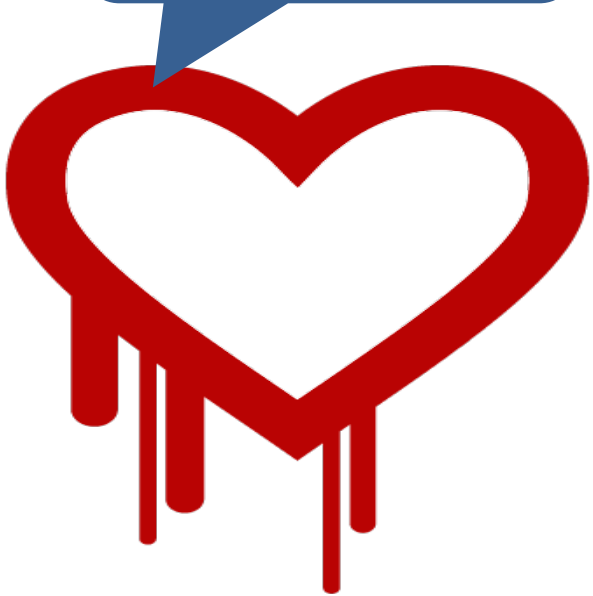
BEYOND HEARTBLEED: OPENSSL IN 2014

(31 IN NIST'S NVD THRU DECEMBER)

CVE-2014-3470	6/5/2014	CVSS Severity: 4.3 MEDIUM ← **SEIMENS** *
CVE-2014-0224	6/5/2014	CVSS Severity: 6.8 MEDIUM ← **SEIMENS** *
CVE-2014-0221	6/5/2014	CVSS Severity: 4.3 MEDIUM
CVE-2014-0195	6/5/2014	CVSS Severity: 6.8 MEDIUM
CVE-2014-0198	5/6/2014	CVSS Severity: 4.3 MEDIUM ← **SEIMENS** *
CVE-2013-7373	4/29/2014	CVSS Severity: 7.5 HIGH
CVE-2014-2734	4/24/2014	CVSS Severity: 5.8 MEDIUM ** DISPUTED **
CVE-2014-0139	4/15/2014	CVSS Severity: 5.8 MEDIUM
CVE-2010-5298	4/14/2014	CVSS Severity: 4.0 MEDIUM
CVE-2014-0160	**4/7/2014**	**CVSS Severity: 5.0 MEDIUM ← HeartBleed**
CVE-2014-0076	3/25/2014	CVSS Severity: 4.3 MEDIUM
CVE-2014-0016	3/24/2014	CVSS Severity: 4.3 MEDIUM
CVE-2014-0017	3/14/2014	CVSS Severity: 1.9 LOW
CVE-2014-2234	3/5/2014	CVSS Severity: 6.4 MEDIUM
CVE-2013-7295	1/17/2014	CVSS Severity: 4.0 MEDIUM
CVE-2013-4353	1/8/2014	CVSS Severity: 4.3 MEDIUM
CVE-2013-6450	1/1/2014	CVSS Severity: 5.8 MEDIUM

…

As of today, internet scans by MassScan reveal 300,000 of original 600,000 remain unpatched or unpatchable



Heartbleed + (UnPatchable) Internet of Things == ____ ?

#RSAC
@joshcorman
@iamthecavalry

In Our Bodies

In Our Homes

In Our Cars

In Our Infrastructure

ShellShock

{bashbug}

A TALE OF TWO QUAKES

In the span of two months, two massive earthquakes struck in Haiti and Chile. But while the temblor in Chile registered much higher on the Richter scale, the loss of life and damage in Haiti was far more severe. Why is that? Chile—which has experienced serious earthquakes in recent decades—has a robust building code to make sure buildings are earthquake resistant; Haiti has no code to speak of. And a look at both quake's scores on the Modified Mercali Intensity Scale—which is used to measure how earthquakes affect those experiencing them—shows that while Chile's quake may have been stronger overall, Haiti had a larger population and more urban areas hit by more intense and damaging shaking.

MODIFIED MERCALI INTENSITY SCALE

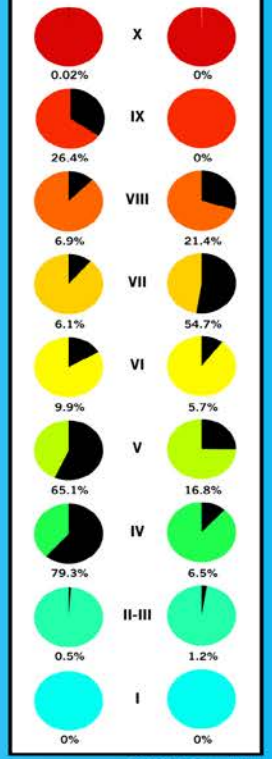
	Shaking	Structural Damage to Resistant Buildings	Structural Damage to Vulnerable Buildings
X	EXTREME	very heavy	very heavy
IX	VIOLENT	heavy	heavy
VIII	SEVERE	moderate/ heavy	heavy
VII	VERY STRONG	moderate	moderate/ heavy
VI	STRONG	light	moderate
V	MODERATE	very light	light
IV	LIGHT	none	none
II-III	WEAK	none	none
I	NOT FELT	none	none

HAITI

January 12, 2010
16:53 Local Time
7.0 Richter Scale
Estimated Fatalities:
230,000

Affected cities of Haiti and their population

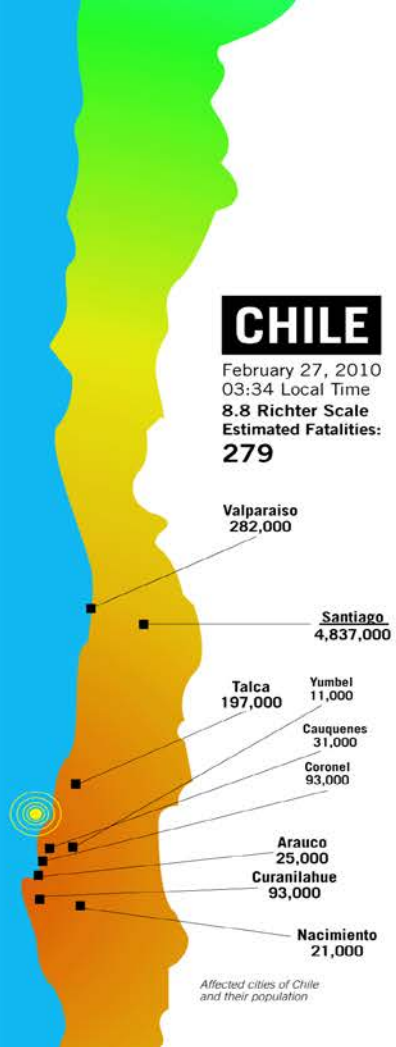
POPULATION AFFECTED
(percentage)



SOURCE U.S. Geological Survey
A collaboration between GOOD and kartssowitkar

CHILE

February 27, 2010
03:34 Local Time
8.8 Richter Scale
Estimated Fatalities:
279



Affected cities of Chile and their population

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 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.

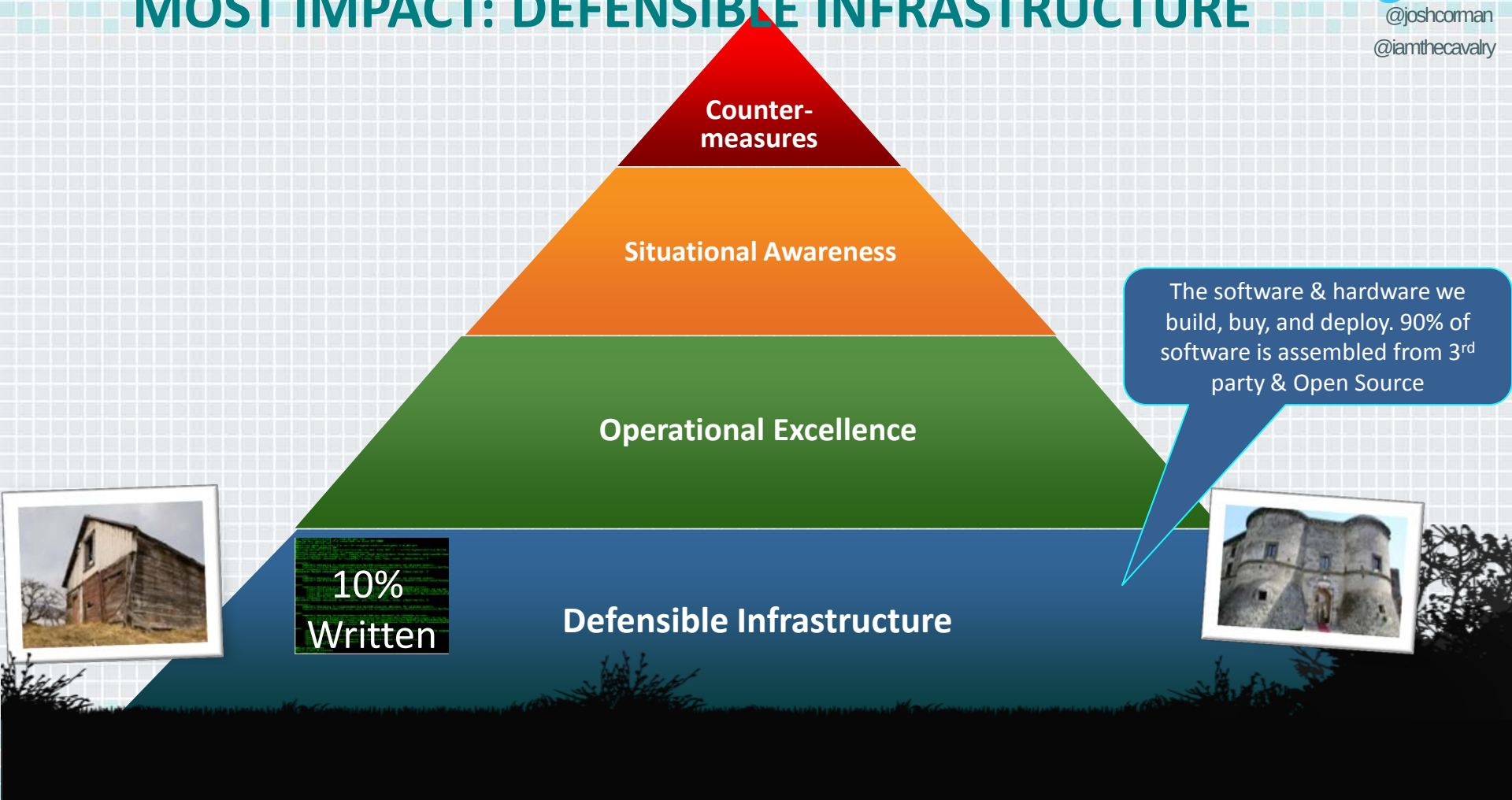
I am rugged because I refuse to be a source of vulnerability or weakness.

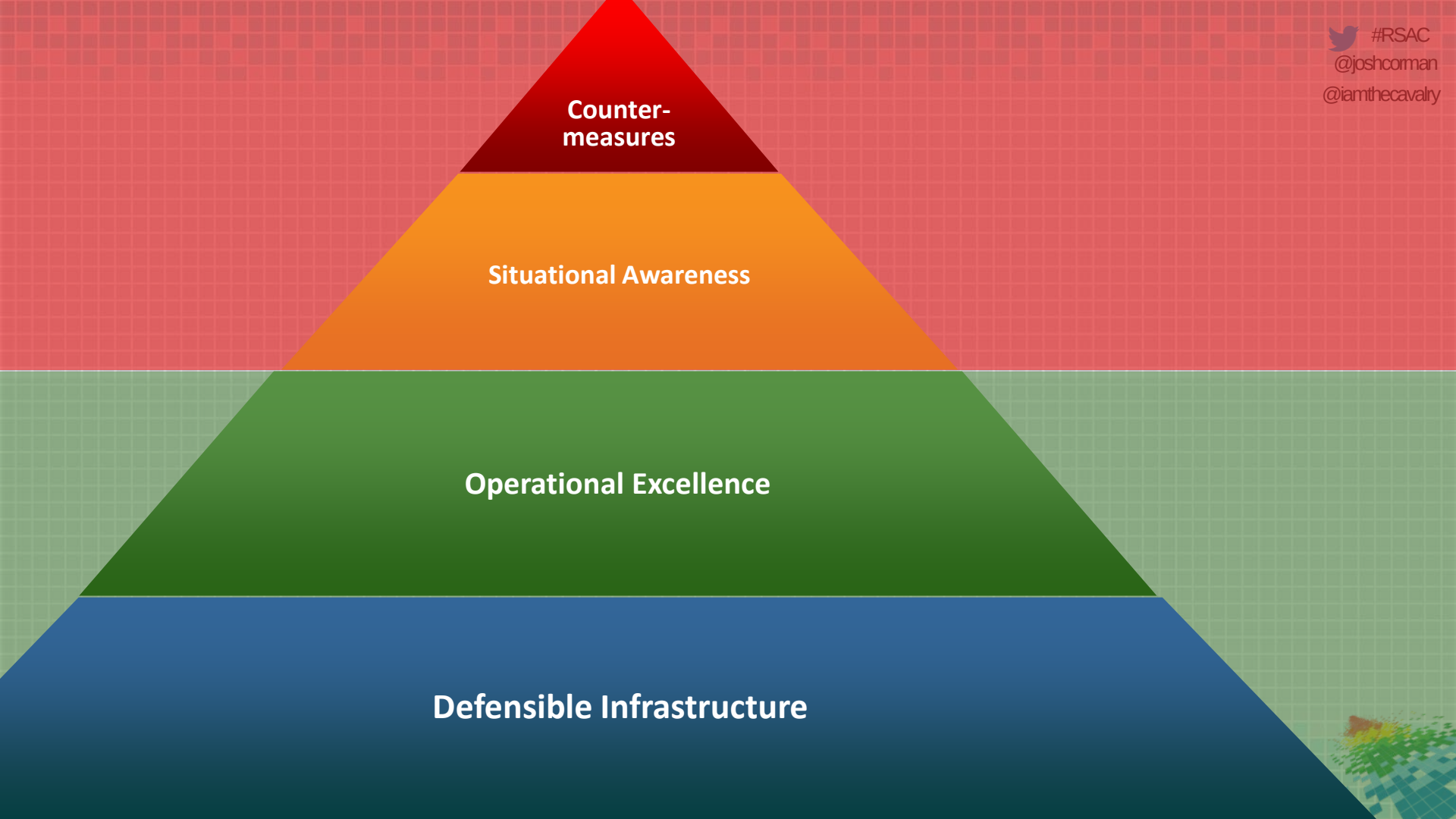
I am rugged because I assure my code will support its mission.

One Sentence…

MOST IMPACT: DEFENSIBLE INFRASTRUCTURE

#RSAC
@joshcorman
@iamthecavalry




Counter-measures
Situational Awareness
Operational Excellence
Defensible Infrastructure

#RSAC
@joshcorman
@iamthecavalry

Counter-measures

Situational Awareness

DevOps

Operational Excellence

DevOps

Defensible Infrastructure

DevOps

I Am The Cavalry

The Cavalry isn't coming… It falls to us

Problem Statement

Our society is adopting connected technology *faster than we are able to secure it*.

Mission Statement

To ensure connected technologies with the potential to impact public safety and human life are *worthy of our trust*.

Medical

Automotive

Connected Home

Public Infrastructure

Why Trust, public safety, human life
How Education, outreach, research
Who Infosec research community
Who Global, grass roots initiative
What Long-term vision for cyber safety

Collecting existing research, researchers, and resources
Connecting researchers with each other, industry, media, policy, and legal
Collaborating across a broad range of backgrounds, interests, and skillsets
Catalyzing positive action sooner than it would have happened on its own

5-Star Framework

Addressing Automotive Cyber Systems

5-Star Capabilities

- ★ **Safety by Design** – Anticipate failure and plan mitigation
- ★ **Third-Party Collaboration** – Engage willing allies
- ★ **Evidence Capture** – Observe and learn from failure
- ★ **Security Updates** – Respond quickly to issues discovered
- ★ **Segmentation & Isolation** – Prevent cascading failure

Connections and Ongoing Collaborations

Security Researchers

Automotive Engineers

Policy Makers

Insurance Analysts

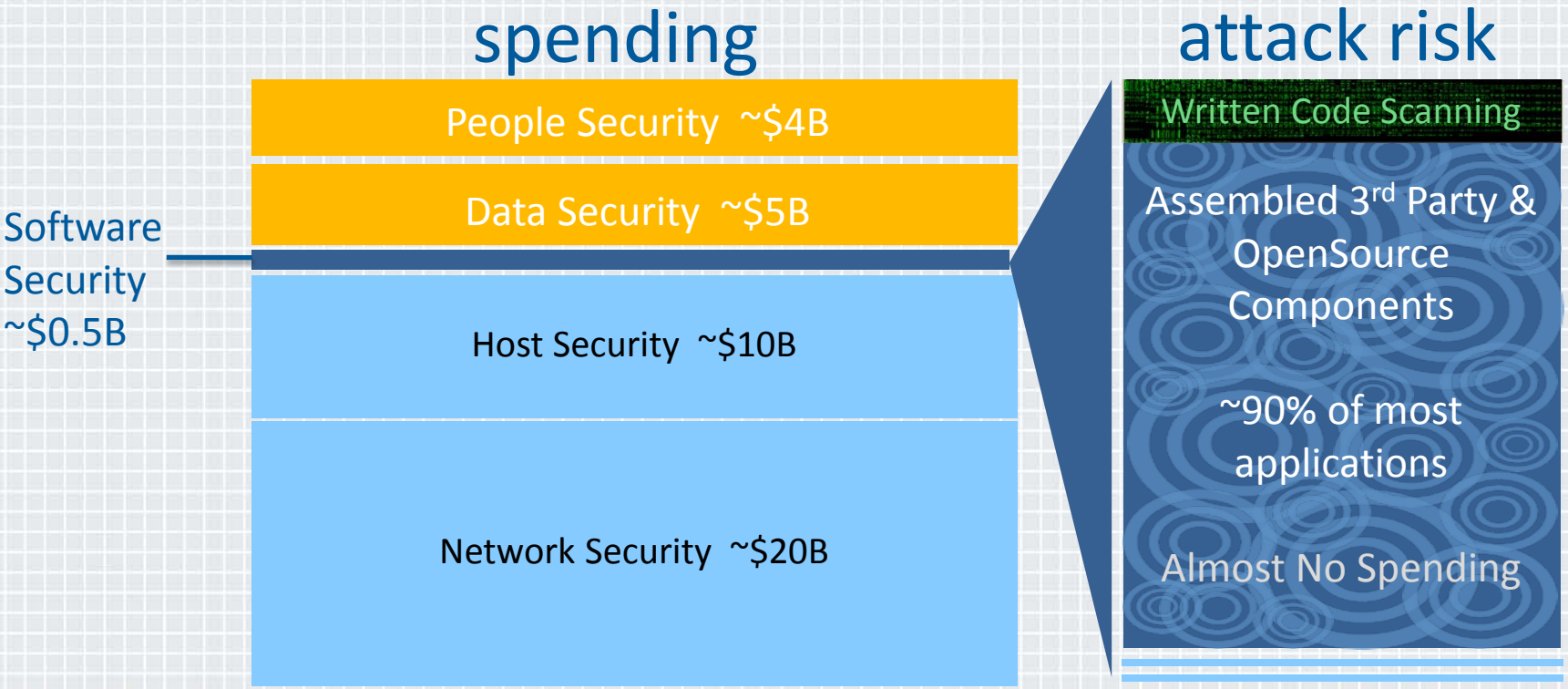
Accident Investigators

Standards Organizations

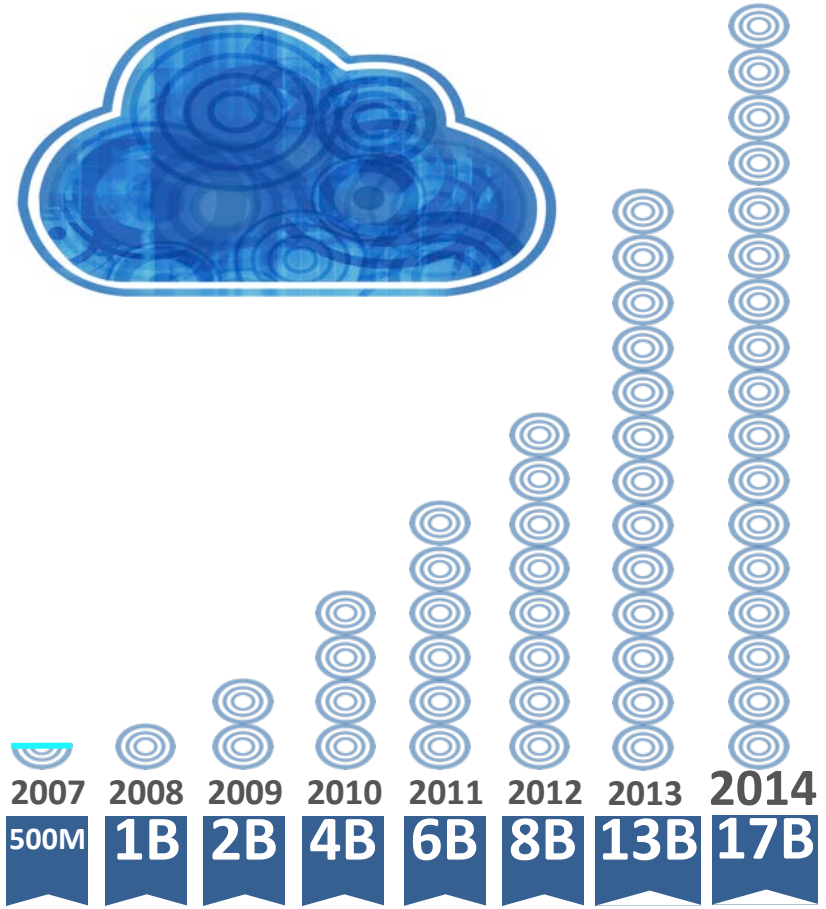
https://www.iamthecavalry.org/auto/5star/

SW Status Quo: Most attacked; least spend

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



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



Open source usage is

EXPLODING

Yesterday's source code is now replaced with

OPEN SOURCE

components

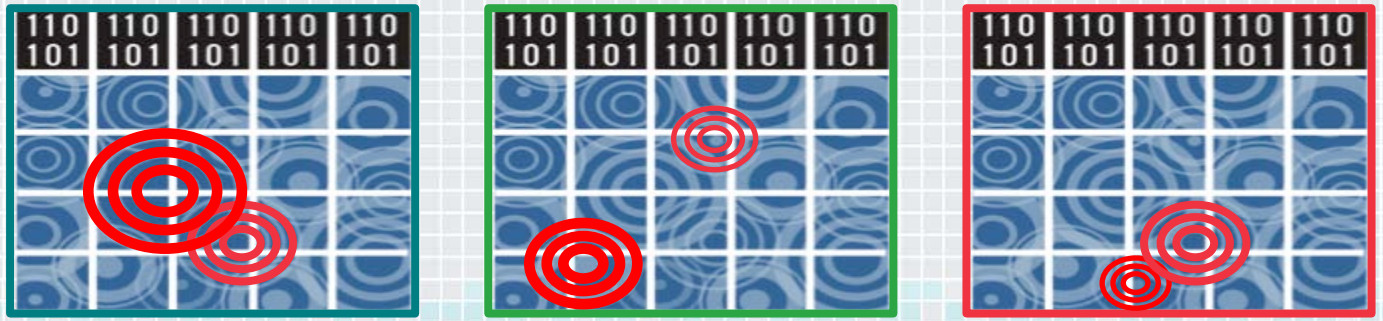
Source: Sonatype, Inc. analysis of (Maven) Central Repository component requests.

THINK LIKE AN ATTACKER

Now that software is

ASSEMBLED…

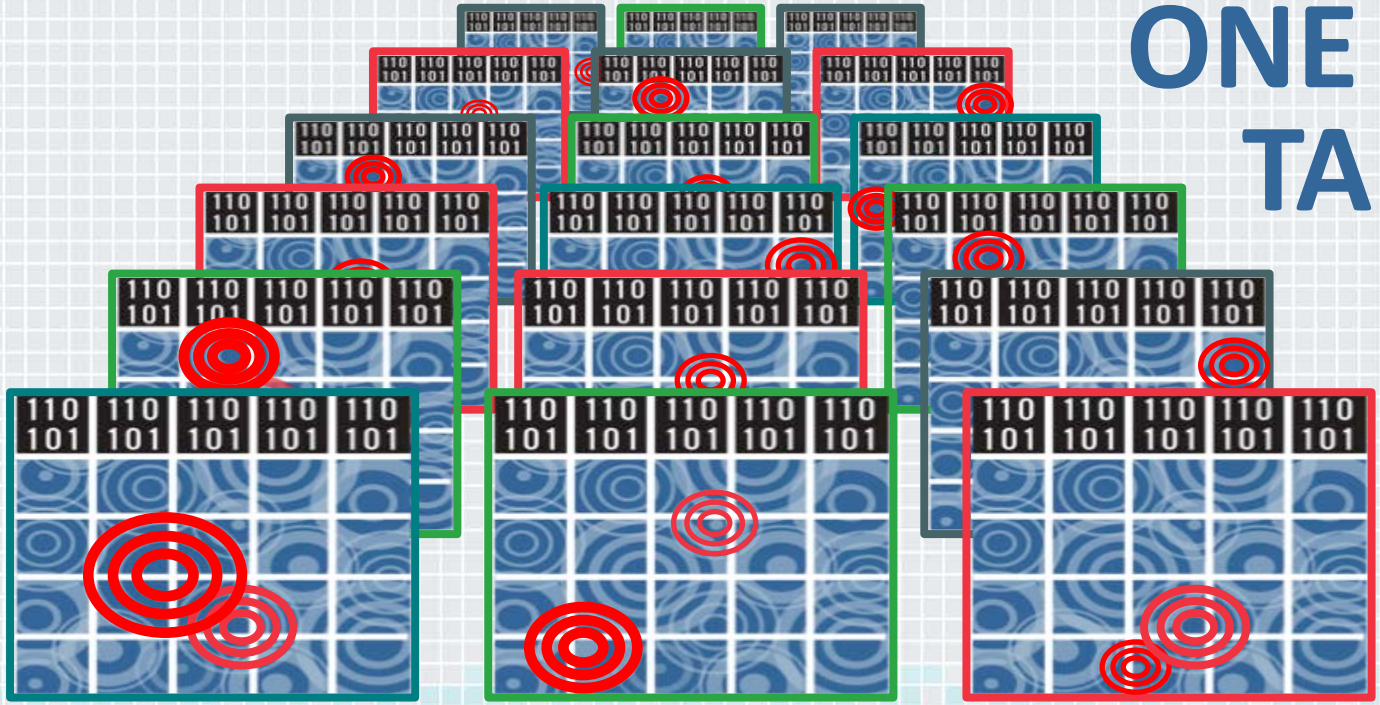
Our shared value becomes
our shared attack surface



THINK LIKE AN ATTACKER

One risky component,
now affects thousands of victims

ONE EASY TARGET



STRUTS

Global Bank

Software Provider

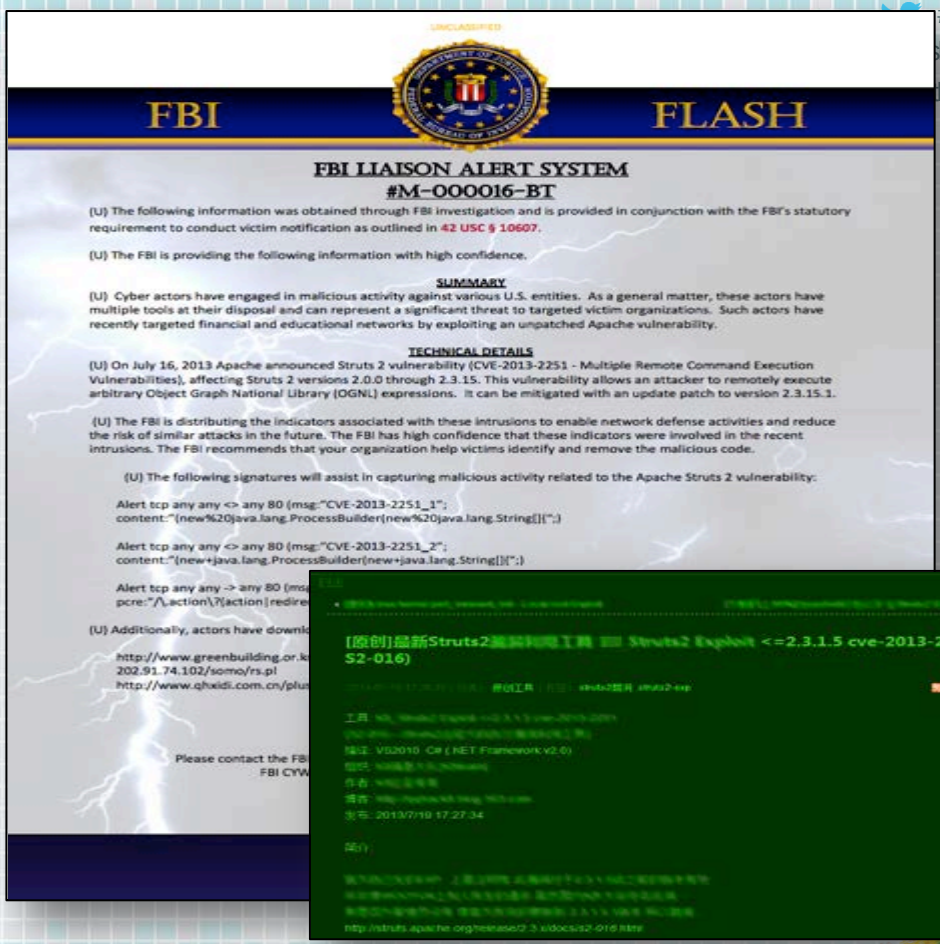
Software Provider's Customer

State University

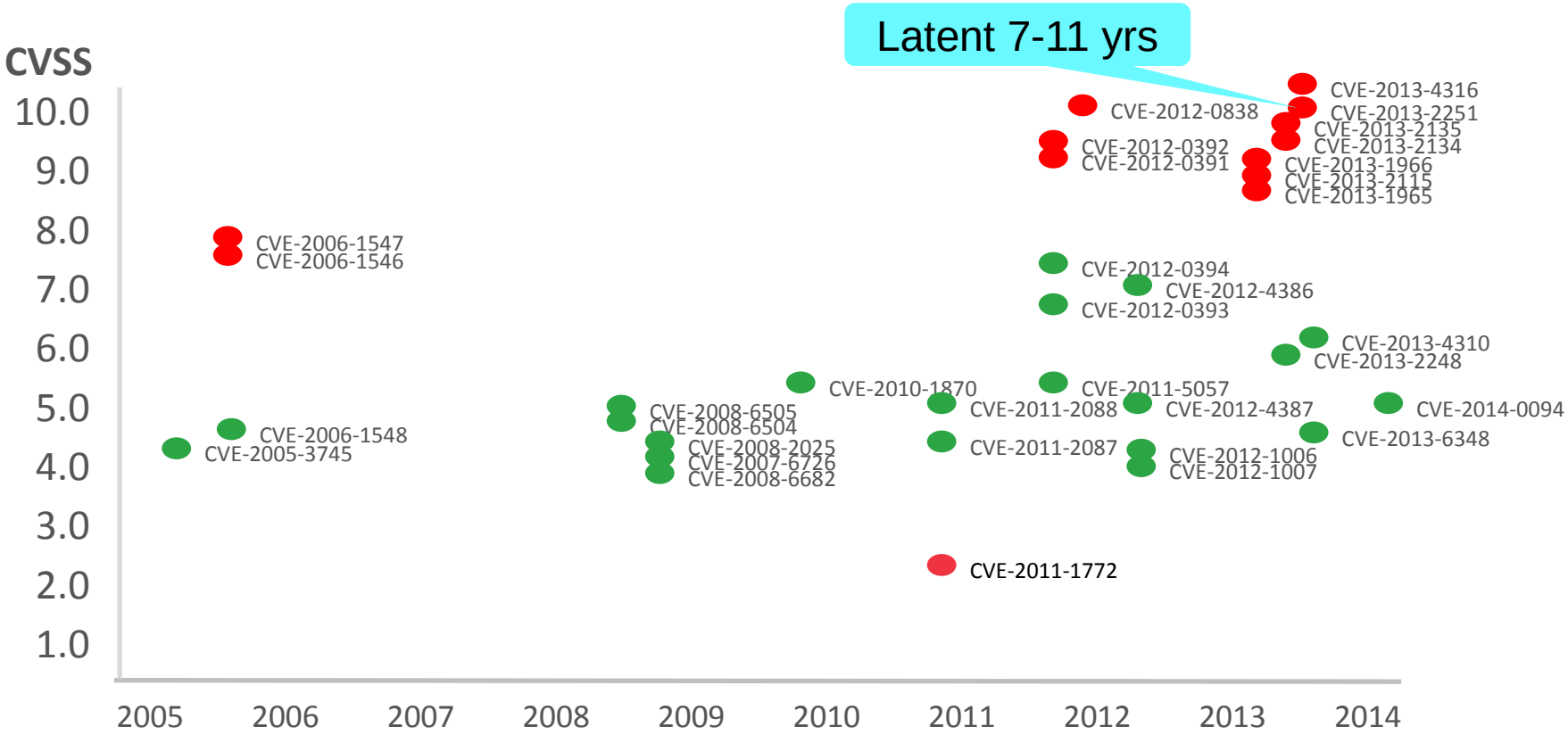
Three-Letter Agency

Large Financial Exchange

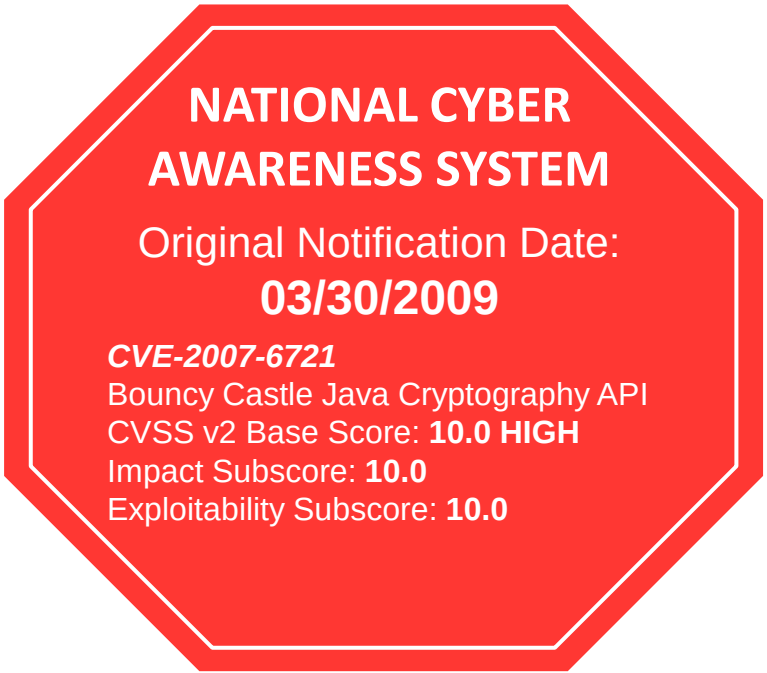
Hundreds of Other Sites



w/many eyeballs, all bugs are SHALLOW? Struts



BOUNCY CASTLE



In 2013, **4,000**
organizations downloaded
a version of Bouncy Castle
with a level 10 vulnerability

20,000 TIMES ...

Into **XXX,XXX** Applications...

SEVEN YEARS

after the vulnerability was fixed

HTTPCLIENT 3.X

In December 2013,

6,916 DIFFERENT

organizations downloaded
a version of httpclient with broken
ssl validation (cve-2012-5783)

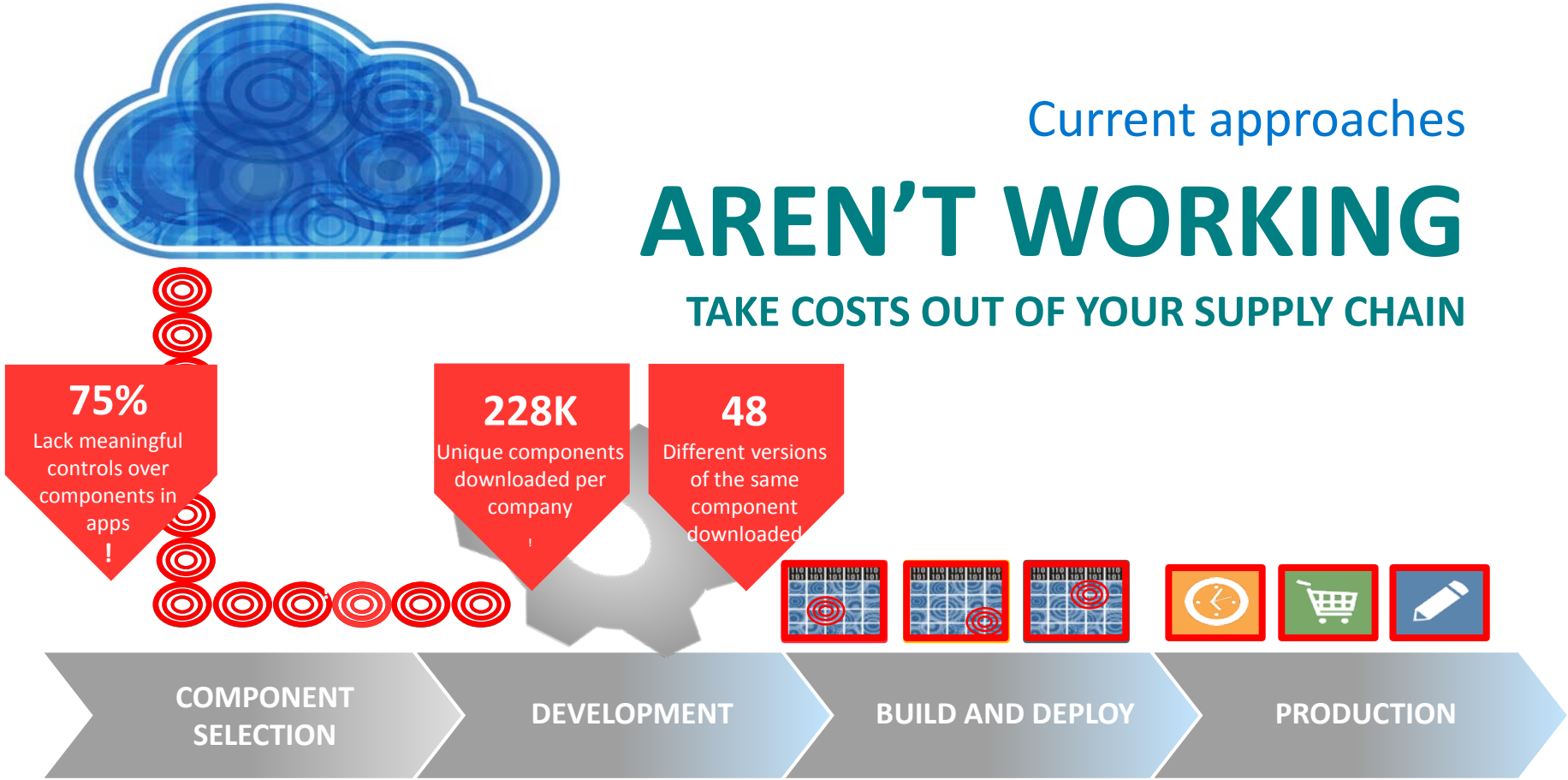
66,824 TIMES ...

More than **ONE YEAR AFTER THE ALERT**

Current approaches

AREN'T WORKING

TAKE COSTS OUT OF YOUR SUPPLY CHAIN



IS IT TIME FOR A SOFTWARE SUPPLY CHAIN?

PRESS RELEASES

Reps. Royce, Jenkins to Shore Up Security of Government Used Software

Washington, Dec 4, 2014 | Saat Alety (202-225-4111) | 0 comments

Today, U.S. Representatives Ed Royce (R-CA) and Lynn Jenkins (R-KS) introduced H.R. 5793, the "Cyber Supply Chain Management and Transparency Act of 2014." The legislation will ensure all contractors of software, firmware or products to the federal government provide the procuring agency with a bill of materials of all third party and open source components used, and demonstrate that those component versions have no known vulnerabilities.

"As a house is only as strong as its foundation, it's no wonder cyber attacks are on the rise with reports showing 71 percent of software contains components with critical vulnerabilities," said Rep. Royce. "This bill protects our nation's cyber infrastructure by ensuring the building blocks that make it up are secure and uncompromised."

"I have voiced concerns to the government agencies in charge of healthcare.gov that our nation's cyber infrastructure was vulnerable and not secure," said Rep. Jenkins. "But the problem is not limited to one website; the entire federal government lacks guidelines for website security. This vital legislation will put the appropriate checks and balances in place to ensure that the government has the tools it needs to create a more sound and secure system for taxpayers."

H.R. 5793 “CYBER SUPPLY CHAIN MANAGEMENT AND TRANSPARENCY ACT OF 2014”

Elegant Procurement Trio

1) Ingredients:

Anything sold to $PROCURING_ENTITY must provide a Bill of Materials of 3rd Party and Open Source Components (along with their Versions)

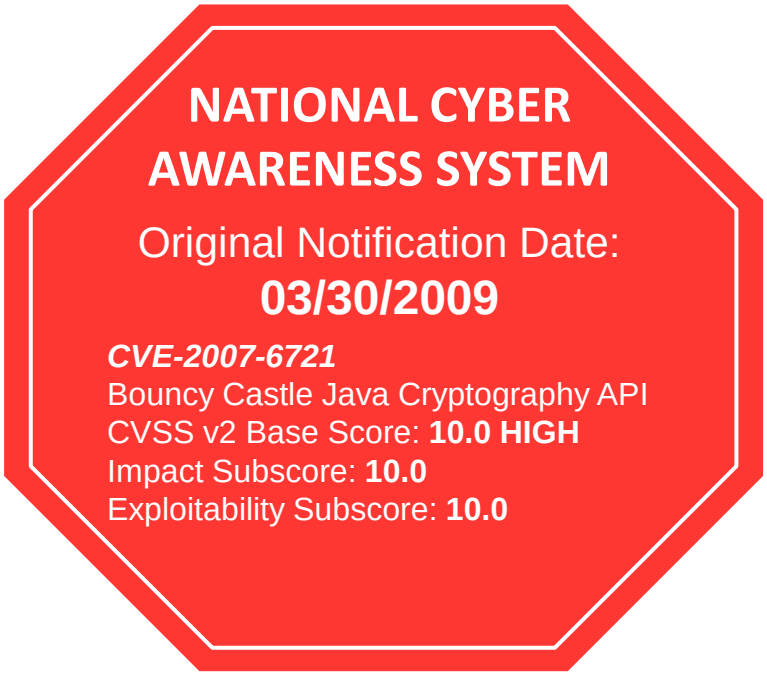
2) Hygiene & Avoidable Risk:

…and cannot use known vulnerable components for which a less vulnerable component is available (without a written and compelling justification accepted by $PROCURING_ENTITY)

3) Remediation:

…and must be patchable/updateable – as new vulnerabilities will inevitably be revealed

PROCUREMENT TRIO + BOUNCY CASTLE



In 2013, **4,000**

organizations downloaded
a version of Bouncy Castle
with a level 10 vulnerability

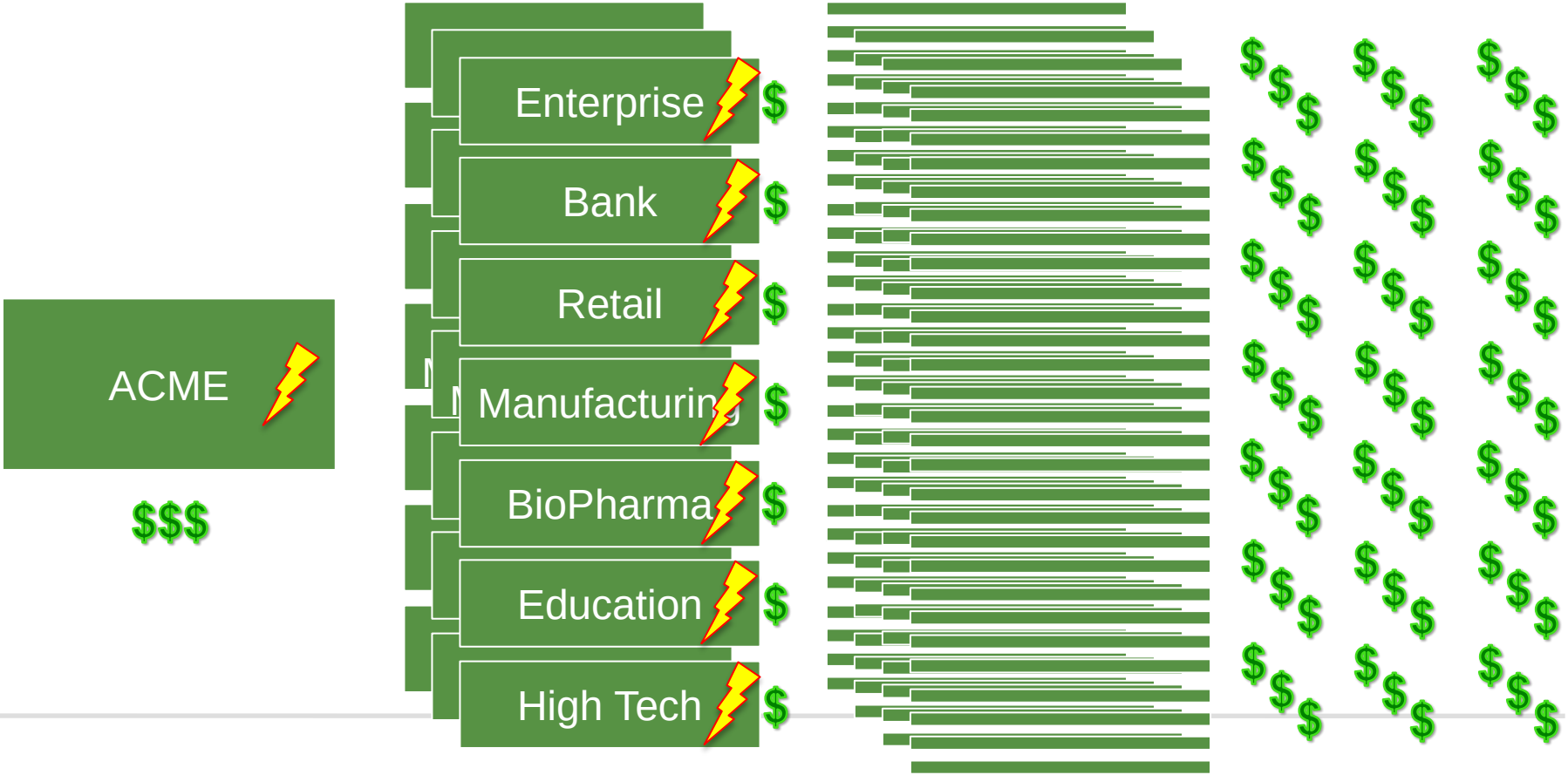
20,000 TIMES …

Into **XXX,XXX** Applications…

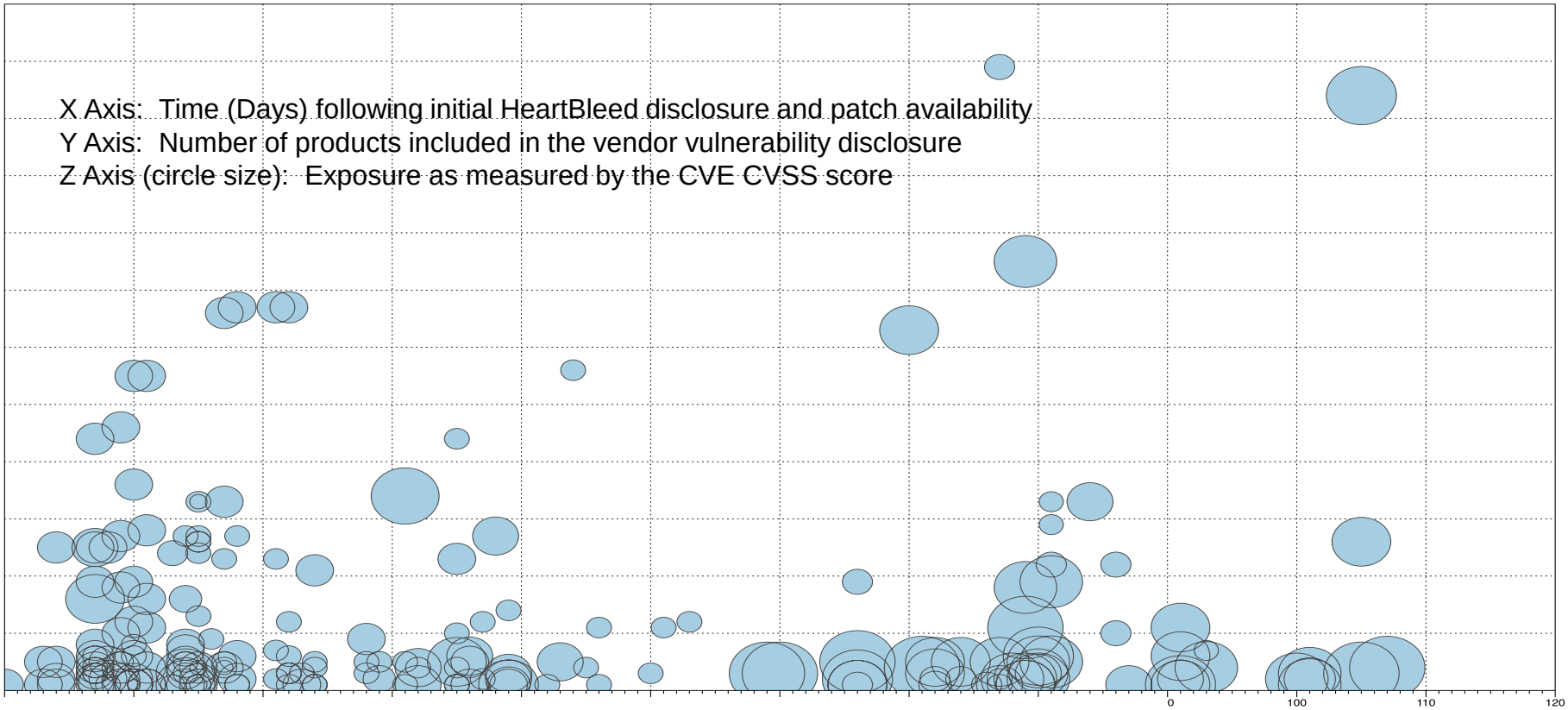
SEVEN YEARS

after the vulnerability was fixed

TRUE COSTS & LEAST COST AVOIDERS: DOWNSTREAM



COMMERCIAL RESPONSES TO OPENSSL



COLUMNS

Almost Too Big to Fail

DAN GEER AND JOSHUA CORMAN

Dan Geer is the CISO for In-Q-Tel and a security researcher with a quantitative bent. He has a long history with the USENIX Association, including officer positions, program committees, etc. dan@geer.org

Joshua Corman is the chief technology officer for Sonatype. Previously, Corman served as a security researcher and strategist at Akamai Technologies, The 451 Group, and IBM Internet Security Systems. A respected innovator, he co-founded Rugged Software and I Am the Cavalry to encourage new security approaches in response to the world's increasing dependence on digital infrastructure. He is also an adjunct faculty for Carnegie Mellon's Heinze College, IANS Research, and a Fellow at the Ponemon Institute. Josh received his bachelor's degree in philosophy, graduating summa cum laude, from the University of New Hampshire. joshcorman@gmail.com

Both dependence on open source and adversary activity around open source are widespread and growing, but the dynamic pattern of use requires new means to estimate if not bound the security implications. In April and May 2014, every security writer has talked about whether it is indeed true that with enough eyeballs, all bugs are shallow. We won't revisit that topic because there may be no minds left to change. Unarguably:

- Dependence on open source is growing in volume and variety.
- Adversary interest tracks installed base.
- Multiple levels of abstraction add noise to remediation needs.

We begin with two open source examples.

Apache Struts CVE-2013-2251, July 6, 2013 - CVSS v2 9.3
Apache Struts is one of the most popular and widely depended upon open source projects in the world. As such, when this highly exploitable vulnerability was discovered, it was promptly used to compromise large swaths of the financial services sector. While Heartbleed (see below) got full media frenzy, many affected by 2013-2251 learned of the problem from FBI victim notifications under 42 U.S.C. § 10607. The FS-ISAC issued guidance [1] telling institutions (read, victims) to scrutinize the security of third-party and open source components throughout their life cycle of use. It is not noteworthy that an open source project could have a severe vulnerability; what *is* of note is that this flaw went undetected for at least seven years (if not a lot longer from WebWork 2/pre-Struts 2 code base)—an existence proof that well-vetted code still needs a backup plan.

OpenSSL (Heartbleed) CVE-2014-0160, April 7, 2014 - CVSS v2 5.0
The Heartbleed vulnerability in OpenSSL garnered tremendous media and attacker activity this past April. While only scored with a CVSS of 5.0, it is a "5 with the power of a 10" since sniffing usernames, passwords, and SSL Certificates provides stepping stones to far greater impact. In contrast to the Struts bug above, this flaw was introduced only two years prior, but it, too, went unnoticed by many eyeballs—it was found by bench analysis [2].

Dependence on Open Source Is Growing

Sonatype, home to author Corman, serves as custodian to Central Repository, the largest parts warehouse in the world for open source components. At the macro level, open source consumption is exploding in Web applications, mobility, cloud, etc., driven in part by increasingly favorable economics. Even (risk averse, highly regulated) government and financial sectors, which previously resisted "code of unknown origin/quality/security," have begun relaxing their resistance. According to both Gartner surveys and Sonatype application analysis, 90+% of modern applications are not so much written as assembled from third-party building blocks. It is the open source building blocks that are taking the field, and not just for commodity applications (see Figure 1).

For the 41%
390 days (median 265 days). CVSS 10s 224 days.

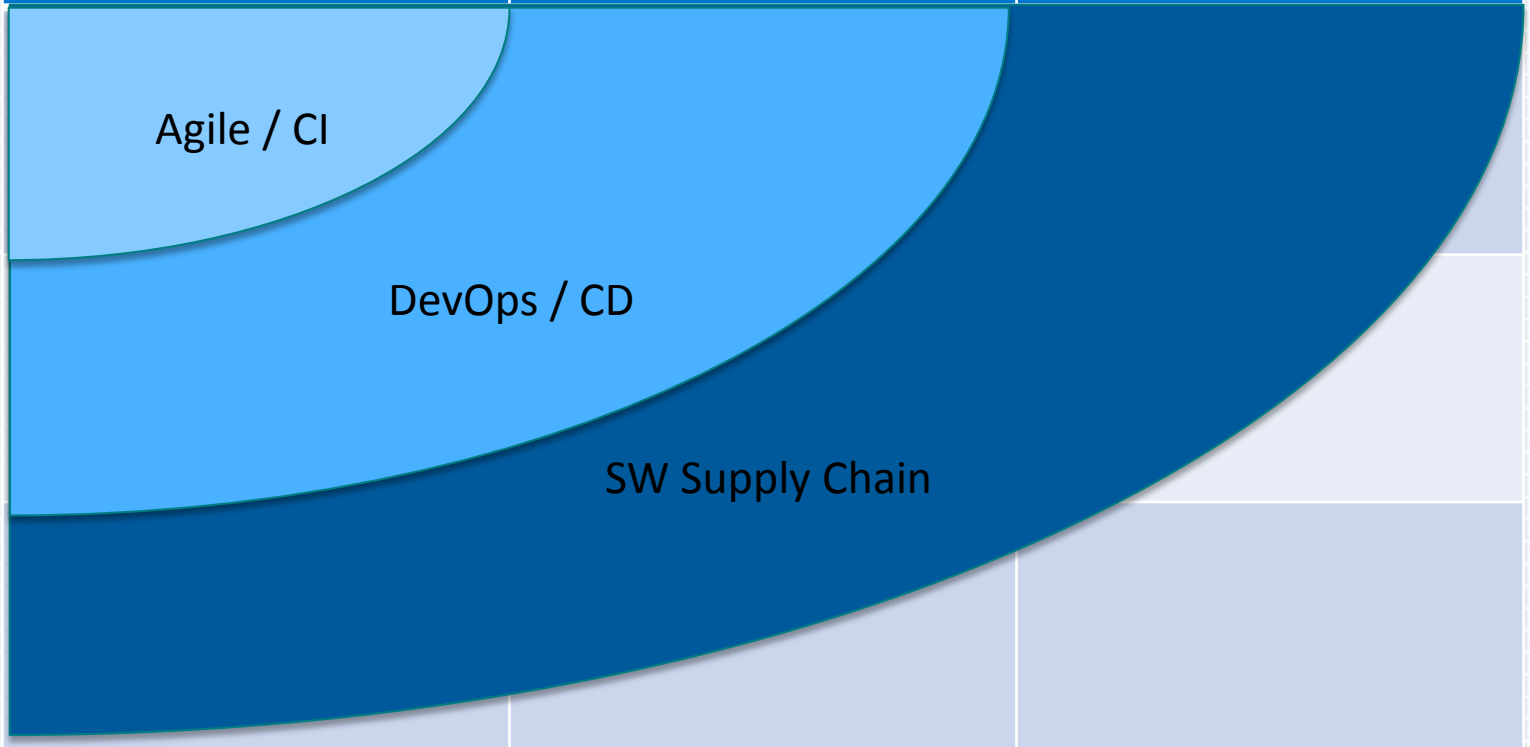
https://www.usenix.org/system/files/login/articles/15_geer_0.pdf

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

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

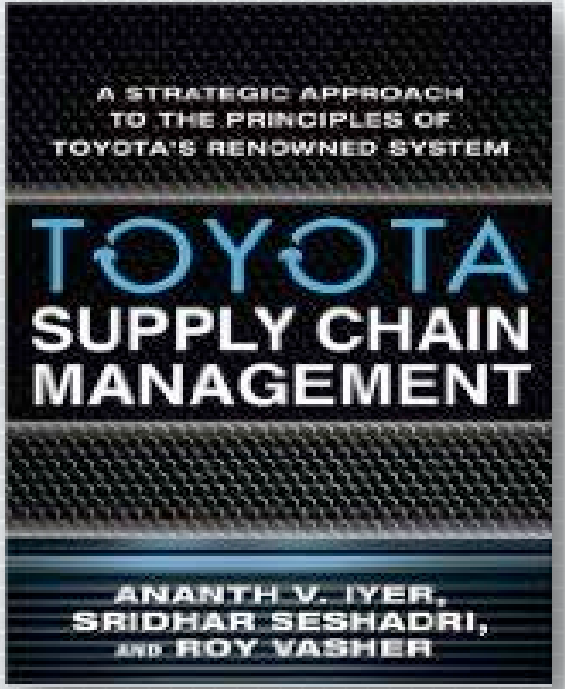
ON BUDGET.
More efficient.
More profitable.
More competitive.

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



Comparing the Prius and the Volt

	Toyota Advantage	Toyota Prius	Chevy Volt
Unit Cost	61%	$24,200	$39,900
Units Sold	13x	23,294	1,788
In-House Production	50%	27%	54%
Plant Suppliers	16% (10x per)	125	800
Firm-Wide Suppliers	*4%*	*224*	*5,500*



TWO LITTLE WORDS

KNOWN VULNERABILITIES

Bonus: Hot off the presses 2015 VZ DBIR

#RSAC
@joshcorman
@iamthecavalry

NOT ALL CVES ARE CREATED EQUAL.

If we look at the frequency of exploitation in Figure 11, we see a much different picture than what's shown by the raw vulnerability count of Figure 12. Ten CVEs account for almost 97% of the exploits observed in 2014. While that's a pretty amazing statistic, don't be lulled into thinking you've found an easy way out of the vulnerability remediation rodeo. Prioritization will definitely help from a risk-cutting perspective, but beyond the top 10 are 7 million other exploited vulnerabilities that may need to be ridden down. And therein, of course, lies the challenge; once the "mega-vulns" are roped in (assuming you could identify them ahead of time), how do you approach addressing the rest of the horde in an orderly, comprehensive, and continuous manner over time?

About half of the CVEs exploited in 2014 went from publish to pwn in less than a month.

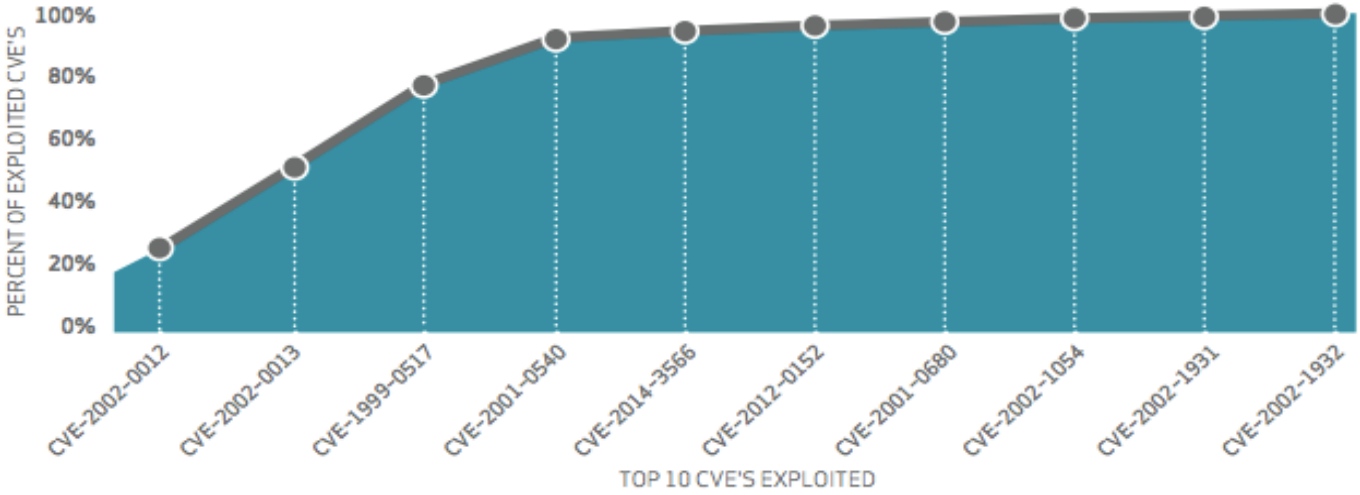
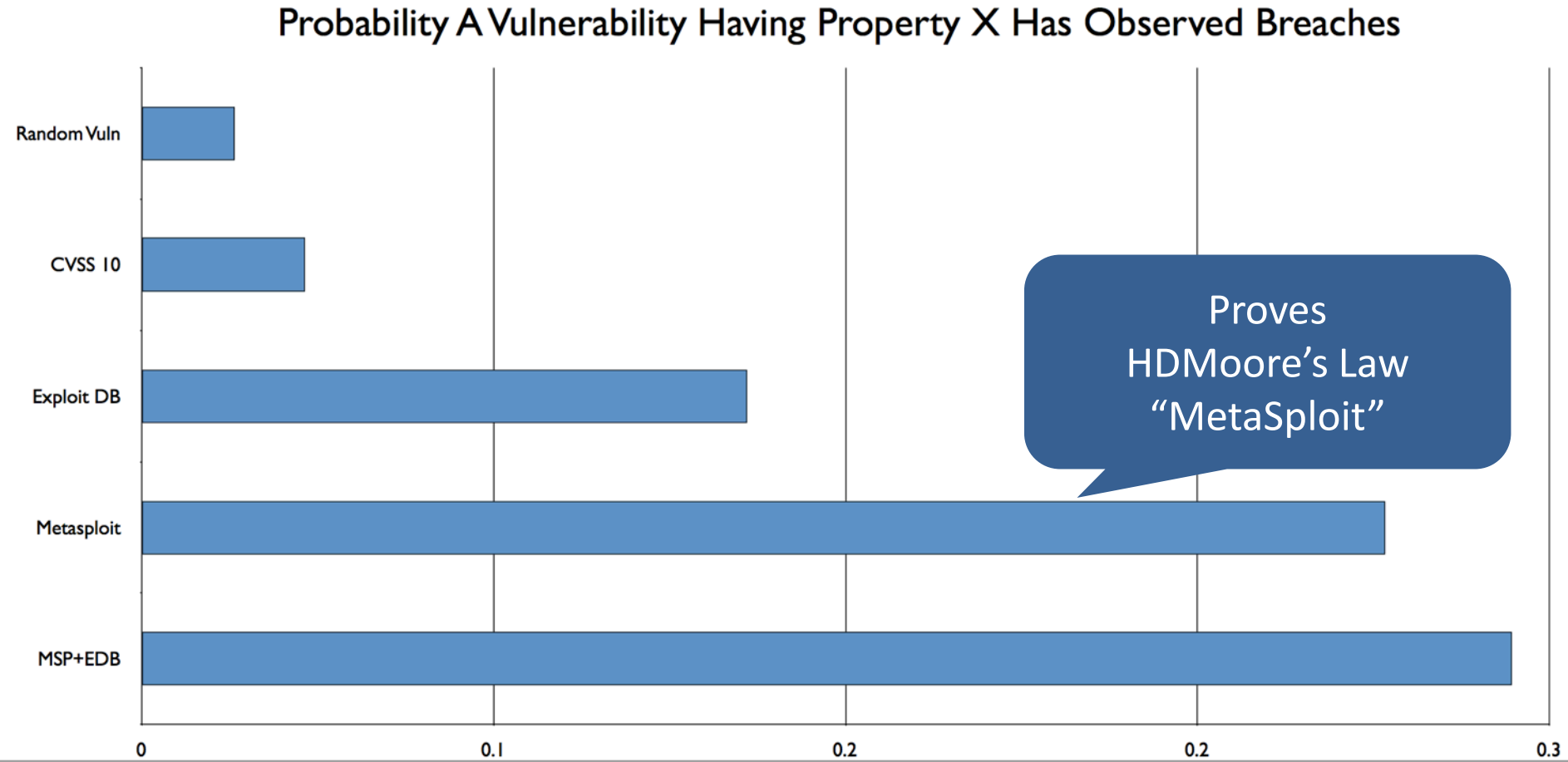


Figure 11.

Cumulative percentage of exploited vulnerabilities by top 10 CVEs

I Love It When You Call Me Big Data



Order of operations

Known Vulnerabilities | Unknown

1) Got Logo?

2) HDMoore's Law

3) CVSS + _

4) Other

Heartbleed + (UnPatchable) Internet of Things == ____ ?

#RSAC
@joshcorman
@iamthecavalry

In Our Bodies

In Our Homes

In Our Cars

In Our Infrastructure

H.R. 5793 “CYBER SUPPLY CHAIN MANAGEMENT AND TRANSPARENCY ACT OF 2014”

Elegant Procurement Trio

1) Ingredients:

Anything sold to $PROCURING_ENTITY must provide a Bill of Materials of 3rd Party and Open Source Components (along with their Versions)

2) Hygiene & Avoidable Risk:

…and cannot use known vulnerable components for which a less vulnerable component is available (without a written and compelling justification accepted by $PROCURING_ENTITY)

3) Remediation:

…and must be patchable/updateable – as new vulnerabilities will inevitably be revealed

Markey, Blumenthal To Introduce Legislation to Protect Drivers from Auto Security and Privacy Vulnerabilities with Standards and "Cyber Dashboard"

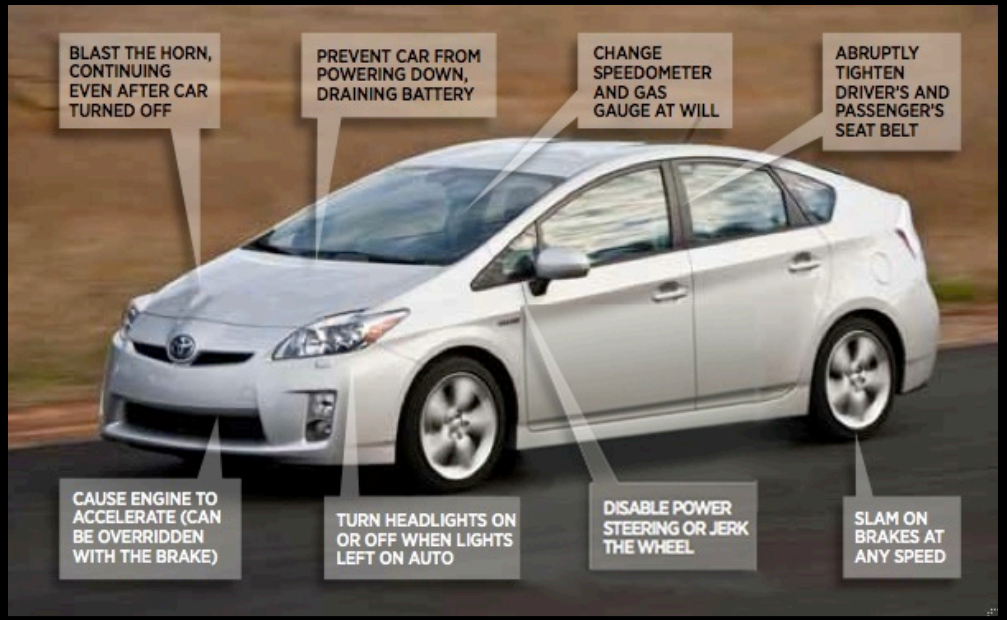
Wednesday, February 11, 2015

Sen. Markey released report this week that revealed wireless technologies are leading to a host of automobile security and privacy vulnerabilities

Automotive Cyber Safety

Facts, Fiction, and a ‘Vehicle’ for Collaboration

! $4f3 @ * $p33d



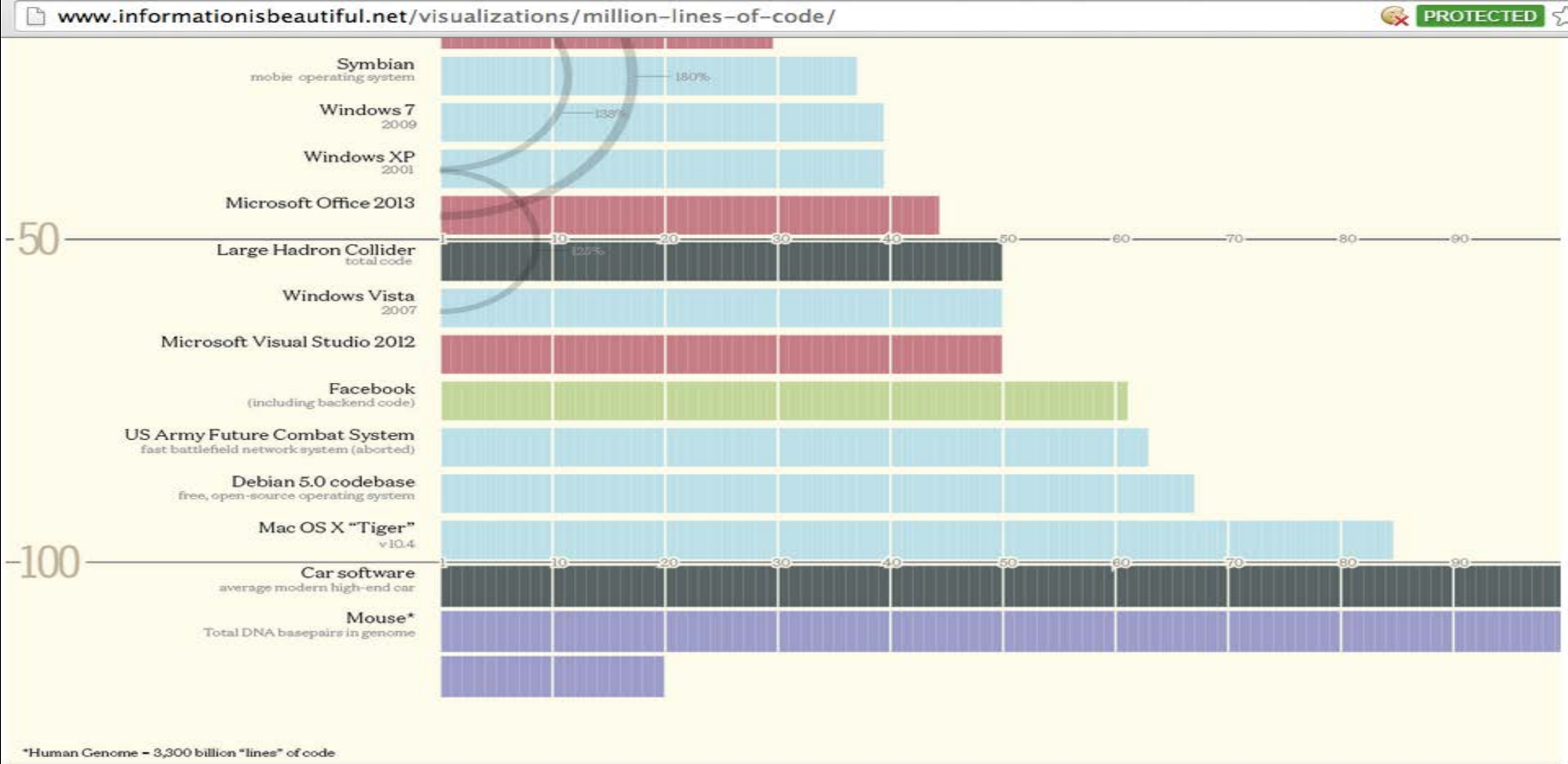
www.iamthecavalry.org
@iamthecavalry

All Systems Fail*

* Yes; all

Poll

Does anyone think vehicles will not be hacked?



*Human Genome = 3,300 billion "lines" of code

concept & design: David McCandless
informationisbeautiful.net
research: Pearl Doughty-White, Miriam Quick

Distances for Hacking Car Features

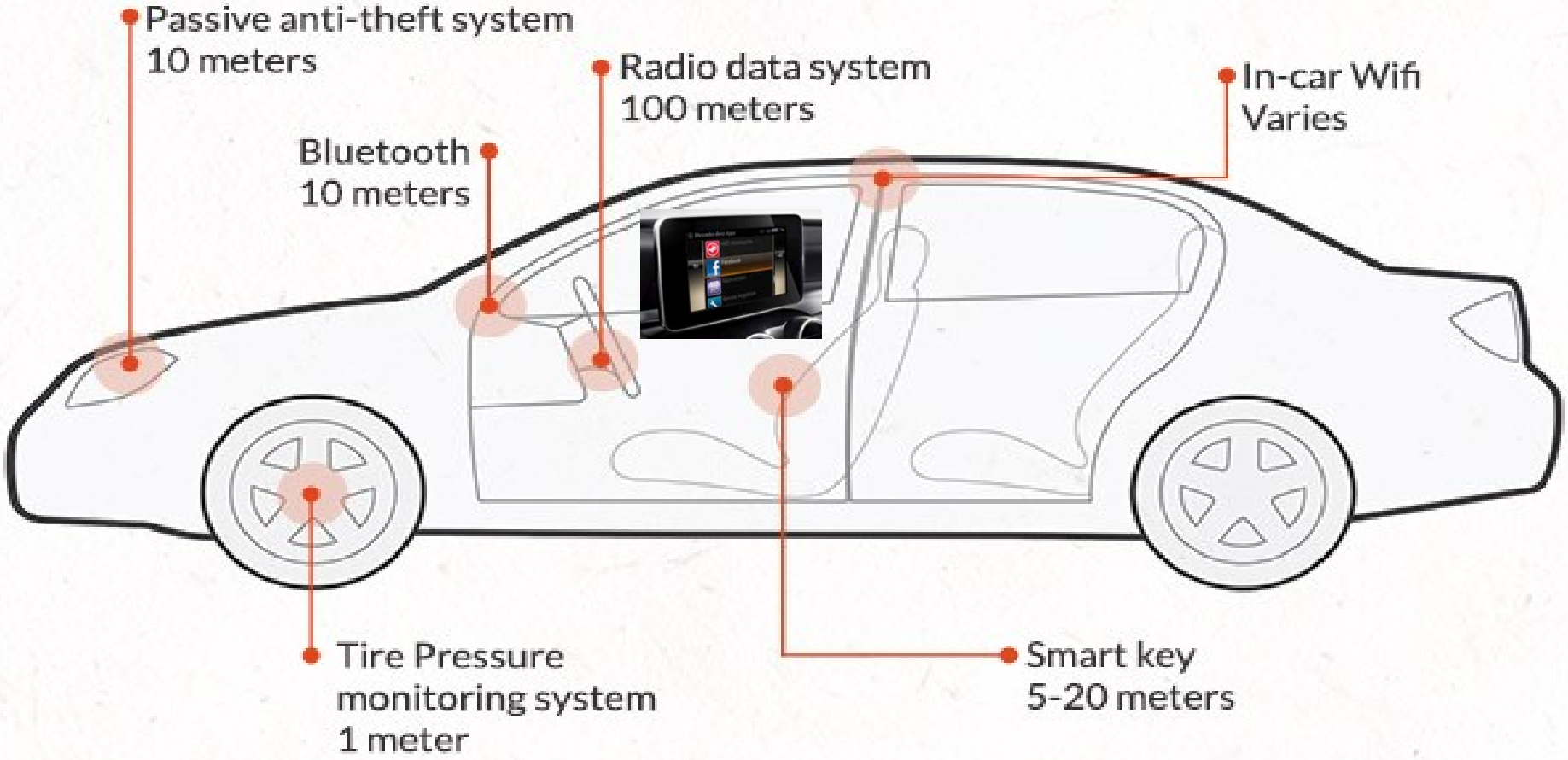


ILLUSTRATION: CNNMONEY

“But they *wouldn’t* hurt you!”

“I’d prefer that they *couldn’t* hurt me…”

Markey, Blumenthal To Introduce Legislation to Protect Drivers from Auto Security and Privacy Vulnerabilities with Standards and "Cyber Dashboard"

Wednesday, February 11, 2015

Sen. Markey released report this week that revealed wireless technologies are leading to a host of automobile security and privacy vulnerabilities

Lawsuit seeks damages against automakers and their hackable cars

A Senate report backs up claims that automakers haven't addressed electronic security

MORE LIKE THIS

Security, privacy gaps put U.S. drivers at risk of hacking

With $15 in Radio Shack parts, 14-year-old hacks a car

Carmakers promise they'll protect driver privacy -- really

on IDG Answers

What were the best new things introduced at this year's CES?

5-Star Cyber Safety

Formal Capacities

1. **Safety By Design**
2. **Third Party Collaboration**
3. **Evidence Capture**
4. **Security Updates**
5. **Segmentation and Isolation**

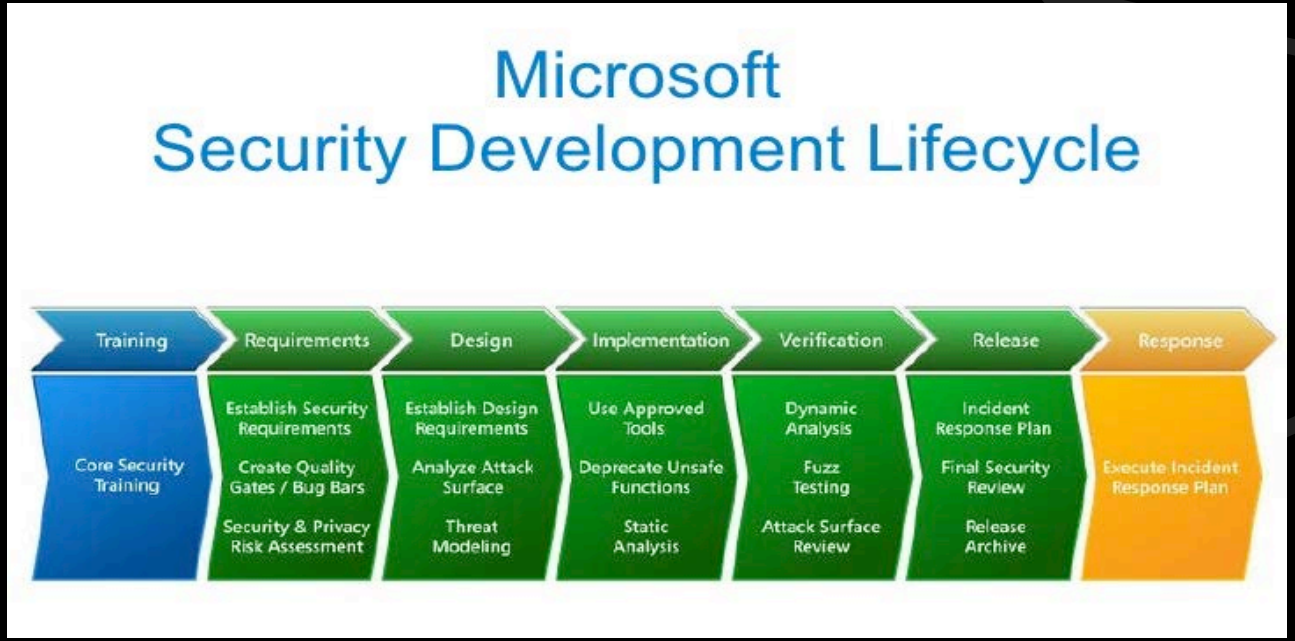
Plain Speak

1. Avoid Failure
2. Engage Allies To Avoid Failure
3. Learn From Failure
4. Respond to Failure
5. Isolate Failure

1) Safety By Design

Do you have a published attestation of your Secure Software Development Lifecycle, summarizing your design, development, and adversarial resilience testing programs for your products and your supply chain?

1) Safety By Design



2) Third Party Collaboration

Do you have a published Coordinated Disclosure policy inviting the assistance of third-party researchers acting in good faith?

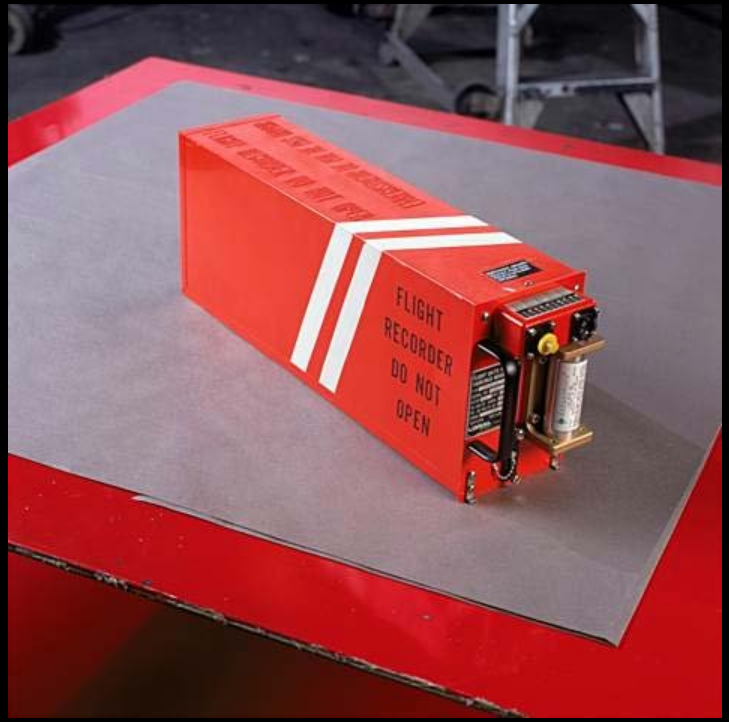
2) Third Party Collaboration

Vs

3) Evidence Capture

Do your vehicle systems provide tamper evident, forensically-sound logging and evidence capture to facilitate safety investigations?

3) Evidence Capture



4) Security Updates

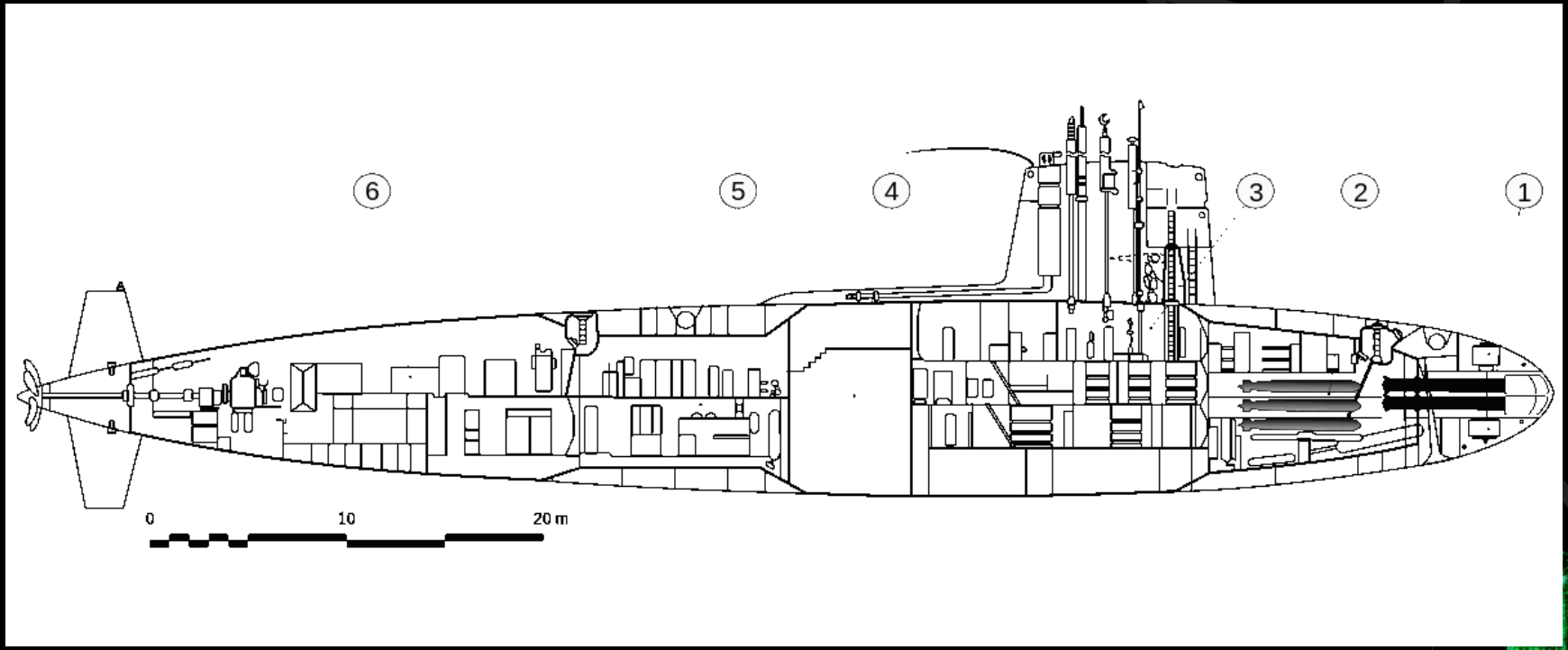
Can your vehicles be securely updated in a prompt and agile manner?

4) Security Updates

5) Segmentation and Isolation

Do you have a published attestation of the physical and logical isolation measures you have implemented to separate critical systems from non-critical systems?

5) Segmentation and Isolation



I Am The Cavalry

Assessment of BMW Door Lock Security Updates

There has been positive news in automotive cyber safety lately. BMW announced that they have fixed a flaw in over 2.2 million of their cars, silently and remotely. The flaw allowed someone other than the driver to remotely unlock the car, through the ConnectedDrive system. BMW pushed out an update over the mobile data network to the affected vehicles, and detailed further security measures they have taken to protect against accidents and adversaries.

The German Automobile Association (ADAC) investigated the cyber security of several BMW models and discovered six security flaws in the design and implementation of the ConnectedDrive software. They disclosed their research to BMW, who collaborated with ADAC researchers to understand and develop a fix for two of the most critical flaws. BMW remotely updated its customers' vehicles, adding HTTPS encryption and server authentication checks. BMW then announced the details of what they found, how they fixed it, and what other measures they have already taken to protect the safety of drivers, passengers, other vehicles, pedestrians, etc.

This is a big, positive step forward for cyber safety in automobiles. First, it shows that remote attacks against vehicles are still real threats, as demonstrated in 2010 and 2011 by security researchers. Second, this establishes the benefits of working with third-party technical experts, as

Microsoft (Then & Now)

www.iamthecavalry.org
@iamthecavalry

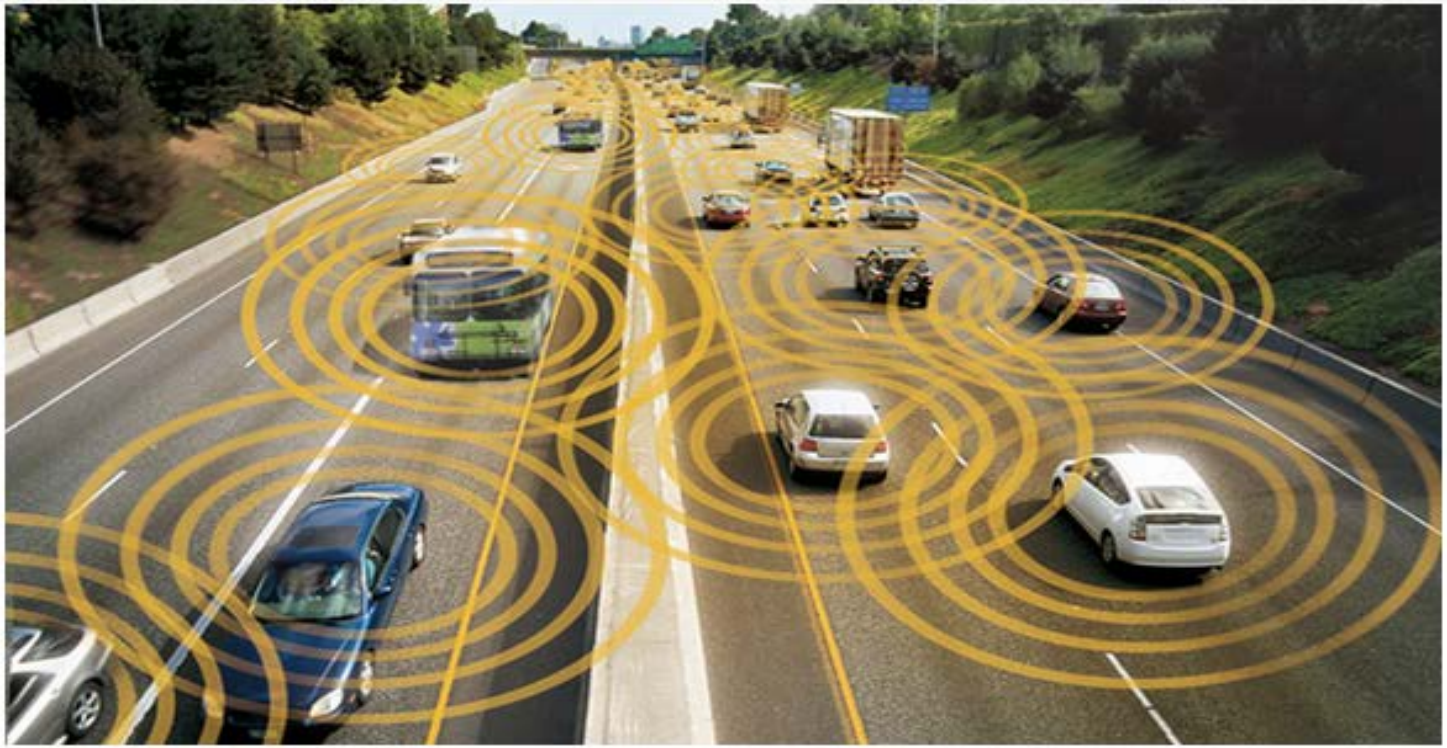
Past versus Future

Bolt-On Vs Built-In


CASE
Max 3
150 165 180 195 210 225
F:-13 182 R:-1
HDG: 195
TRN: 0.3
DOCUMENTING

WIRED

Here's a Terrible Idea: Robot Cars With Adjustable Ethics Settings



U.S. Department of Transportation

LAT
NEW

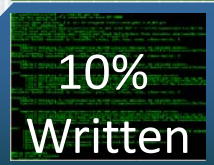
THANK YOU

@joshcorman
@iamthecavalry
@OpenGarages

www.iamthecavalry.org
@iamthecavalry

GOOD, BAD, & UGLY! LAWS & E.O.S

#RSAC
@joshcorman
@iamthecavalry

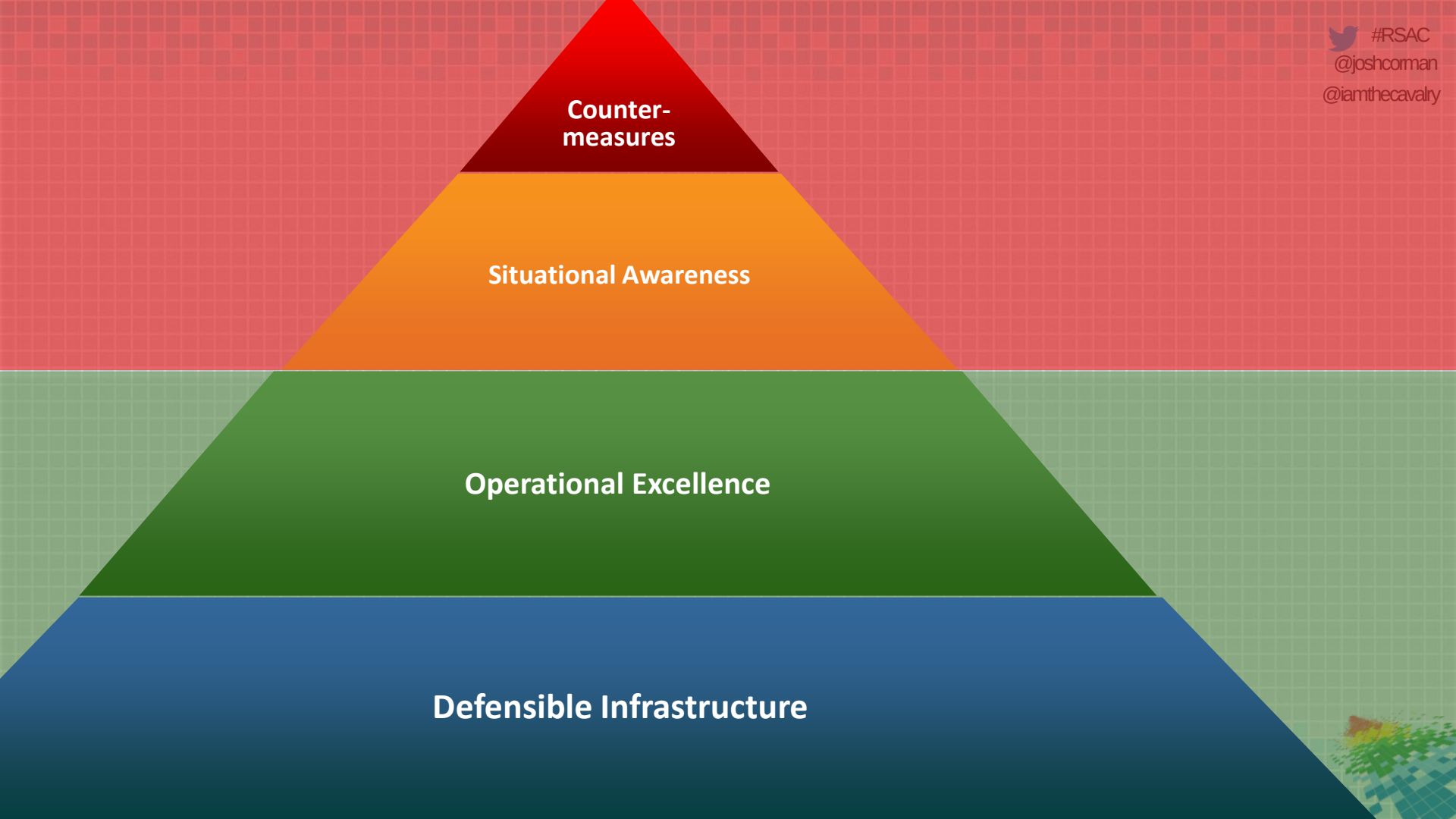


Counter-measures

Situational Awareness

Operational Excellence

Defensible Infrastructure


Counter-measures
Situational Awareness
Operational Excellence
Defensible Infrastructure

Apply! “We get the CyberGov We Deserve!”

- Choose:
  - Lead, Follow, or Get Out Of The Way
- Review Pending/Coming CyberLegislation
  - To act in your own self-interest, one must know it ☺
- “Table Top” w/Your Executive Stakeholders! (BC/DR)
- YOU Are The Cavalry!
  - Look into ways to help w/ Public Safety & Human Life
  - www.iamthecavalry.org

RSAConference2015

San Francisco | April 20-24 | Moscone Center

We Get The Government We Deserve…

#RSAC