RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

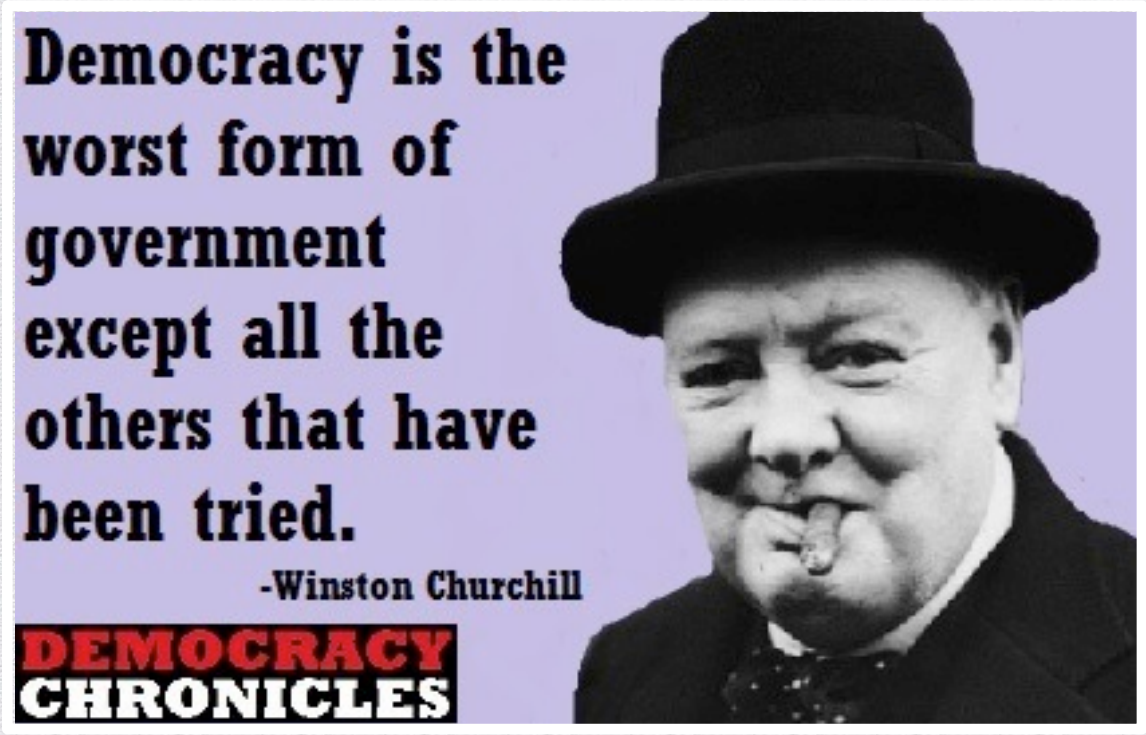
Software Liability?: The Worst Possible Idea (Except For All Others)

SESSION ID: ASEC-F01

Jake Kouns
Chief Information Security Officer
Risk Based Security
@jkouns

Joshua Corman
CTO
Sonatype
@joshcorman

Worst quality image (except all others)



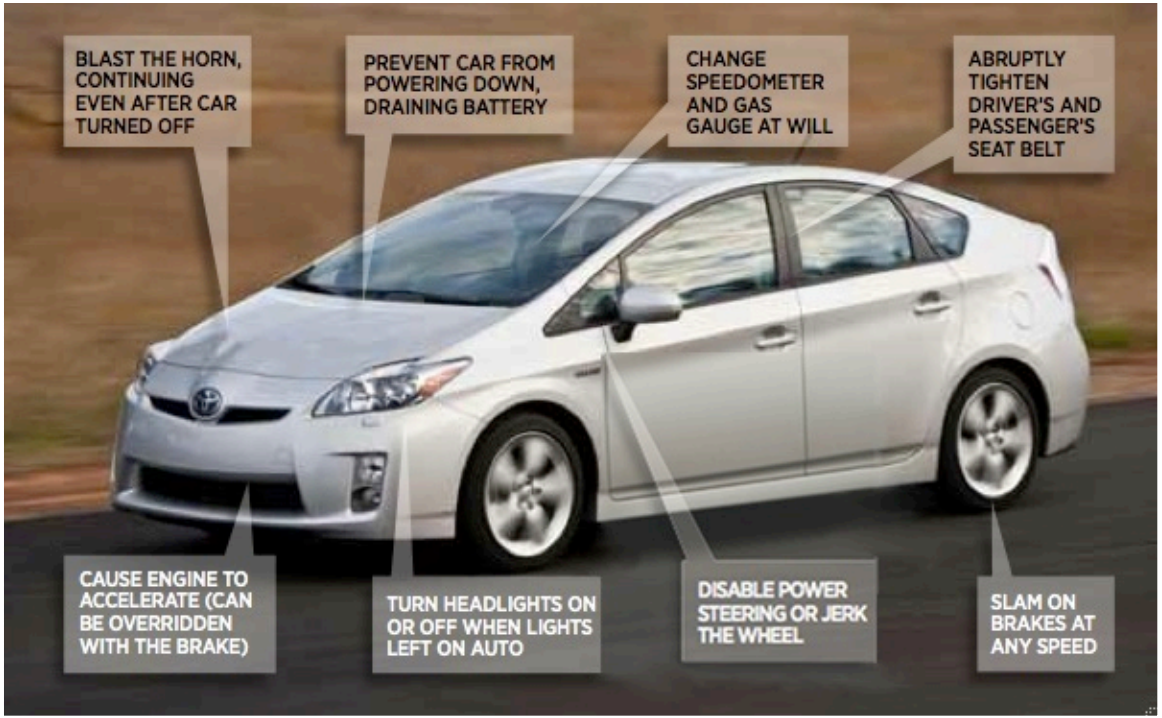
Agenda

- Why Liability? Why now?
- Product Liability 101
- Product Liability Implementation
- Why NOT to have Product Liability for Software Vendors
- Some Economics
- What is Changing the Equation

Triggers…

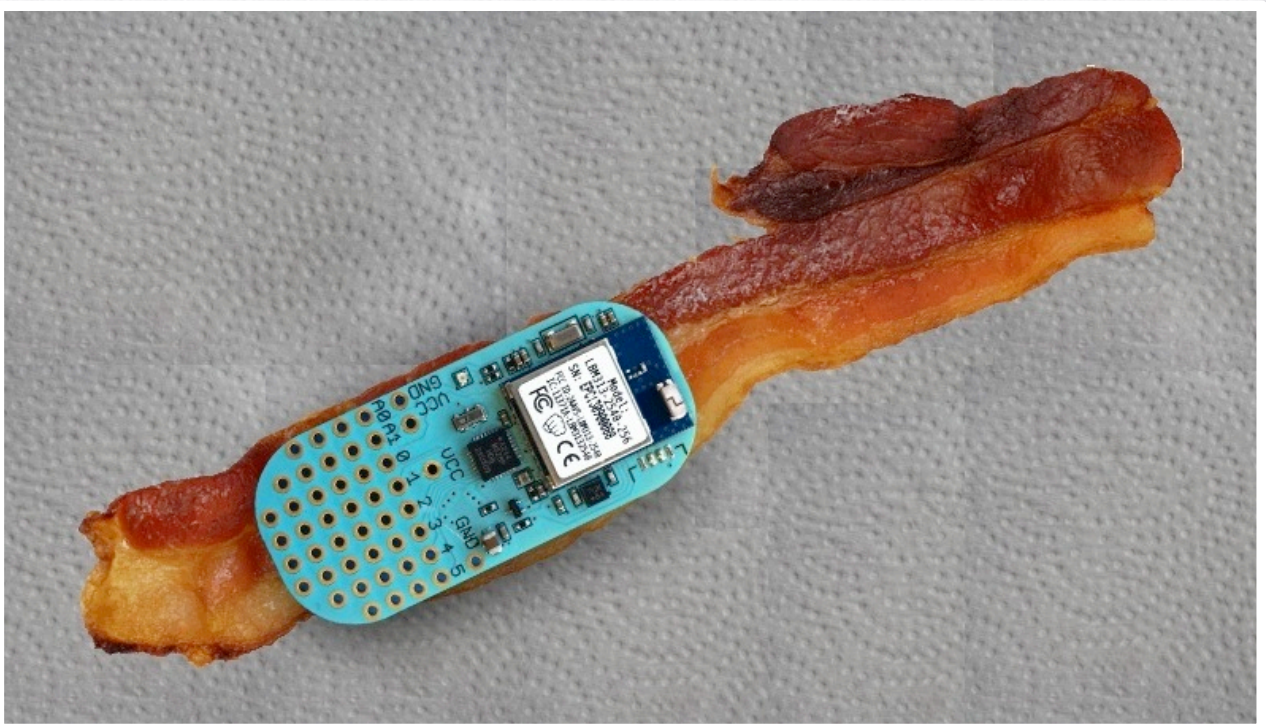

Energy Monitor
45 F
ENGINE
BATTERY
ELEC.MOTOR
Consumption
Current
0.0 MPG
DISPLAY
INFO
AUDIO
ODO TRIP
km/h MPH
PWR
VOL
SEEK·TRACK
AM
FM
DISC·AUX
SCAN
TUNE·FILE
TOYOTA
MP3 WMA
POWER
P
R
N
D
B

! $4f3 @ * $p33d



RiskBased SECURITY Sonatype

Our Bodies

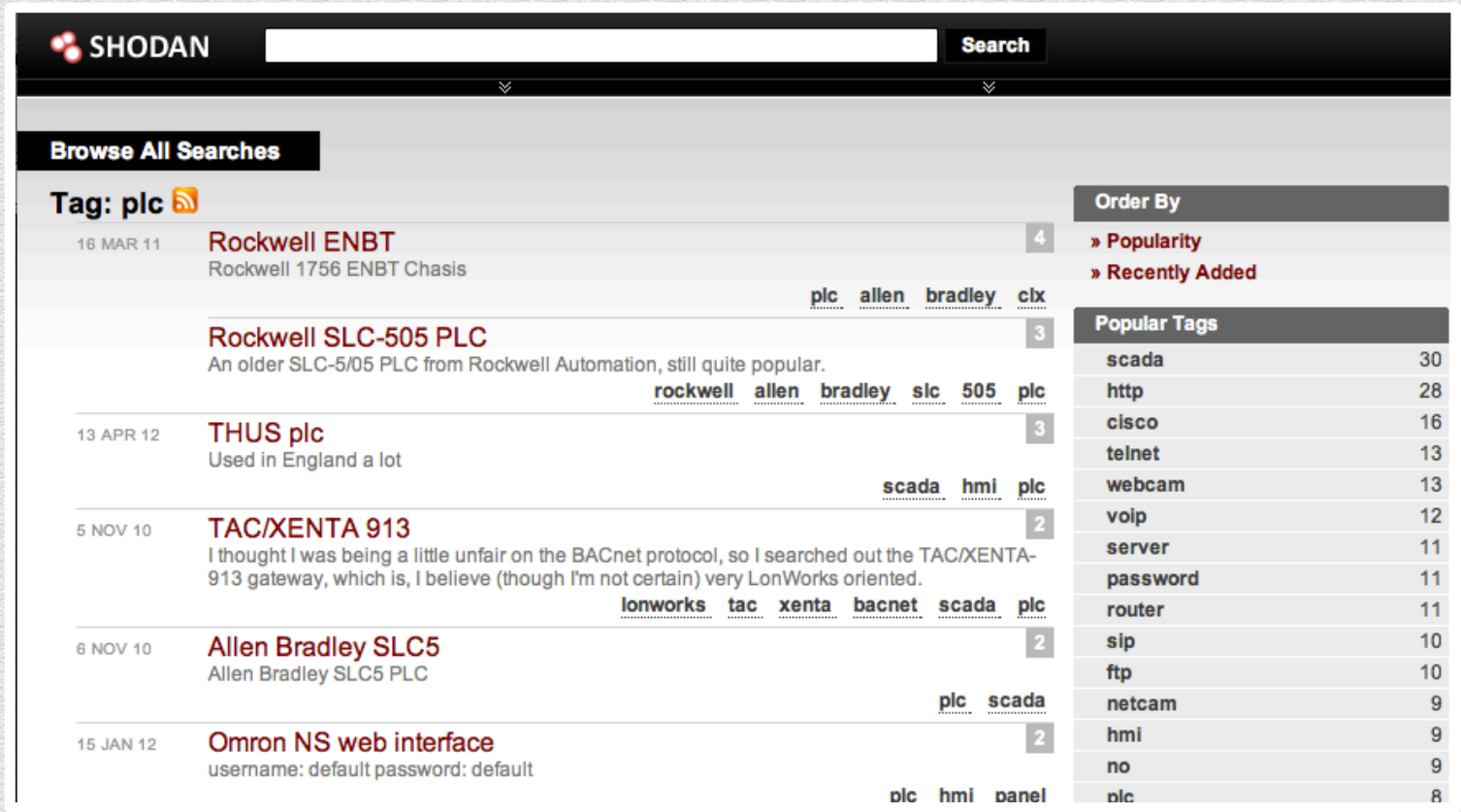

GND
VCC
P0
P1
P2
GND
VCC
0
1
2
3
4
5

In our homes

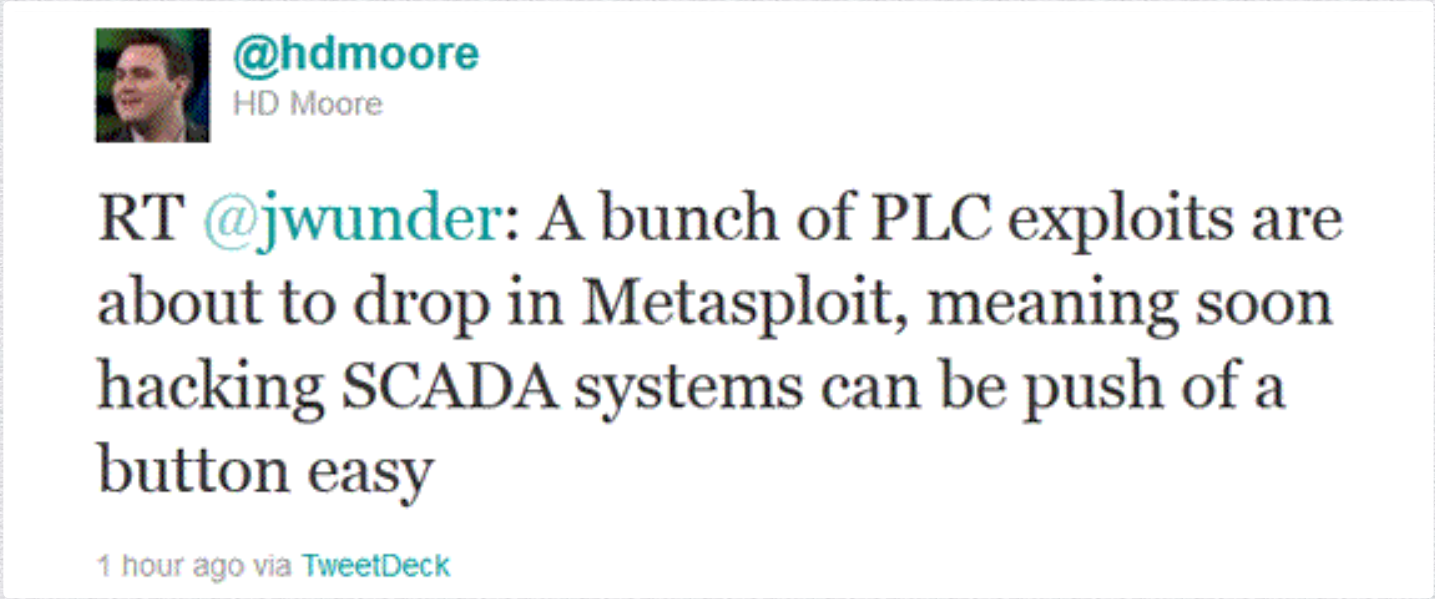
Miss Teen USA: Screamed upon learning she was 'sextortion' victim

By **Phil Gast, Mariano Castillo** and **Greg Botelho,** CNN

updated 9:39 AM EDT, Sat September 28, 2013


SHODAN
Search
Browse All Searches
Tag: plc
16 MAR 11
Rockwell ENBT
4
Rockwell 1756 ENBT Chasis
plc allen bradley clx
Rockwell SLC-505 PLC
3
An older SLC-5/05 PLC from Rockwell Automation, still quite popular.
rockwell allen bradley slc 505 plc
13 APR 12
THUS plc
3
Used in England a lot
scada hmi plc
5 NOV 10
TAC/XENTA 913
2
I thought I was being a little unfair on the BACnet protocol, so I searched out the TAC/XENTA-913 gateway, which is, I believe (though I'm not certain) very LonWorks oriented.
lonworks tac xenta bacnet scada plc
6 NOV 10
Allen Bradley SLC5
2
Allen Bradley SLC5 PLC
plc scada
15 JAN 12
Omron NS web interface
2
username: default password: default
plc hmi panel
Order By
» Popularity
» Recently Added
Popular Tags
scada 30
http 28
cisco 16
telnet 13
webcam 13
voip 12
server 11
password 11
router 11
sip 10
ftp 10
netcam 9
hmi 9
no 9
plc 8

Our Infrastructure



Product Liability

Defined

- Wikipedia definition:
  - Product liability is the area of law in which manufacturers, distributors, suppliers, retailers, and others who make products available to the public are held responsible for the injuries those products cause.
  - Although the word "product" has broad connotations, product liability as an area of law is **traditionally limited to products in the form of tangible personal property.**

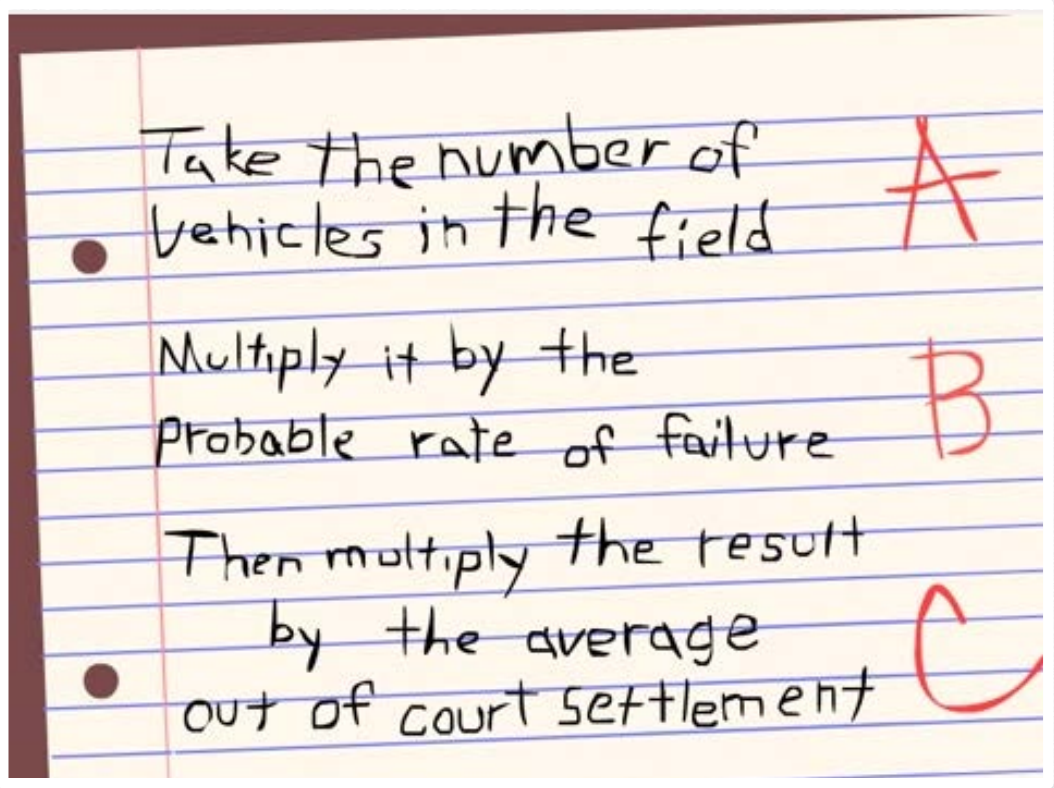
Manufacturing Defects

Design Defects

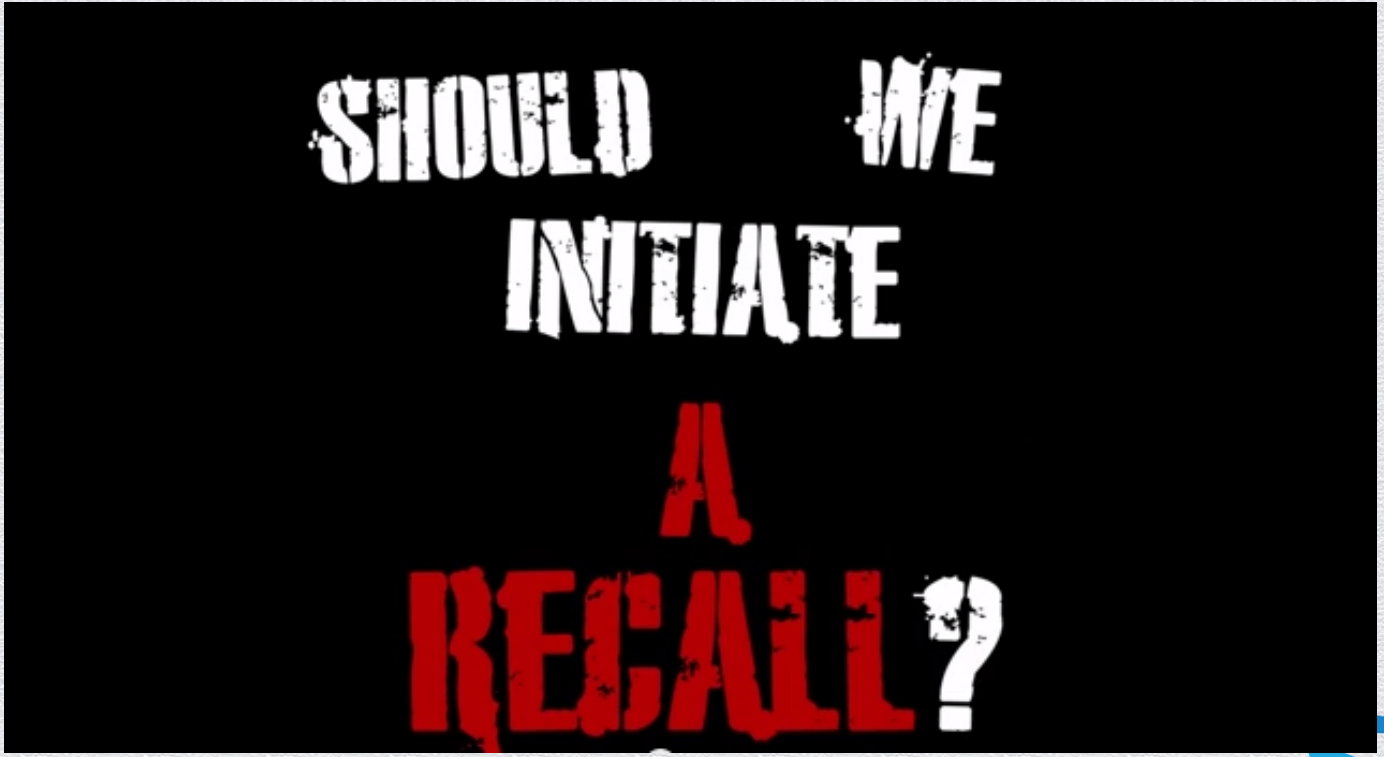
Failure To Warn

Failure To Warn

Failure To Warn



Failure To Warn



Breach of Warranty

Warranty Certificate

DIAMOND STANDARD PARTS ARE GUARANTEED AS A REPLACEMENT PART FOR FIT, FINISH AND FUNCTION. DS PARTS ARE TESTED FOR SAFETY AND MEET ALL FEDERAL AND STATE LAWS WHERE APPLICABLE. DS ABSORBERS MEET FMVSS 302 FOR FLAMMABILITY. DS STEPBUMPERS MEET VESC V-5 RATINGS FOR TOWABILITY. DS FRONT BUMPERS, BRACKETS AND REINFORCEMENT BARS ARE PRODUCED USING HSS OR ULHSS STRENGTH STEELS. OUR STEEL REPLACEMENT HOODS ARE STRIKER AND LOAD CARRYING PERFORMANCE TESTED.

DS PLATED PARTS CARRY A LIFETIME WARRANTY TO THE ORIGINAL OWNER. ROAD HAZARD, IMPROPER INSTALLATION, DAMAGE OR ACTS OF GOD ARE EXCLUDED.

DS PARTS ARE TESTED BY MGA RESEARCH, BURLINGTON, WISCONSIN AND REVIEWED BY FORMER NHTSA DIRECTORS PRIOR TO BEING OFFERED FOR SALE.

DS PARTS ARE ONLY SOLD THROUGH QUALIFIED ISO9001 DISTRIBUTORS.

TEN YEAR ... ED WARRANTY

limited warranty certificate covering your use of the ...d by Country Lane Woodworking, New Holland, PA. ...-transferable and applies only to the original purchaser ...inal location, unless the product was relocated by a ... working approved installer. Relocating the covered ... party automatically invalidates this warranty.

...riately and maintained properly, Country Lane ...ntees that this product will remain structurally ... and tear, fading of exterior surfaces, and general ...ging, which is common of any outdoor product that ... exposed to natural elements, is not covered under ...arranty. As with any building which is located on ...p of the ground, settling may occur. You also will ...ed to periodically clean, paint, caulk and keep ...getation from growing around the edges of the ...zebo which will cut off ventilation.

...ginal invoice must be attached to this guarantee.

...king Installer Date Invoice #

...untry Lane ...OODWORKING CUSTOM GAZEBOS

LIMITED WARRANTY

BULLET EXPRESS TRIO ONE-YEAR LIMITED WARRANTY

At Bullet Express, LLC, we take pride in our products. We go out of our way to make products of superior quality and craftsmanship, products designed to meet or exceed the demands placed on them through everyday use. Because of this commitment to quality, we warrant the BULLET EXPRESS TRIO to be free of defects for one full year. Here's the deal: If your BULLET EXPRESS TRIO stops operating to your satisfaction due to defects in materials or workmanship, we'll gladly repair it or replace it for free (excluding shipping and handling charges). For warranty service, simply call our customer service department @ 1-877-9-BUL-EXP (1-877-928-5397) or contact us via e-mail from our web site at **http://www.BulletExpress.com**, simply click the Customer Service link, fill out and submit the Customer Service contact form and we will be glad to help you. At Bullet Express, LLC, your complete satisfaction is our daily goal (hey, we know what it's like to be the customer!).

Bullet Express, LLC. warrants that the BULLET EXPRESS TRIO is free of defects in materials and workmanship for one year from the date of purchase. This warranty is valid only in accordance with the conditions set forth below:

1. Normal wear and tear are not covered by this warranty. This warranty applies to consumer use only, and is void when the product is used in a commercial or institutional setting.
2. This warranty extends only to the original consumer purchaser and is not transferable. In addition, proof of purchase must be demonstrated. This warranty is void if the product has been subject to accident, misuse, abuse, improper maintenance or repair, or unauthorized modification.
3. This limited warranty is the only written or express warranty given by Bullet Express, LLC. Any implied warranties on the product (including but not limited to any implied warranties of merchantability or fitness for a particular purpose) are limited in duration to the duration of this warranty. Some states do not allow limitations on how long an implied warranty lasts, so the above limitation may not apply to you.
4. Repair or replacement of the product (or, if repair or replacement is not feasible, a refund of the purchase price) is the exclusive remedy of the consumer under this warranty. Bullet Express, LLC. shall not be liable for any incidental or consequential damages for breach of this warranty or any implied warranty on this product. Some states do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you.
5. This warranty gives you specific legal rights, and you may also have other rights which vary from state to state.

Consumer Protection

RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Product Liability Implementation

Who knows the name of this car?

Ford Pinto

Ford Pinto (1971 – 1980)

- Allegations
- 27 deaths
- According

uel tank filler neck to bre
ear-end collision, re
e, Ford allegedly w
r a redesign, and decide
uits.

Intended Value and Impact

- Companies put a larger emphasis on prevention of issues
- Companies put a larger emphasis on testing / precautions
- Companies put a culture in place and don't take unnecessary risks due to financial impact
- Better risk management for the entire company
- If a company becomes aware of an issue, they act quickly to correct

Any issues with hot coffee?

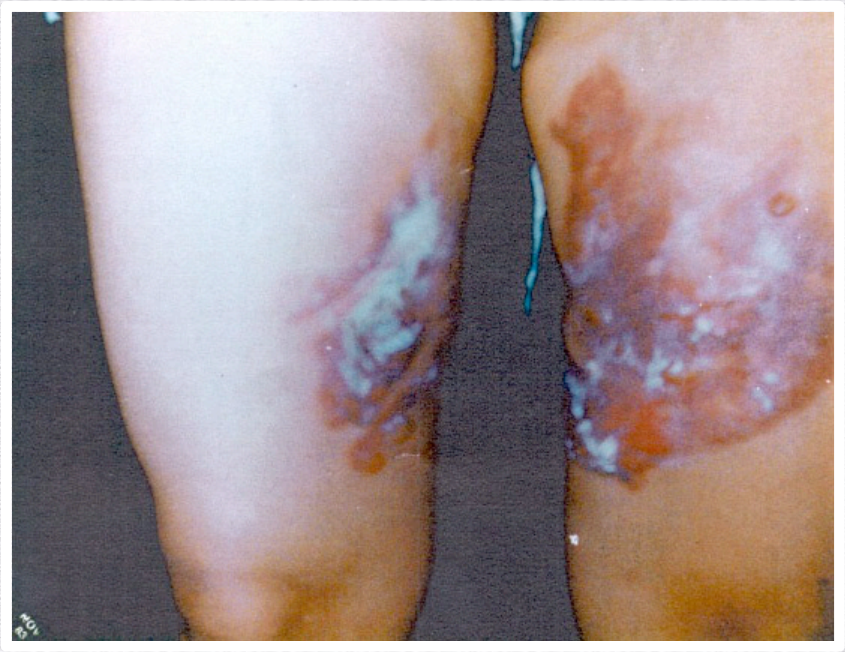
Very well known case!

Liebeck v. McDonald’s Restaurants (1994)

- Known as the McDonald's coffee case and the hot coffee lawsuit
- A New Mexico civil jury awarded $2.86 million to plaintiff Stella Liebeck who had suffered third-degree burns in her pelvic region when she accidentally spilled hot coffee in her lap after purchasing it from a McDonald's restaurant.
- Liebeck was hospitalized for eight days while she underwent skin grafting, followed by two years of medical treatment.

When Product Liability Goes Wrong?

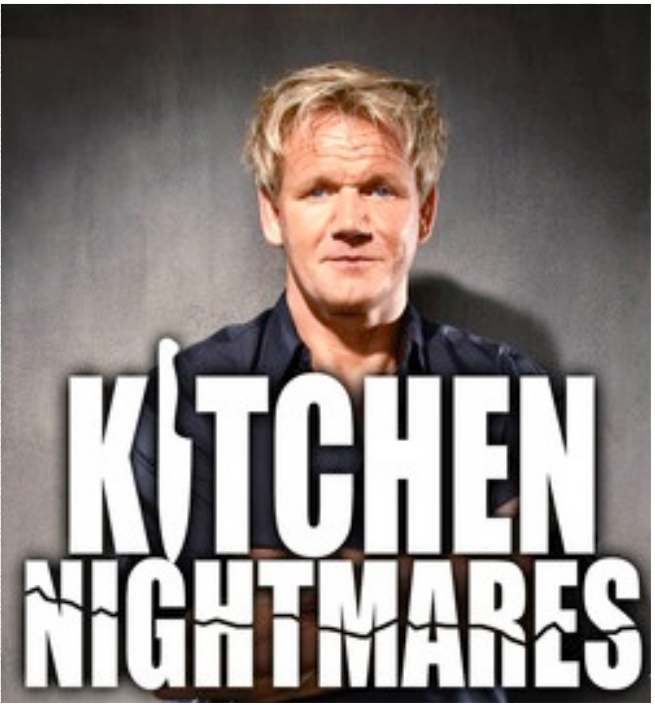
- McDonald’s hot coffee is thought to be when legal system goes wrong!
- Most actually don’t know the correct full story!
- This is really a case of “Failure To Warn”
  - Documents obtained from McDonald's showed that from 1982 to 1992 the company had received more than 700 reports of people burned by McDonald's coffee
  - Varying degrees of severity, and had settled claims arising from scalding injuries for more than $500,000.
- Questions were asked why was it so hot?

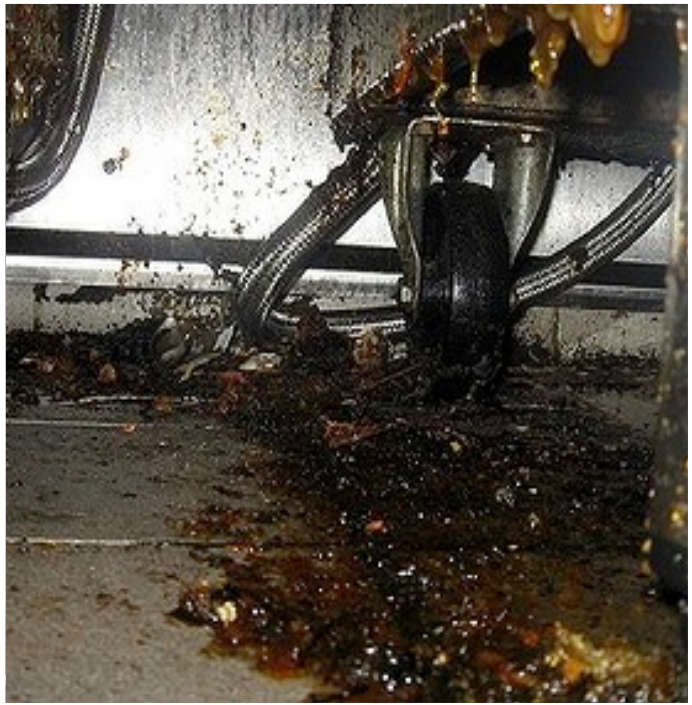


Does this provide value to end consumers / users of the product?

McDonald's Coffee

Restaurant Health Codes





Deceptive Products

FTC takes action against deceptive weight-loss products

Alison Young, USA TODAY 6:13 p.m. EST January 7, 2014

(Photo: Federal Trade Commission)

SHARE f 2938 CONNECT 210 TWEET 36 COMMENT EMAIL MORE

As dieters work on new year's resolutions to shed pounds, the Federal Trade Commission on Tuesday announced enforcement actions against four companies the agency says have used deceptive advertising claims to sell weight-loss products.

The products lured consumers with promises of making weight-loss easy. But "the chances of being successful just by sprinkling something on your food, rubbing cream on your thighs, or using a supplement are slim to none," said Jessica Rich, director of the FTC's consumer protection bureau. "The science just isn't there."

The FTC announced the following enforcement actions:

• The marketers of Sensa, a weight-loss powder sprinkled on food, will pay $26.5 million to settle

STORY HIGHLIGHTS

- Enforcement actions taken against four companies
- Companies sold food sprinkles, body creams, supplements and hormone drops
- Federal regulators warn of bogus weight-loss claims that make big promises

Product Recalls

- Consumer Products
  - appliances, clothing, electronic / electrical. furniture, household, children's products, lighting / lighter, outdoor, sports / exercise
- Motor Vehicles and Tires
- Child Safety Seats
- Food and Medicine
- Cosmetics and Environmental Products

Software Product Recalls?

When the product is marketed to be secure and it isn't how do software vendors handle it?

No more security patches of fixes for the product?

RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Product Liability for Software Vendors

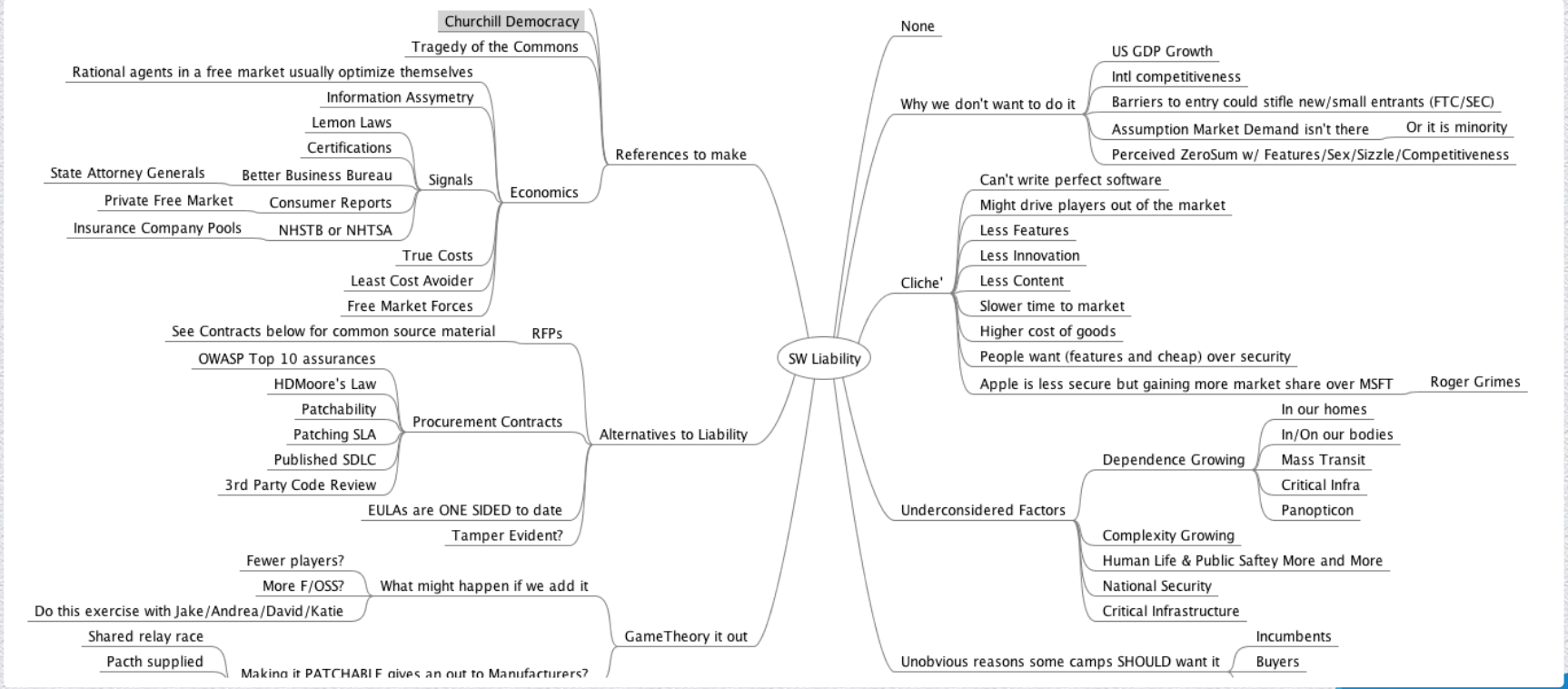
Sonatype

Software Liability

- Software
  - Debate
- At this po
  - With mo

012

Software Liability: Worst Idea



Reason #1 - The Worst Possible Idea

- Stifle Innovation
  - New features and ideas would be slow to market due to financials exposures
  - Fewer features
  - Slower time to market
  - Could hurt competitiveness and/or client satisfaction

Reason #2 - The Worst Possible Idea

- Barriers to Entry?
  - Could Hurt Small Businesses and Startups
  - Large enterprises would easily adjust to additional overhead, but cripple new and small businesses

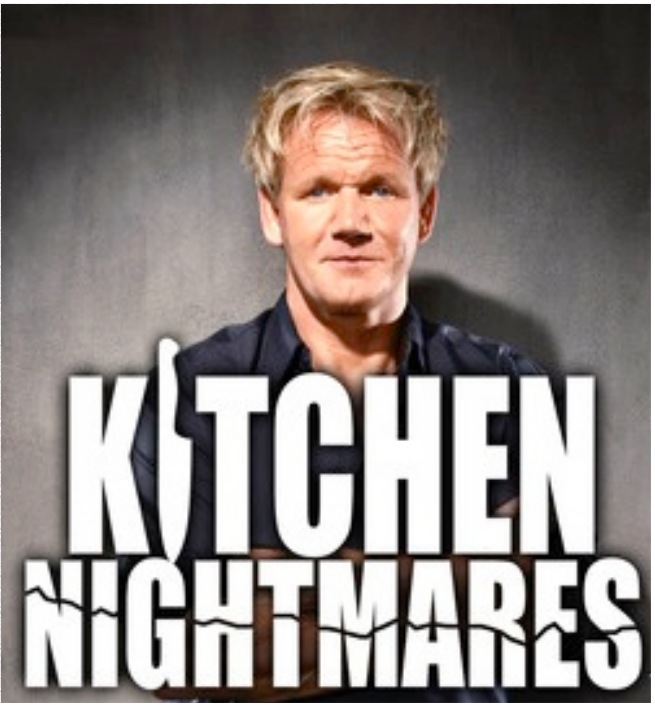
Reason #3 - The Worst Possible Idea

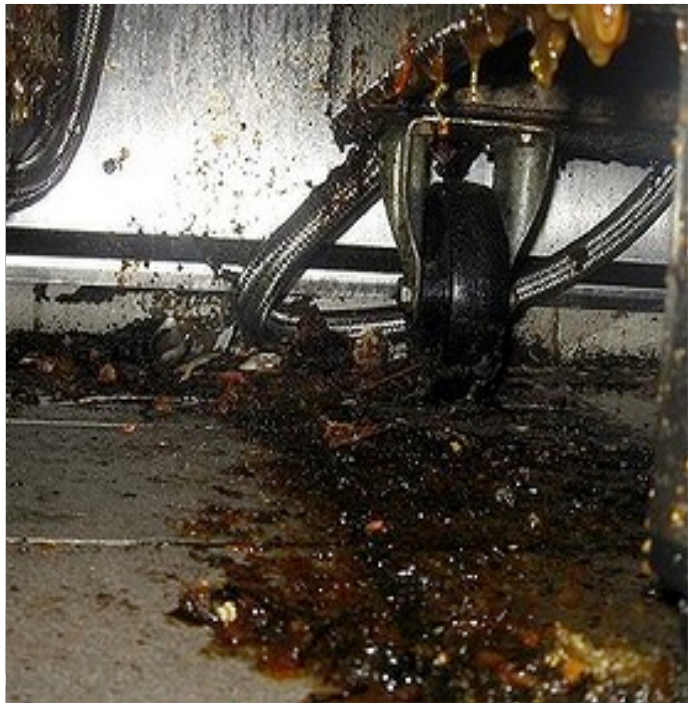
- Economic Impacts
  - What does this mean to the economy? Potential for massive amount of money to change hands. The uncertainty alone makes it an awful idea.
  - “IT” and Software we/are HUGE parts of the US GDP (and growing faster)

Reason #4 - The Worst Possible Idea

- Vendor Impact
  - Companies unable to handle the cost
  - Raise prices
    - But this is specious for a few reasons:
      - True Costs and Least Cost Avoiders are more efficient for the system
      - Hidden Costs and Cost of Ownership changes must be factored

Restaurant Health Codes





Counters to: The Worst Possible Idea

	Food Safety	Cars
1) Stifle Innovation	Chef's can't innovate?	Safety Differentiation
2) Barriers to Entry	Good!	Outstanding!
3) Economic Impact	Doubtful	Premium Pricing
4) Raise Prices/Exit Markets	To avoid illness/disease?	Free Market Demand

RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

What's Working To Influence Better Security Practices?

RiskBased SECURITY

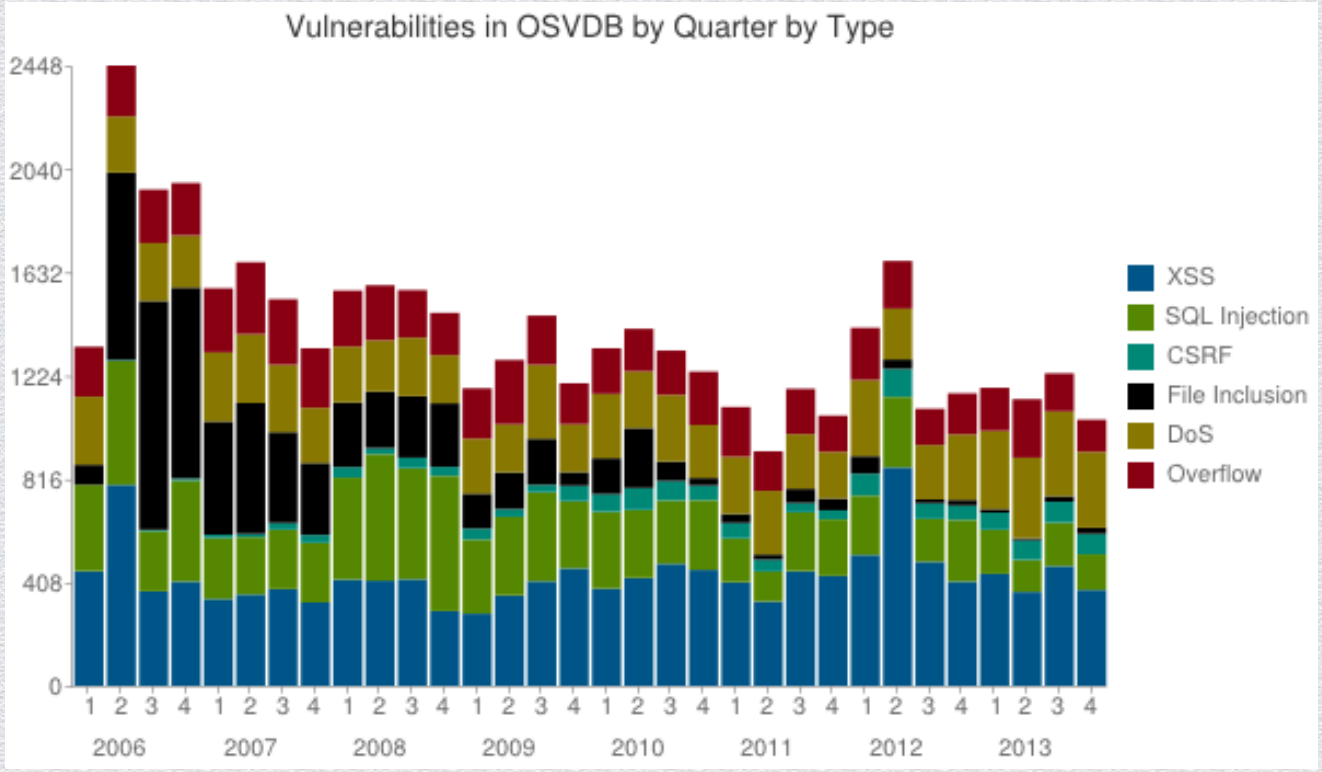
Sonatype

What Are We Doing To Improve Security?

- PCI/DSS*
- SOX*
- Market Forces*
  - Companies only pick secure software (if they care)
- HHS/HITECH (regulatory fines)*
- SEC*
- FTC*

*Debatable

Software Vulnerabilities Over time



2013: 10,580

2012: 10,070

2011: 7,807

2010: 9,098

2009: 8,124

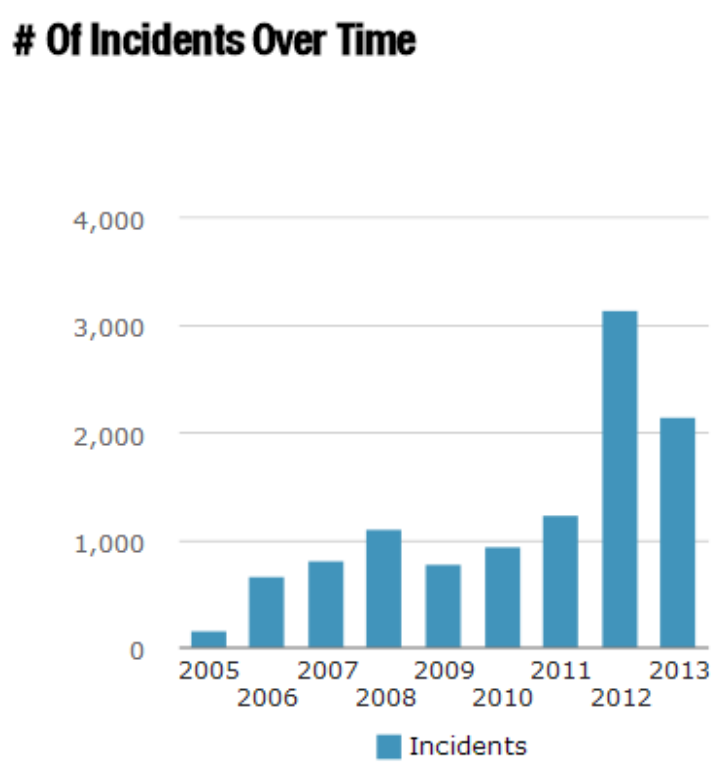
2008: 9,719

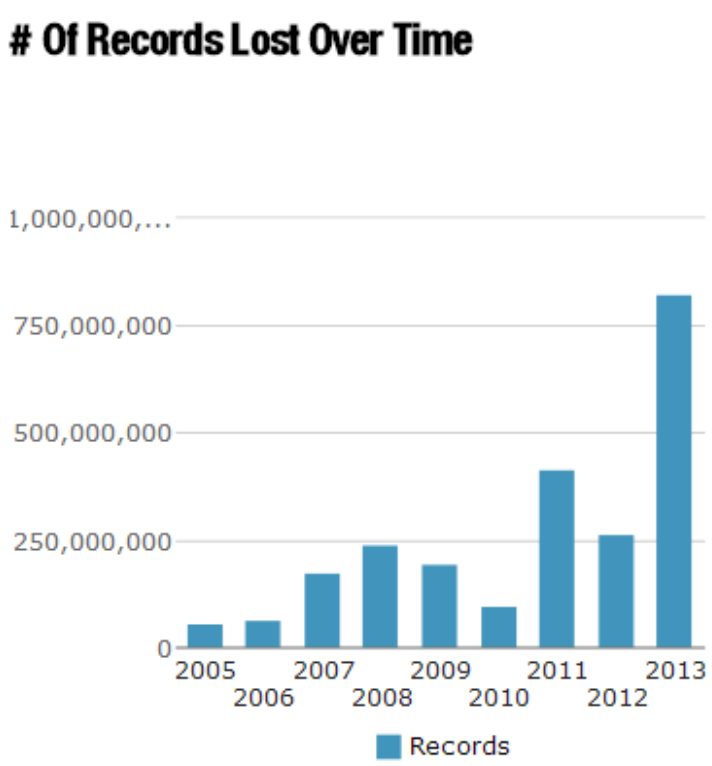
2007: 9,553

2006: 11,040

2005: 7,864

Data Breaches Over Time





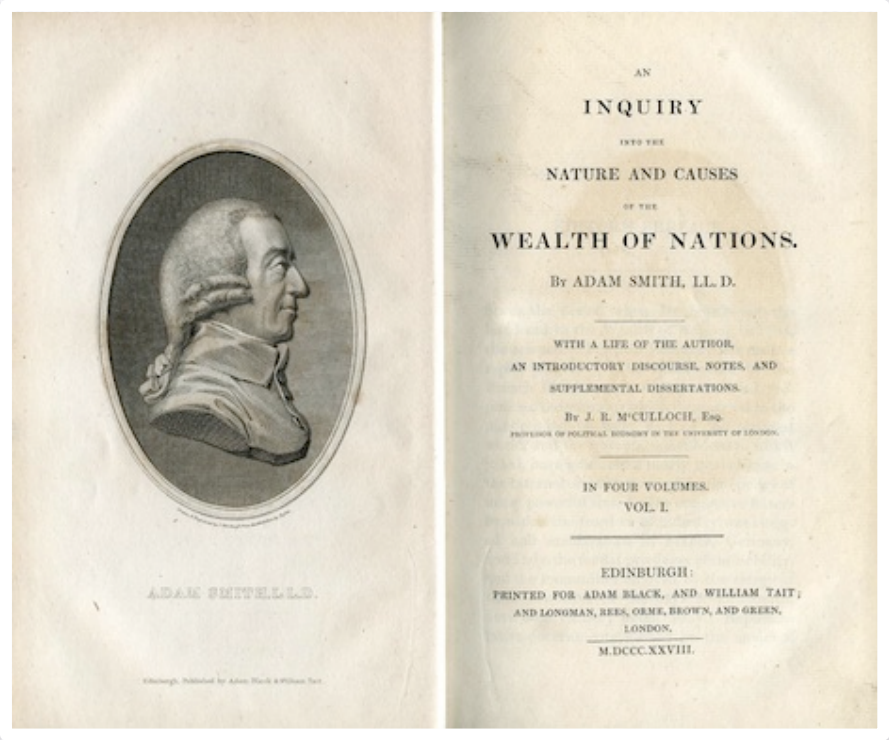
Source: Risk Based Security - https://cyberriskanalytics.com

Why Aren’t We Improving?

- Complexity
- Costs
- No real impact to end consumer?
- No real property or injury type issues?
- People just don’t really care?

Some Economics

On Free Market Forces…



AN

INQUIRY

INTO THE

NATURE AND CAUSES

OF THE

WEALTH OF NATIONS.

By ADAM SMITH, LL. D.

WITH A LIFE OF THE AUTHOR,
AN INTRODUCTORY DISCOURSE, NOTES, AND
SUPPLEMENTAL DISSERTATIONS.

By J. R. M'CULLOCH, Esq.

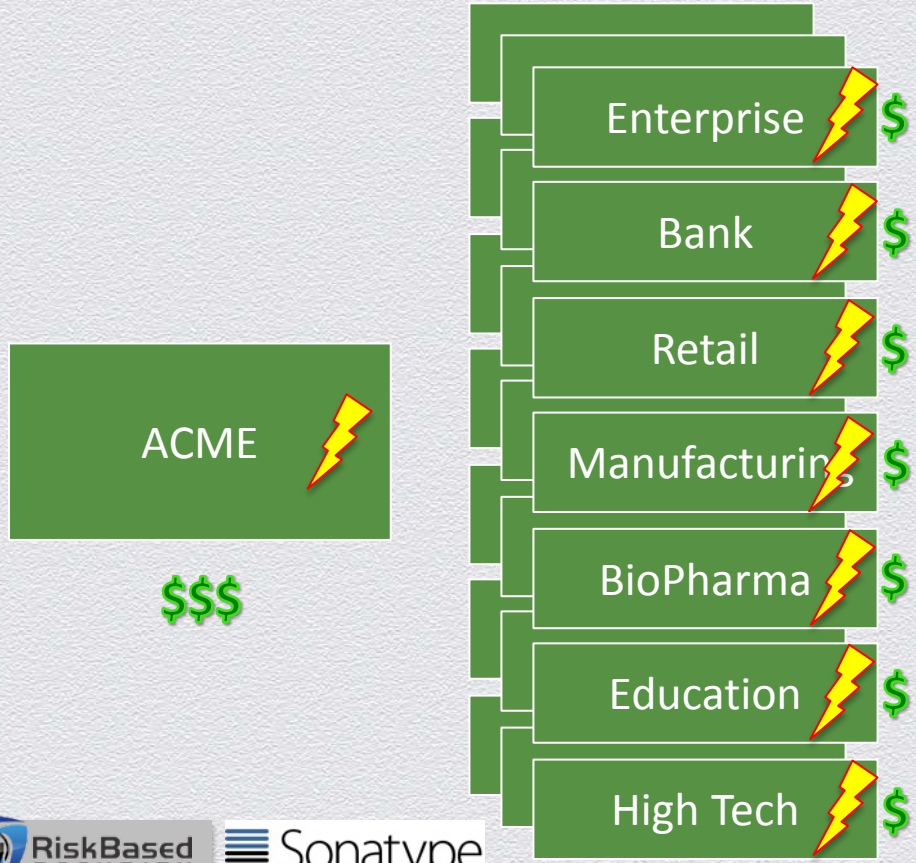
IN FOUR VOLUMES.
VOL. I.

EDINBURGH:
PRINTED FOR ADAM BLACK, AND WILLIAM TAIT;
AND LONGMAN, REES, ORME, BROWN, AND GREEN,
LONDON.

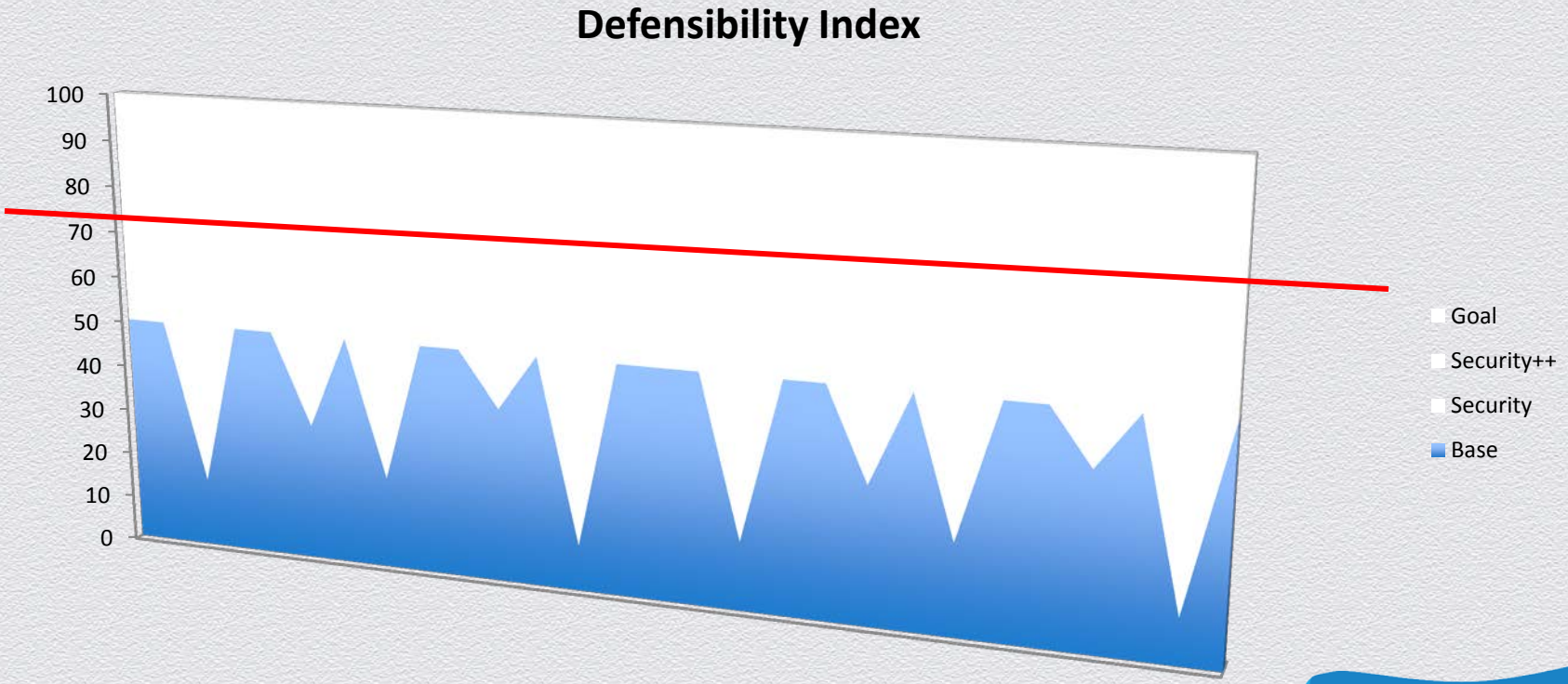
M.DCCC.XXVIII.

Information Asymmetry and Signaling

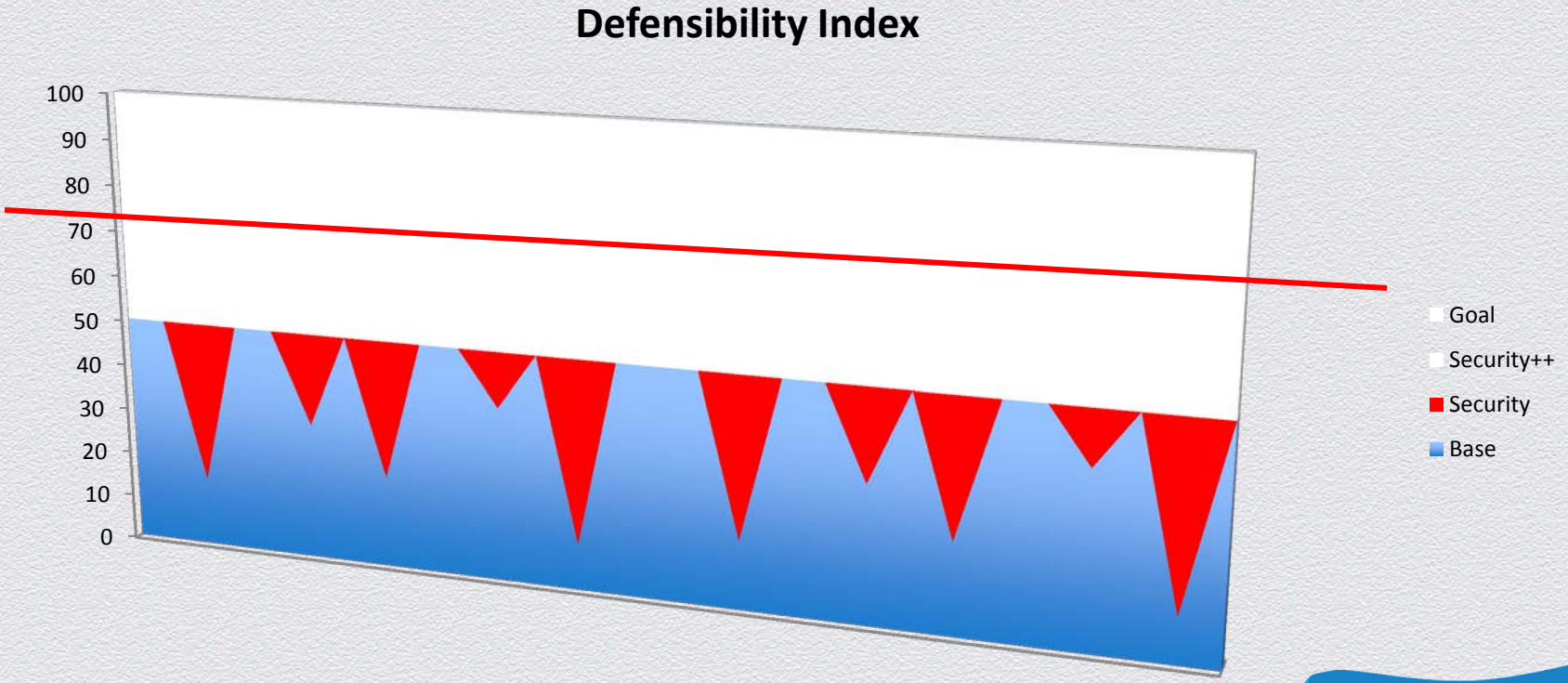
True Costs & Least Cost Avoiders



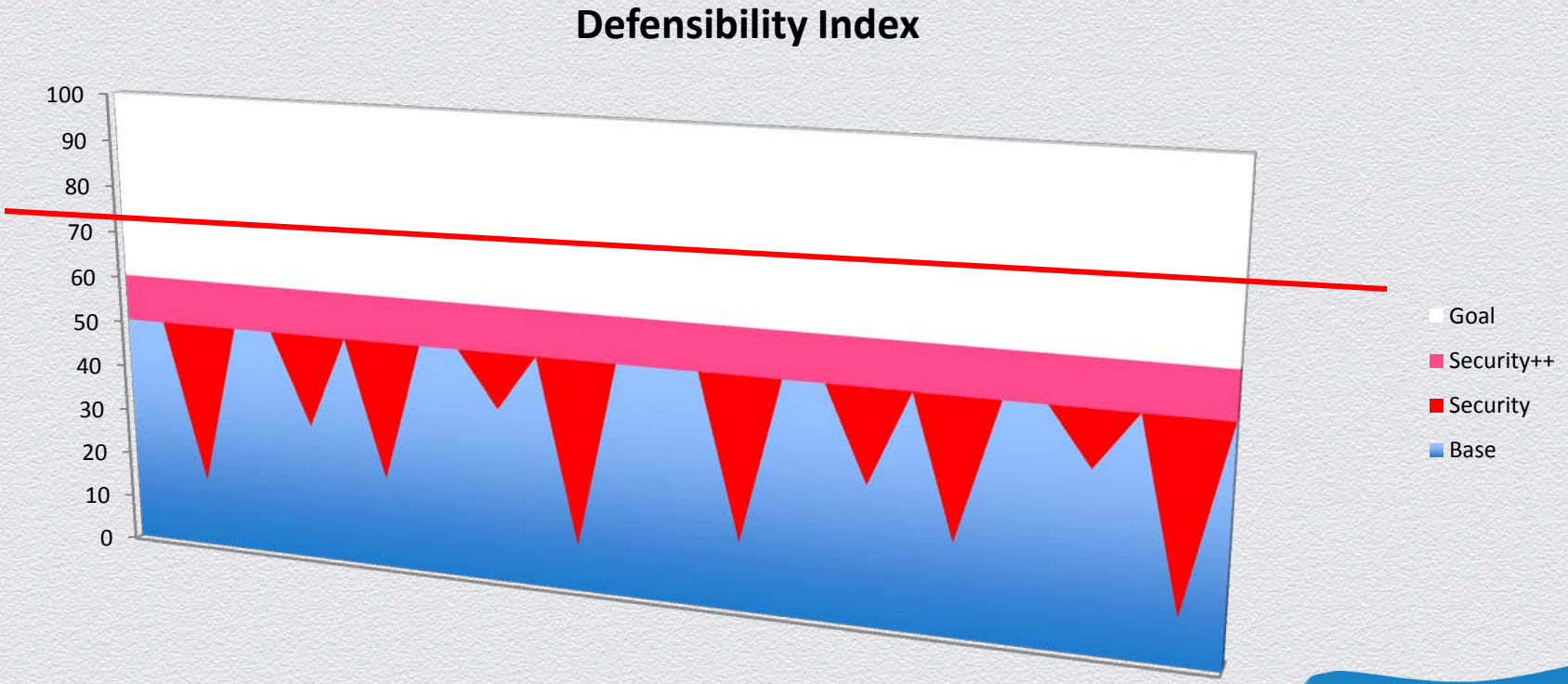
Passing the Buck (and Cost)



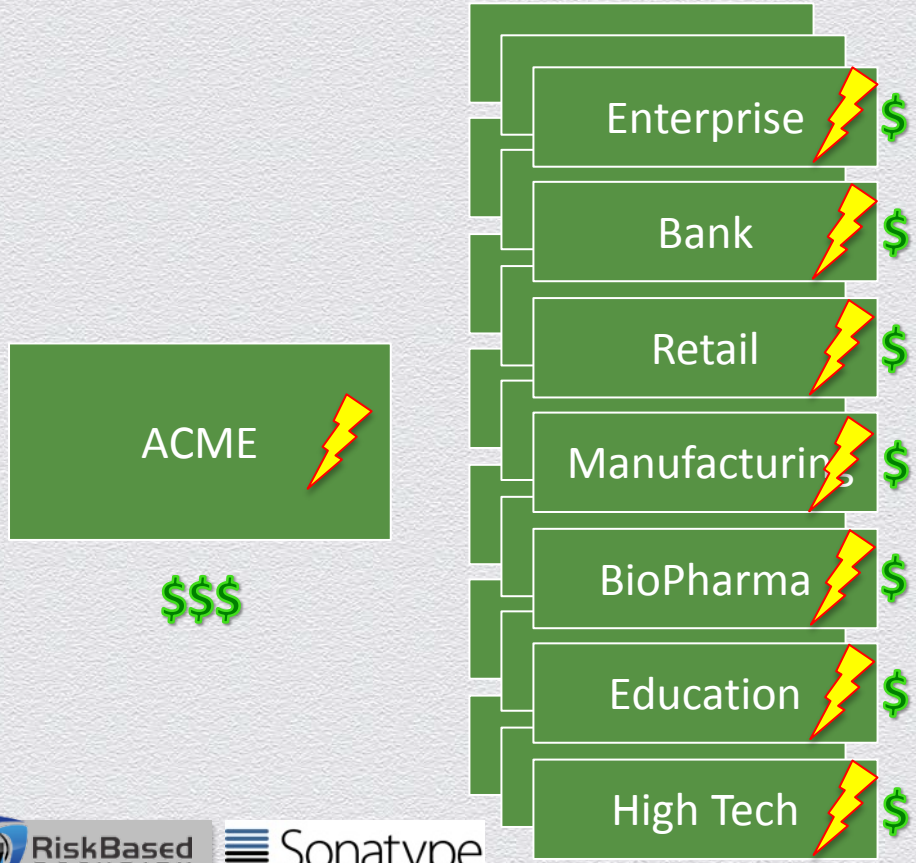
Passing the Buck (and Cost)



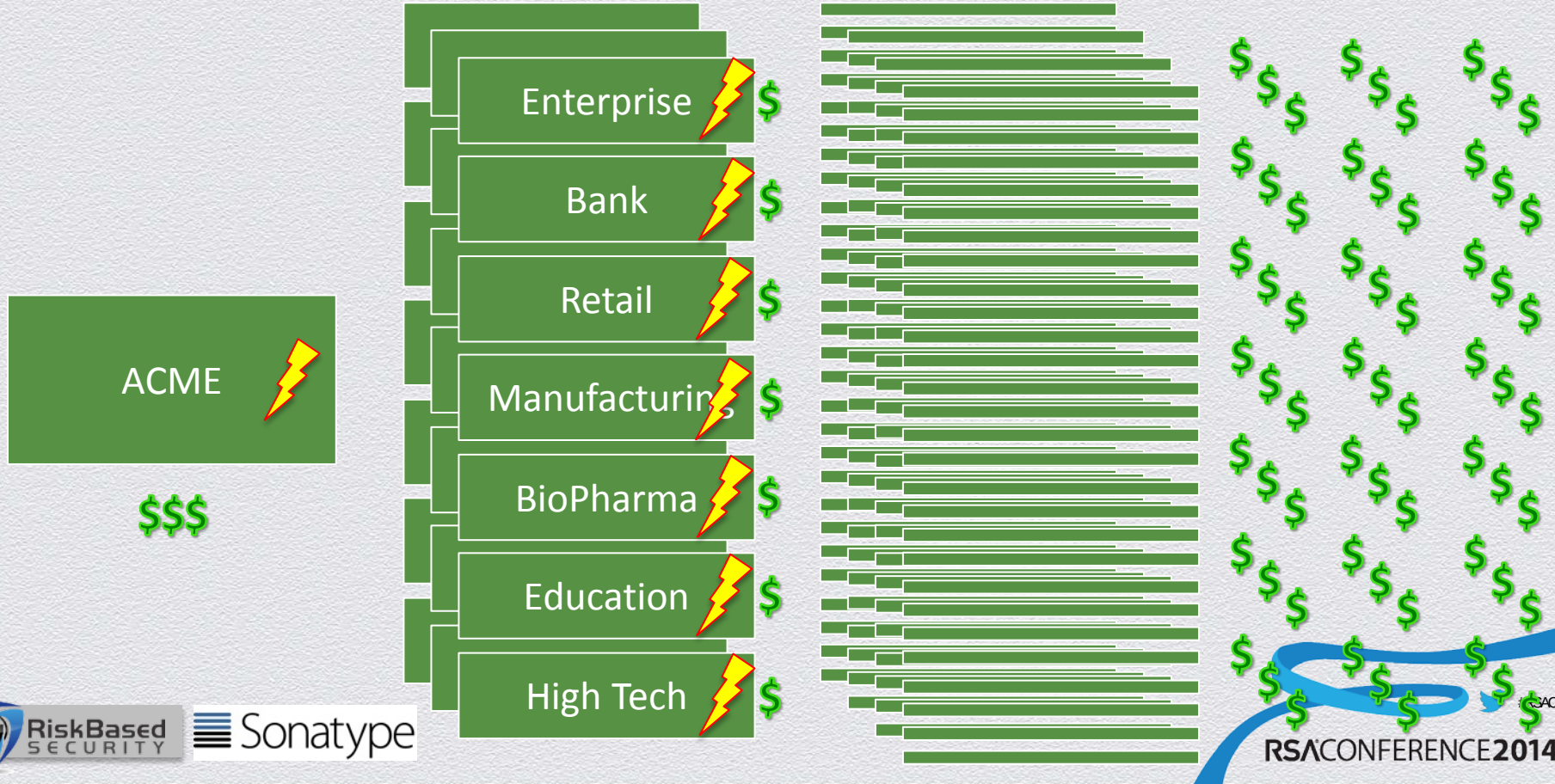
Passing the Buck (and Cost)



True Costs & Least Cost Avoiders



True Costs & Least Cost Avoiders: Downstream



RiskBased SECURITY

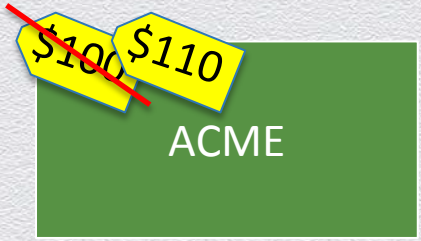
Sonatype

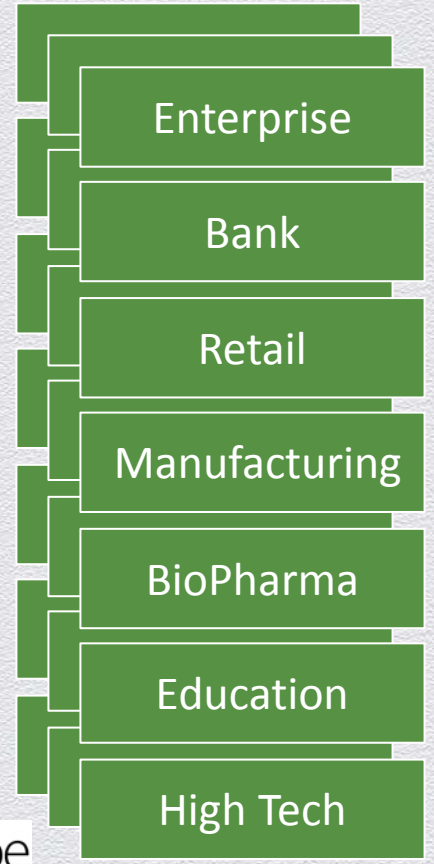
RSACONFERENCE2014

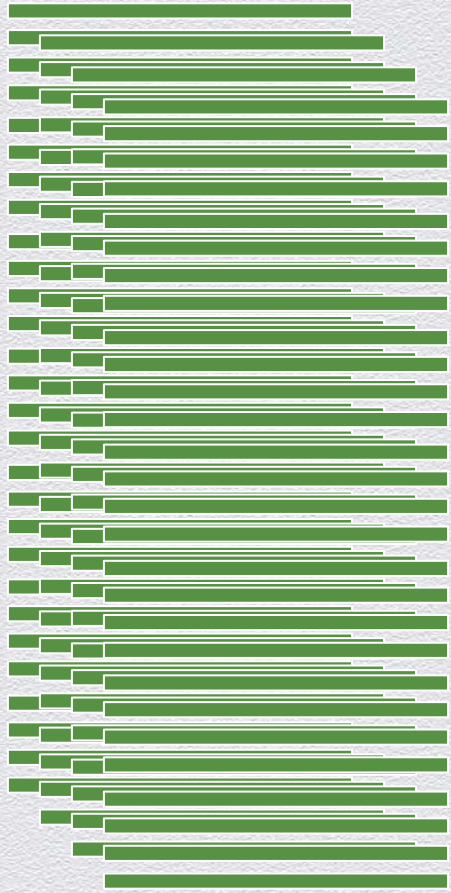
The Fallacy of Broken Windows

The Broken Window Fallacy

True Costs & Least Cost Avoiders







RiskBased SECURITY

Sonatype

#RSAC

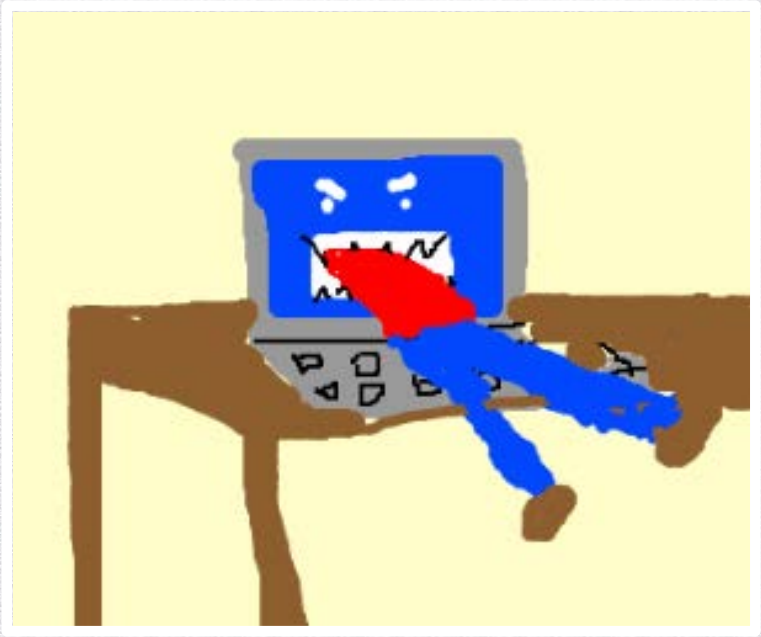
RSACONFERENCE2014

Where Do We Go From Here?

RiskBased SECURITY Sonatype

The World Is Changing

Reliance On Poor Software



Poor software with security issues in the new Internet of Things world can now lead to:

- Bodily Injury
- Property Damage
- Financial Harm

Product Liability Is Already Here

- Its not the software that hurts the people, it's a component of a larger finished product, making it a product failure not just the software.
- ***MacPherson v. Buick Motor Co.***, 217 N.Y. 382, 111 N.E. 1050 (1916)
  - Donald C. MacPherson was injured when one of the wooden wheels of his 1909 "Buick Runabout" collapsed
  - Buick Motor Company, had manufactured the vehicle, but not the wheel, which had been manufactured by another party but installed by defendant.
- Software responsibility is going to be on final good manufacturer (no matter what) that is delivering the final product

Product Liability Is Already Here

- The important portion of the *MacPherson* opinion:
  - "If the nature of a thing is such that it is **reasonably certain to place life and limb in peril when negligently made**, it is then a thing of danger. Its nature gives warning of the consequence to be expected. If to the element of danger there is added knowledge that the thing will be used by persons other than the purchaser, and used without new tests, then**, irrespective of contract, the manufacturer of this thing of danger is under a duty to make it carefully.** That is as far as we need to go for the decision of this case . . . . If he is negligent, where danger is to be foreseen, a liability will follow"

Software Part Of The Final Product

Open Automotive Alliance aims to bring Android inside the car

Can Google make your car safer and friendlier to use?

by **Jason Inofuentes** - Jan 6 2014, 9:33am EST

ANDROID MOBILE COMPUTING 49

Kārlis Dambrāns

Google, Audi, GM, Honda, Hyundai, and Nvidia have formed the Open Automotive Alliance (OAA) in the hopes of improving our automotive experience through

ARS AT CES 2014

The flat-out truth on curved TVs

Never miss an update *Follow AppleInsider* Like 13k Follow 152K followers RSS

Friday, July 26, 2013, 05:09 am PT (08:09 am ET)

Why Apple is revving iOS in the Car for an aggressive 2014 launch

By Daniel Eran Dilger

Apple's chief executive Tim Cook described the company's 2014 launch of iOS in the Car as "very, very important" and a "key focus for us." Here's a look at what the industry thinks, the competition Apple faces in automotive, and why it's pushing so hard for an immediate launch next year.

RiskBased SECURITY Sonatype

#RSAC

RSACONFERENCE2014

Financial Liability For Data Breach Already Exists

Target Confirms Point-Of-Sale Data Breach, Announces It Exposed 40 Million Credit Card Numbers

Posted Dec 19, 2013 by John Biggs (@johnbiggs)

28 Like 2k Tweet 409 Share 64 Next Story

Today retailer Target announced that between November 27 and December 15 its point-of-sale systems – the cash registers mounted at the check-out areas of its stores – suffered an attack that exposed an estimated 40 million credit and debit card numbers. The company announced that it has "alerted authorities and financial institutions immediately after it was made aware of the unauthorized access, and is putting all appropriate resources behind these efforts." It said it has hired outside support to investigate the source and method of the breach.

Thieves made off with customer names, card numbers, as well as expiration dates and the three-digit CVV security code. Only customers who visited Target stores were compromised.

CrunchBase

Target

Financial Liability For Data Breach Already Exists

Convenience Store POS Software with StorePoint

With rising retail market competition and a new generation of demanding, well-connected shoppers, convenience store chains have come under increasing pressure to consolidate and streamline their operations.

Retalix StorePoint's POS & Store Management has been designed from the ground up to enable retailers to do just that. It is comprised of highly appealing, easy-to-use and configurable touchscreen-based points of sale, combining such multiple concepts as convenience store, fuel and QSR (Quick Service Restaurant) sales, supporting both retail chain-owned and franchised channels, and capable of incorporating multiple profit and loss centers in individual stores. POS terminals can be deployed over any hardware platform and integrated with a broad range of retail-related devices - scanners, scales, printers, electronic payment devices, video cameras, kiosks, electronic safes and others – as well as with multiple payment networks and forecourt services.

The solution provides optimized management of multiple points of sale – both in-store and outdoor – effectively enabling convenience store chains to maintain the highest customer checkout throughput.

How Can It Help You? | **What Makes It Unique?**

- High consistency and operational efficiency via robust and scalable architecture
- Freedom of choice and cost efficiency through complete hardware independence
- Increased productivity and user-friendliness via state-of-the art, touchscreen-based POS terminals with a customizable virtual keyboard and flexible GUI
- High versatility with support for a broad range of promotions, discounts and loyalty functions

Retalix StorePoint

"Enhanced security and manageability via comprehensive and flexible access and authorization control"

Expansion Of Liability Is Likely Coming

- Liability already exists due to a data breach
  - Currently on the company that had the breach regardless if it was the fault of a software product they purchased and expect security in place
- Large companies can handle the costs, however, small businesses filing for bankruptcy
  - Doing everything right but the software they purchased with an expectation to be secure isn't
- Is this right?

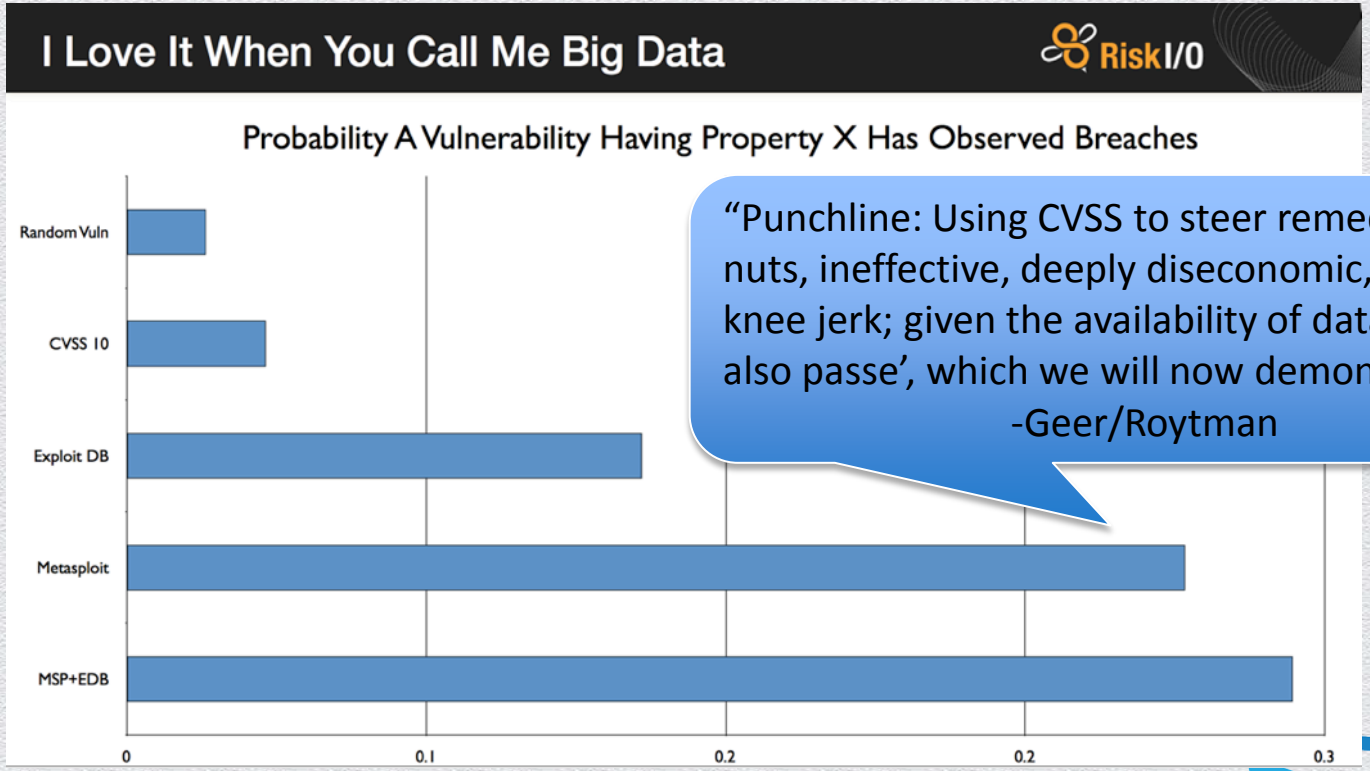
Not from Whole Cloth

- UL for electronics
- NTSB & ASRS for aviation
- NHSTB? or NHTSA? for vehicles
- FDA & DHS ICS-CERT for medical
- FCC for “radio controlled”
- FTC for enforcement
- SEC for publically traded
- Consumer Reports?

Taking Care: Incentives Incentivize (Perversely)

- Let's NOT recreate PCI DSS
  - Outcomes over Inputs (Control Objectives over Controls)
  - Visibility to support Free Market Forces and Choice
- Filter on "With the potential to affect human life and public safety"
- Due Care / Negligence / Reasonability
  - Software must be "Patchable"
  - HDMoore's Law (and/or OWASP Top 10?)
- ***We had better know what we really want to incentivize…***

Yes… HDMoore's Law (Bellis & Roytman [&Geer])

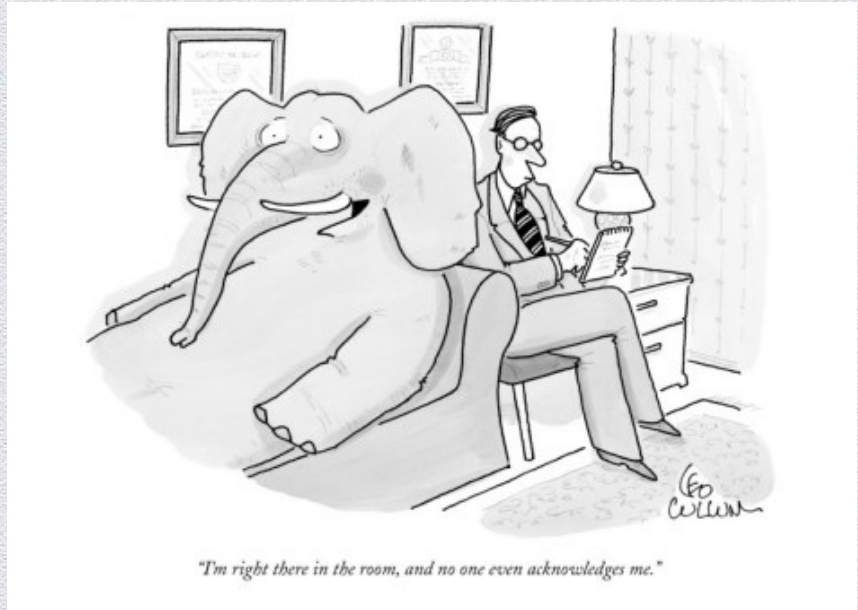


How Could Software Liability Work?

- Not be prescriptive on what needs to be done / security implement
- Allow for the concept of liability to exist in software world
  - Not just for tangible products
  - Not just for Bodily Injury / Property Damage
- Ensure security is not the last items on the priority list (new features FTW)

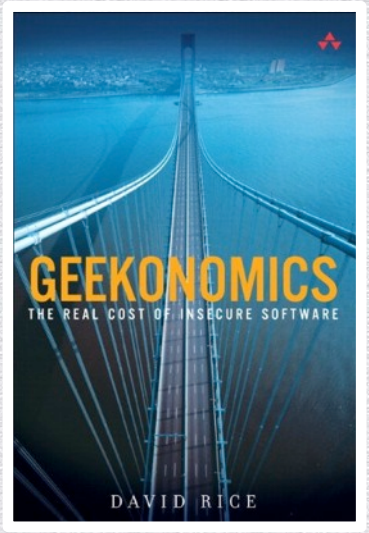
The EULA Elephant in the Room…

- EULAs may be the primary obstacle
- These 1 sided contracts cannot be overlooked
- EULA Reform may be close
  - E.g. No more than 1 page of plain speak



Things you can do

- Investigate/Join “The Cavalry” @iamthecavalry
  - Public Safety & Human Life
- Watch
  - Hot Coffee
- Reading:
  - *Geekonomics* by David Rice
  - Therac-25 History



Discussion!

RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Software Liability?: The Worst Possible Idea (Except for all Others)

SESSION ID: ASEC-F01

Jake Kouns
Chief Information Security Officer
Risk Based Security
@jkouns

Joshua Corman
CTO
Sonatype
@joshcorman