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

Jake Kouns
Chief Information Security Officer
Risk Based Security
@jkouns

Joshua Corman
CTO
Sonatype
@joshcorman

#RSAC @RSACConference
Democracy is the worst form of government except all the others that have been tried.

-Winston Churchill
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…
Our Bodies
In our homes
Miss Teen USA: Screamed upon learning she was 'sextortion' victim

By Phil Gast, Mariano Castillo and Greg Botelho, CNN

updated 0:30 AM EDT, Sat September 28, 2013
Tag: plc

16 MAR 11  Rockwell ENBT
Rockwell 1756 ENBT Chasis

13 APR 12  THUS plc
Used in England a lot

5 NOV 10  TAC/XENTA 913
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.

6 NOV 10  Allen Bradley SLC5
Allen Bradley SLC5 PLC

15 JAN 12  Omron NS web interface
username: default password: default
RT @jwunder: A bunch of PLC exploits are about to drop in Metasploit, meaning soon hacking SCADA systems can be push of a button easy
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

Take the number of vehicles in the field

Multiply it by the probable rate of failure

Then multiply the result by the average out of court settlement
Failure To Warn

SHOULD WE INITIATE A RECALL?
Breach of Warranty

Warranty Certificate

DIAMOND STANDARD PARTS ARE GUARANTEED AS A REPLACEMENT PART FOR
DIAMOND STANDARD PARTS ARE GUARANTEED AS A REPLACEMENT PART FOR
DIAMOND STANDARD PARTS ARE GUARANTEED AS A REPLACEMENT PART FOR
DIAMOND STANDARD PARTS ARE GUARANTEED AS A REPLACEMENT PART FOR
DIAMOND STANDARD PARTS ARE GUARANTEED AS A REPLACEMENT PART FOR
DIAMOND STANDARD PARTS ARE GUARANTEED AS A REPLACEMENT PART FOR
DIAMOND STANDARD PARTS ARE GUARANTEED AS A REPLACEMENT PART FOR
DIAMOND STANDARD PARTS ARE GUARANTEED AS A REPLACEMENT PART FOR
DIAMOND STANDARD PARTS ARE GUARANTEED AS A REPLACEMENT PART FOR
DIAMOND STANDARD PARTS ARE GUARANTEED AS A REPLACEMENT PART FOR
DIAMOND STANDARD PARTS ARE GUARANTEED AS A REPLACEMENT PART FOR

TEN YEAR LIMITED WARRANTY

Ten Year Limited Warranty certificate covering your use of the
ten Year Limited Warranty certificate covering your use of the
ten Year Limited Warranty certificate covering your use of the
ten Year Limited Warranty certificate covering your use of the
ten Year Limited Warranty certificate covering your use of the

LIMITED WARRANTY

BULLET EXPRESS TRIO ONE-YEAR LIMITED WARRANTY

As Bullet Express, LLC, we take pride in our products. We go out of our way to make
As Bullet Express, LLC, we take pride in our products. We go out of our way to make
As Bullet Express, LLC, we take pride in our products. We go out of our way to make
As Bullet Express, LLC, we take pride in our products. We go out of our way to make
As Bullet Express, LLC, we take pride in our products. We go out of our way to make
As Bullet Express, LLC, we take pride in our products. We go out of our way to make

© 2014 EMC Corporation. All rights reserved.
Product Liability Implementation
Who knows the name of this car?

- Allegations that the Pinto's structural design allowed its fuel tank filler neck to break off and the fuel tank to be punctured in a rear-end collision, resulting in deadly fires from spilled fuel.
- 27 deaths were attributed to Pinto fires.
- According to a 1977 *Mother Jones* article by Mark Dowie, Ford allegedly was aware of the design flaw, refused to pay for a redesign, and decided it would be cheaper to pay off possible lawsuits.

- Allegations that the Pinto’s structural design allowed its fuel tank filler neck to break off and the fuel tank to be punctured in a rear-end collision, resulting in deadly fires from spilled fuel.
- 27 deaths were attributed to Pinto fires.
- According to a 1977 *Mother Jones* article by Mark Dowie, Ford allegedly was aware of the design flaw, refused to pay for a redesign, and decided it would be cheaper to pay off possible lawsuits.
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

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

$0 DOWN with AT&T Next. 13 megapixel camera for super-sharp pictures
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?

April 8, 2014
Product Liability for Software Vendors
Software Liability

• Software Liability: Our Saving Grace or Kiss of Death?
  – Debated by Marcus Ranum and Bruce Schneier at RSA 2012

• At this point, the issue seems to be still unresolved
  – With most people being on the side that it is an awful idea
Software Liability

• Software Liability: Our Saving Grace or Kiss of Death?
  – Debated by Marcus Ranum and Bruce Schneier at RSA 2012

• At this point, the issue seems to be still unresolved
  – With most people being on the side that it is an awful idea
Software Liability: Worst Idea

Churchill Democracy
Tragedy of the Commons
Rational agents in a free market usually optimize themselves
Information Asymmetry
Lemon Laws
Certifications
Signals
Economics
True Costs
Least Cost Avoider
Free Market Forces

None
Why we don’t want to do it
US GDP Growth
Init competitiveness
Barriers to entry could stifle new/small entrants (FTC/SEC)
Assumption Market Demand isn’t there or it is minority
Perceived ZeroSum w/ Features/Sex/Sizzle/Competitiveness

Can’t write perfect software
Might drive players out of the market
Less Features
Less Innovation
Less Content
Slower time to market
Higher cost of goods
People want (features and cheap) over security

Apple is less secure but gaining more market share over MSFT

Roger Grimes
In our homes
In/On our bodies
Mass Transit
Critical Infra
Panopticon

Complexity Growing
Human Life & Public Safety More and More
National Security
Critical Infrastructure

Underconsidered Factors
Incumbents
Buyers

Unobvious reasons some camps SHOULD want it

SW Liability
Alternatives to Liability

OWASP Top 10 assurances
HDMoore’s Law
Patchability
Patching SLA
Published SDLC
3rd Party Code Review
EULAs are ONE SIDED to date
Tamper Evident?

RFPs

Do this exercise with Jake/Andrea/David/Katie
More F/IOS7
What might happen if we add it

Fewer players?

Game Theory it out

Shared relay race
Pach supplied
Making IT PATCHABLE does an out to Manufacturers?
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

<table>
<thead>
<tr>
<th></th>
<th>Food Safety</th>
<th>Cars</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Stifle Innovation</td>
<td>Chef’s can’t innovate?</td>
<td>Safety Differentiation</td>
</tr>
<tr>
<td>2) Barriers to Entry</td>
<td>Good!</td>
<td>Outstanding!</td>
</tr>
<tr>
<td>3) Economic Impact</td>
<td>Doubtful</td>
<td>Premium Pricing</td>
</tr>
<tr>
<td>4) Raise Prices/Exit</td>
<td>To avoid illness/disease?</td>
<td>Free Market Demand</td>
</tr>
</tbody>
</table>

Markets
What’s Working To Influence Better Security Practices?
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

<table>
<thead>
<tr>
<th>Year</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013</td>
<td>10,280</td>
</tr>
<tr>
<td>2012</td>
<td>9,909</td>
</tr>
<tr>
<td>2011</td>
<td>7,751</td>
</tr>
<tr>
<td>2010</td>
<td>9,054</td>
</tr>
<tr>
<td>2009</td>
<td>8,092</td>
</tr>
<tr>
<td>2008</td>
<td>9,696</td>
</tr>
<tr>
<td>2007</td>
<td>9,538</td>
</tr>
<tr>
<td>2006</td>
<td>11,009</td>
</tr>
<tr>
<td>2005</td>
<td>7,858</td>
</tr>
</tbody>
</table>
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...
True Costs & Least Cost Avoiders

ACME

Enterprise
Bank
Retail
Manufacturing
BioPharma
Education
High Tech

$$$
Passing the Buck (and Cost)

Defensibility Index

Goal
Security++
Security
Base
Passing the Buck (and Cost)

Defensibility Index

Goal
Security++
Security
Base
Passing the Buck (and Cost)
True Costs & Least Cost Avoiders

ACME

Enterprise

Bank

Retail

Manufacturing

BioPharma

Education

High Tech

$$$
True Costs & Least Cost Avoiders: Downstream

- Enterprise
- Bank
- Retail
- Manufacturing
- BioPharma
- Education
- High Tech

ACME

© 2014 EMC Corporation. All rights reserved.
The Fallacy of Broken Windows

The Broken Window Fallacy
True Costs & Least Cost Avoiders

ACME

Enterprise
Bank
Retail
Manufacturing
BioPharma
Education
High Tech

$100
$110
Where Do We Go From Here?
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

- It's 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.

  - 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”
Open Automotive Alliance aims to bring Android inside the car
Can Google make your car safer and friendlier to use?

by JasonIfnostioues - Jan 6 2014, 9:33am EST

Google, Audi, GM, Honda, Hyundai, and Nokia have formed the Open Automotive Alliance (OAA) in the hopes of improving our automotive experience through an open platform for smartphone integration. How does this fit into Google’s larger plan to become a destination for greener, safer, and smarter cars? And what could this mean for Android’s overall strategy in mobile computing? 

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

By Danial Harig

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.
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)

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.
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.

Retailix 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?

- 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

What Makes It Unique?

“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])

“Punchline: Using CVSS to steer remediation is nuts, ineffective, deeply diseconomic, and knee jerk; given the availability of data it is also passe’, which we will now demonstrate.”

-Geer/Roytman
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

“I’m right there in the room, and no one even acknowledges me.”
Things you can do

• Investigate/Join “The Cavalry” @iamthecavalry
  – Public Safety & Human Life
• Watch
  – Hot Coffee
• Reading:
  – *Geekonomics* by David Rice
  – Therac-25 History
Software Liability?: The Worst Possible Idea (Except for all Others)

Jake Kouns
Chief Information Security Officer
Risk Based Security
@jkouns

Joshua Corman
CTO
Sonatype
@joshcorman