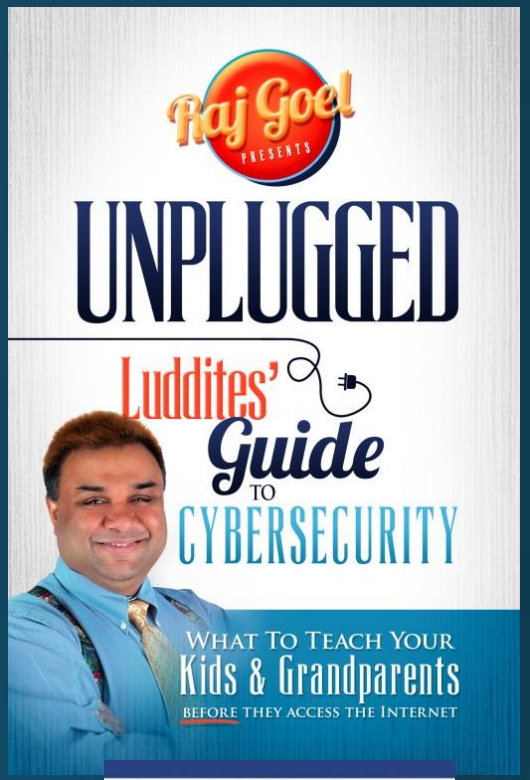
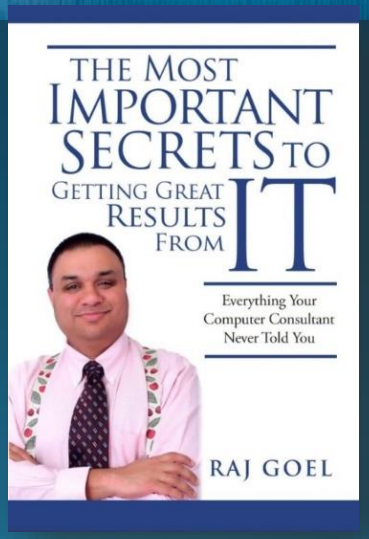
Supply Chain Insecurity: WannaCry, NotPetya, & Meltdown vs. Dieselgate

Raj Goel, CISSP
raj@brainlink.com / 917-685-7731
www.RajGoel.com
@rajgoel_ny





ISC2 Article – A Bitter Pill

A SOUNDING BOARD FOR THOSE WITH SOMETHING TO SAY

members' corner

BY RAJ GOEL, CISSP

A Bitter Pill

Stronger software liability would fix much of what ails us.

"Software is eating the world." –*Marc Andreesen*

"If builders built buildings the way programmers wrote programs, then the first woodpecker that came along would destroy civilization." –*Gerald Weinberg*

Both of those quotes give us much to ponder. Software is eating the world…and shoddy software is caving in on us. Consider:

- **Medical device** (pacemakers, insulin pumps, medication dispensing robots, etc.) hacks as assassination tools have jumped from spy thrillers and TV shows to real-life possibilities, as demonstrated by University of South Alabama students and reported in *Computerworld* in September 2015.
- Almost every major brand of **car** (Jeep, Mercedes, BMW, Tesla, Ford, etc.) has been hacked in tests, according to a July 2015 *Wired* report.
- **Web browser** security is an oxymoron. Seeing every major browser get hacked at pwn2own has become a rite of passage, as well as big prize money as posted by Trend Micro in March 2016.
- **Adobe Flash** is the poster child for massively insecure software. Steve Jobs famously banned it from Apple products, describing his concerns in 2010 in an online post.

Raj Goel, CISSP, is CEO of New York-based Brainlink and can be reached at raj@brainlink.com.

I've long advocated for us to adopt software liability laws. And a typical response is: "We'll never get rid of zero-days."

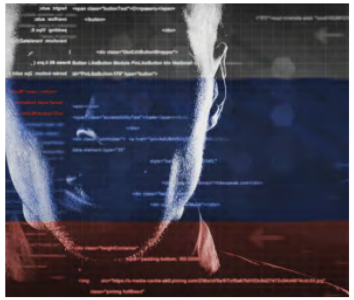
I believe that, as an industry, we fetishize zero-days a bit too much. Yes, they exist and are used in some attacks, but the vast majority of attacks succeed due to insufficient patching, inadequate monitoring and shoddily developed software.

Photographs: Thinkstock

But, since people like to bring up zero-days, let's put that to bed.

The most impressive zero-day attack that occurred in the real world, in my opinion, was the 1982 Chicago Tylenol murders. An unknown individual (or individuals) bought Tylenol bottles in the Chicago area, opened them, added cyanide capsules to the bottles and replaced them on the store shelves. Seven people died as a result. No one was ever caught.

With millions of dollars at stake, not to mention public safety, Johnson & Johnson took what was at that time an extraordinary approach—a massive product recall. "Before 1982, nobody ever recalled anything," said Albert Tortorella, a managing director at Burson-Marsteller Inc., the New York public relations firm that advised Johnson & Johnson. Its board and management decided to put patient safety first. Breaking with industry tradition, they went public with the details. They offered a free recall of every Tylenol bottle in America. The recall cost Johnson & Johnson more than $100 million, and it initially lost market share.



In less than a decade, not only did the company regain market share, it exceeded its previous market share for over-the-counter pain relief medication. As a footnote, Johnson & Johnson and the pharmaceutical industry developed tamper-proof packaging, caplets, and made secure, tamper-proof packaging an industry requirement.

Another excuse for opposing software liability regulations: "I can't do anything about it—it's too big an issue." Here is a case study that refutes that claim.

Fed up with shoddy and dangerous food production practices (rotting meat, vermin, animal feces, excessive workplace injuries, etc.), Upton Sinclair wrote the expose *The Jungle* in 1906, leading to massive public outcry and the eventual passage of the Pure Food and Drug Act, the precursor of the U.S. Food and Drug Administration (FDA), which arguably has saved more lives than any other act of Congress.

The Pure Food and Drug Act also led to thousands of food manufacturers and patent medicine manufacturers going bankrupt. Big or small, if they couldn't produce food safe for human consumption or so-called "elixirs" that weren't poisonous, they weren't allowed to sell their wares.

A third common excuse for not supporting software liability laws: "Software is too complicated and too important to the economy to be regulated."

Every industry, like every company, begins as a startup. That includes railroads, manufacturing, telecom, automobiles and software. As industries mature, they become central to the economy. Billions of dollars are made by a handful of individuals or firms that focus on generating profits and externalize safety costs.

It usually takes horrific accidents or a large number of deaths to capture the public's imagination and/or require these industries to change practices. I strongly recommend you watch *Modern Marvels: Engineering Disaster*, a History Channel docudrama, to see how industry after industry (grain processing, sugar processing, bridge construction, stadium construction, shipping, etc.) investigated failures, developed new standards, made them mandatory and improved society.

I think it's time we drew lessons from history and started agitating for software liability reform.

The industry closest to software, in my mind, is the cigarette industry.

In the 1920s, cigarette manufacturers advertised their cigarettes as weight-loss products and adding sex appeal. By the 1950s, as revealed in later litigation, the cigarette industry knew that smoking tobacco caused cancers and other health issues but the dangers were not commonly known. It wasn't until the 1990s when 40 U.S. states joined a class-action lawsuit that led to $206 billion in fines, elimination of cigarette marketing to children and a robust anti-smoking education campaign.

As information security professionals, IT managers or simply end users, we are the crash test dummies for software developers and until we start telling the truth to ourselves, our clients and vendors, we will keep suffering from compromises due to faulty products.

The Mirai botnet, a collection of 400,000 infected bots ready to create DDoS attacks, is not an accident. Nor is Business Email Compromise (BEC) an unintentional industry. Ransomware did not arise by chance, either. All are the result of decades of commercial incentives that let developers ship software with no security, no controls and no responsibility.

I think it's time we drew lessons from history and started agitating for software liability reform. It's 2017 and we're overdue for an overhaul. We need to apply existing consumer protection laws to software, revoke EULAs and uphold our right to buy only software that's fit for safe use.

In my mind, only two industries exist in the United States with zero consumer protection laws: illegal drugs and software. And both industries call their customers "users." ■

"Software is eating the world"
- Marc Andressen

"I've got food poisoning ☹"
- EVERYONE ELSE

Famous Recalls in History

FORD PINTO

- Ford recalled more than 1.5 million Pintos in 1978 due to the faulty position of fuel tanks. In some cases, the fuel tank burst into flames after a rear-end collisions. At least 27 people died as a result.

TYLENOL

- About 35 years ago, Johnson & Johnson recalled more than 20 million bottles of Tylenol capsules after someone laced the painkillers with cyanide and put them in store shelves in the Chicago area. Seven people were killed. Johnson & Johnson repackaged Tylenol with tamper-resistant packaging, showing how a company could emerge from a disaster and improve an industry.

Famous Recalls in History

FIRESTONE TIRES

- About 6.5 million Firestone tires were recalled in 2000 because the tires could shred, blow out or fail. Most of the tires were used in Ford SUVs and light pickup trucks. The National Highway Traffic Safety Administration said in 2001 that it received 271 reports of deaths and 800 injuries related to the faulty tires.

EASY-BAKE OVENS

- Nearly one million Easy-Bake Ovens were recalled in 2007 after toy maker Hasbro received reports that kids were getting their hands stuck in the oven's opening. Some kids sustained burns.

KEURIG COFFEE MACHINE

- Keurig recalled more than 7 million of its single-serve coffee brewing machines after reports that some of them spewed hot liquids and injured people.

Dieselgate

- VW & other auto manufacturers used software to cheat on Diesel emission tests
- Blamed low-level engineers
- Regulators didn't buy that excuse or reasoning

Dieselgate - Penalties

- VW paid $25 BILLION in fines
- Porsche Executive arrested
- VW US Engineering boss, **Oliver Schmidt**, sentenced to **SEVEN YEARS IN PRISON + $400,000 fine**

Toyota Brakes – The Saga Begins

- Floor mats. In some cases, an unsecured driver's floor mat can supposedly jam the gas pedal. Complaints and deaths stemming from this issue led to the first Toyota recall. Secure your floor mats, take them out, or, if you're too lazy to do either of those and the mat jams the accelerator, shift to neutral.
- Sticky throttles. The accelerator may stick in some Toyotas. NHTSA hasn't determined that this has actually caused any fatalities, but there is enough evidence that the throttle may stick to warrant a recall. If this happens to you, shift to neutral.
- The "electronic issue." Unlike vehicles from some other automakers, Toyotas don't kill the throttle when you hit the brakes. **This means it's possible to apply both at the same time**

https://www.caranddriver.com/features/toyota-recall-scandal-media-circus-and-stupid-drivers-feature

Toyota Recalls

- 1st Recall – 4.2 Million cars
- 2nd Recall – 2.3 Million cars

In addition, 1.7 million vehicles are covered by both recalls. All 2009 and 2010 Pontiac Vibes, which are mechanically identical to the Toyota Matrix and built in the same plant, are also affected.

http://www.motortrend.com/news/toyota-recall-crisis/

Toyota Investigations & Costs

- NHTSA (National Highway Traffic Safety Administration, US)
- MLIT (Ministry of Land, Infrastructure, Transport & Tourism, Japan)
- US Congressional hearings

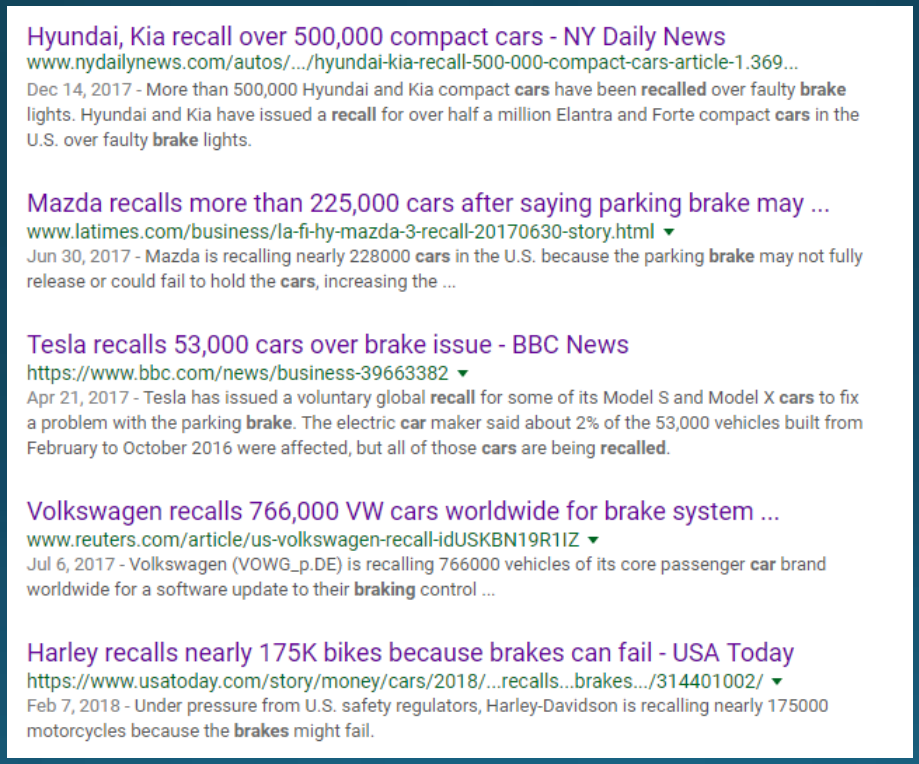
Each DEALER lost $1.75M-$2M per month in revenue

$2.5Billion lost revenue across the industry

$2billion in losses to Toyota

https://en.wikipedia.org/wiki/2009-11_Toyota_vehicle_recalls

Recalls – it ain't a SOLO story



Hyundai, Kia recall over 500,000 compact cars - NY Daily News
www.nydailynews.com/autos/.../hyundai-kia-recall-500-000-compact-cars-article-1.369...
Dec 14, 2017 - More than 500,000 Hyundai and Kia compact **cars** have been **recalled** over faulty **brake** lights. Hyundai and Kia have issued a **recall** for over half a million Elantra and Forte compact **cars** in the U.S. over faulty **brake** lights.

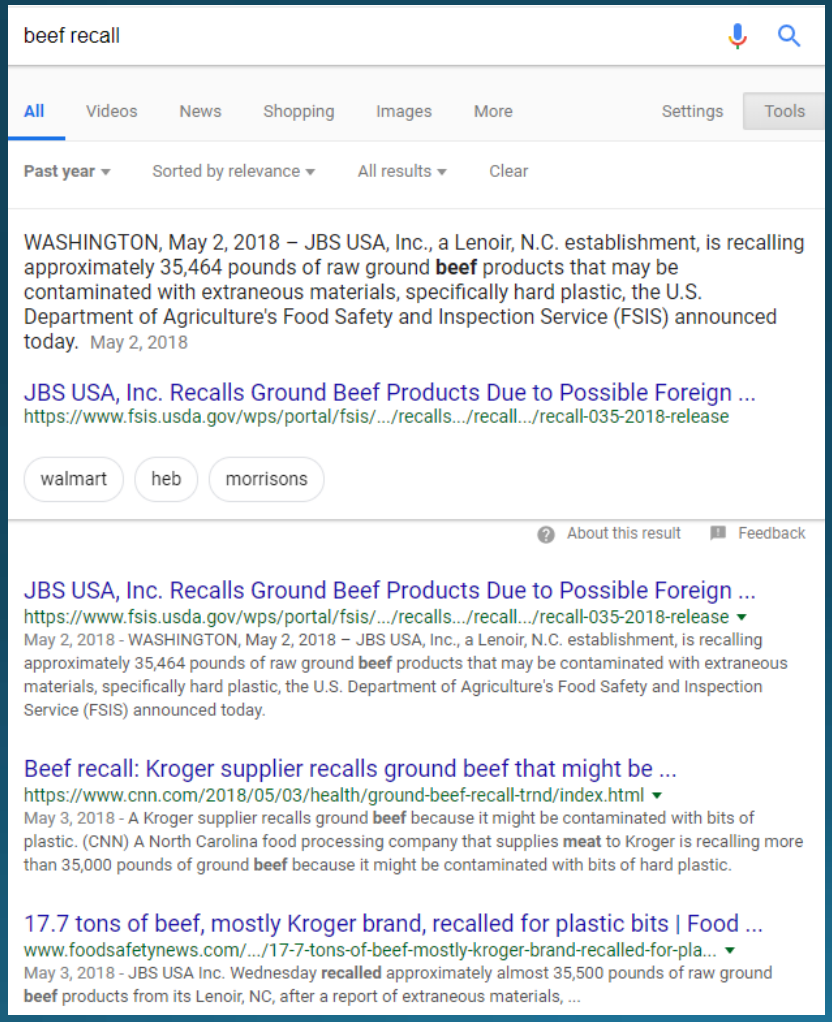
Mazda recalls more than 225,000 cars after saying parking brake may ...
www.latimes.com/business/la-fi-hy-mazda-3-recall-20170630-story.html
Jun 30, 2017 - Mazda is recalling nearly 228000 **cars** in the U.S. because the parking **brake** may not fully release or could fail to hold the **cars**, increasing the ...

Tesla recalls 53,000 cars over brake issue - BBC News
https://www.bbc.com/news/business-39663382
Apr 21, 2017 - Tesla has issued a voluntary global **recall** for some of its Model S and Model X **cars** to fix a problem with the parking **brake**. The electric **car** maker said about 2% of the 53,000 vehicles built from February to October 2016 were affected, but all of those **cars** are being **recalled**.

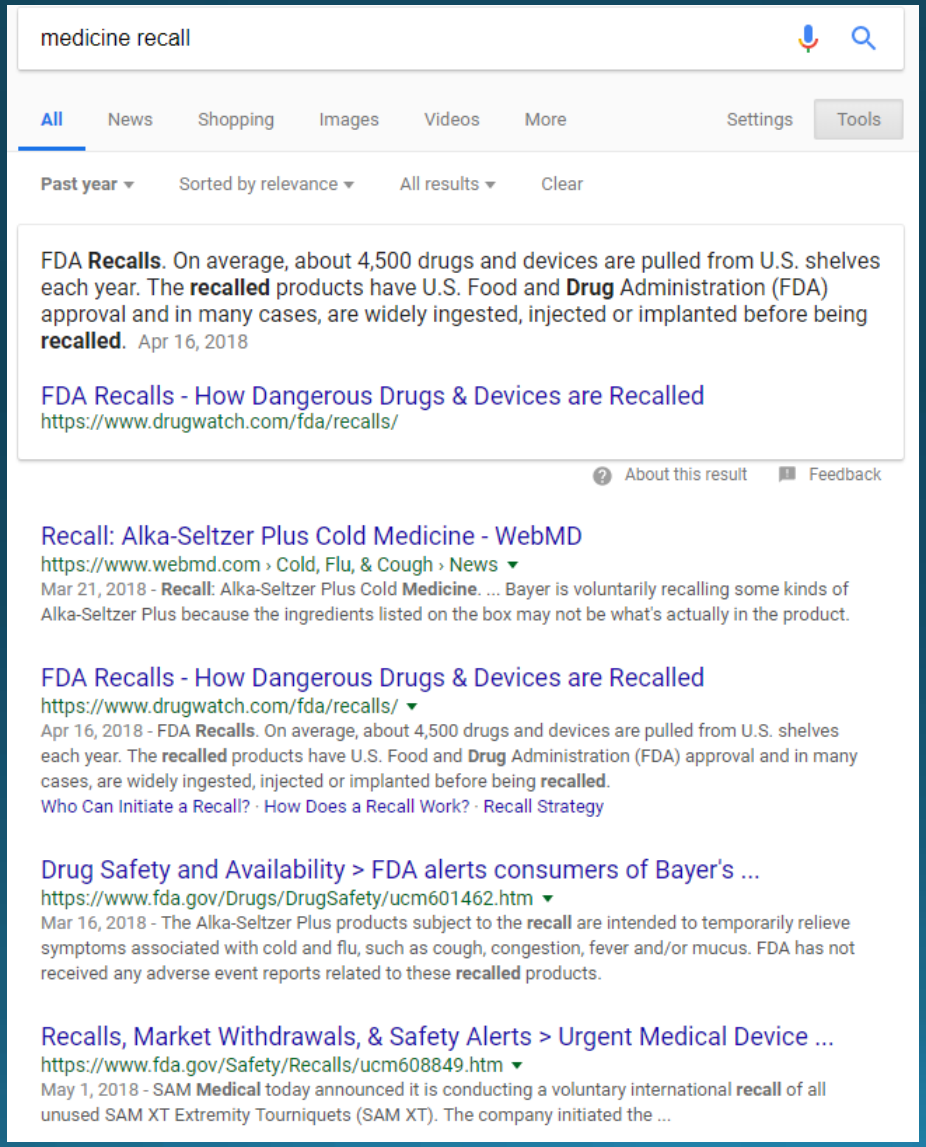
Volkswagen recalls 766,000 VW cars worldwide for brake system ...
www.reuters.com/article/us-volkswagen-recall-idUSKBN19R1IZ
Jul 6, 2017 - Volkswagen (VOWG_p.DE) is recalling 766000 vehicles of its core passenger **car** brand worldwide for a software update to their **braking** control ...

Harley recalls nearly 175K bikes because brakes can fail - USA Today
https://www.usatoday.com/story/money/cars/2018/...recalls...brakes.../314401002/
Feb 7, 2018 - Under pressure from U.S. safety regulators, Harley-Davidson is recalling nearly 175000 motorcycles because the **brakes** might fail.

Where's the (tainted) Beef?



Dr. Bad Medicine



What We HAVE


Parliament
Basic
Marlboro
FILTER CIGARETTES
Microsoft
Windows 10
Pro
Windows 10
Home
WinFuture

What We WANT


Windows 10
Microsoft
Windows 10
Pro
WARNING: Use of this software may be injurious to your health, safety, privacy & civil rights
Microsoft
Windows 10
Home
WARNING: Use of this software may be injurious to your health, safety, privacy & civil rights
WARNING: Use of this product may be injurious to your safety, privacy & civil rights

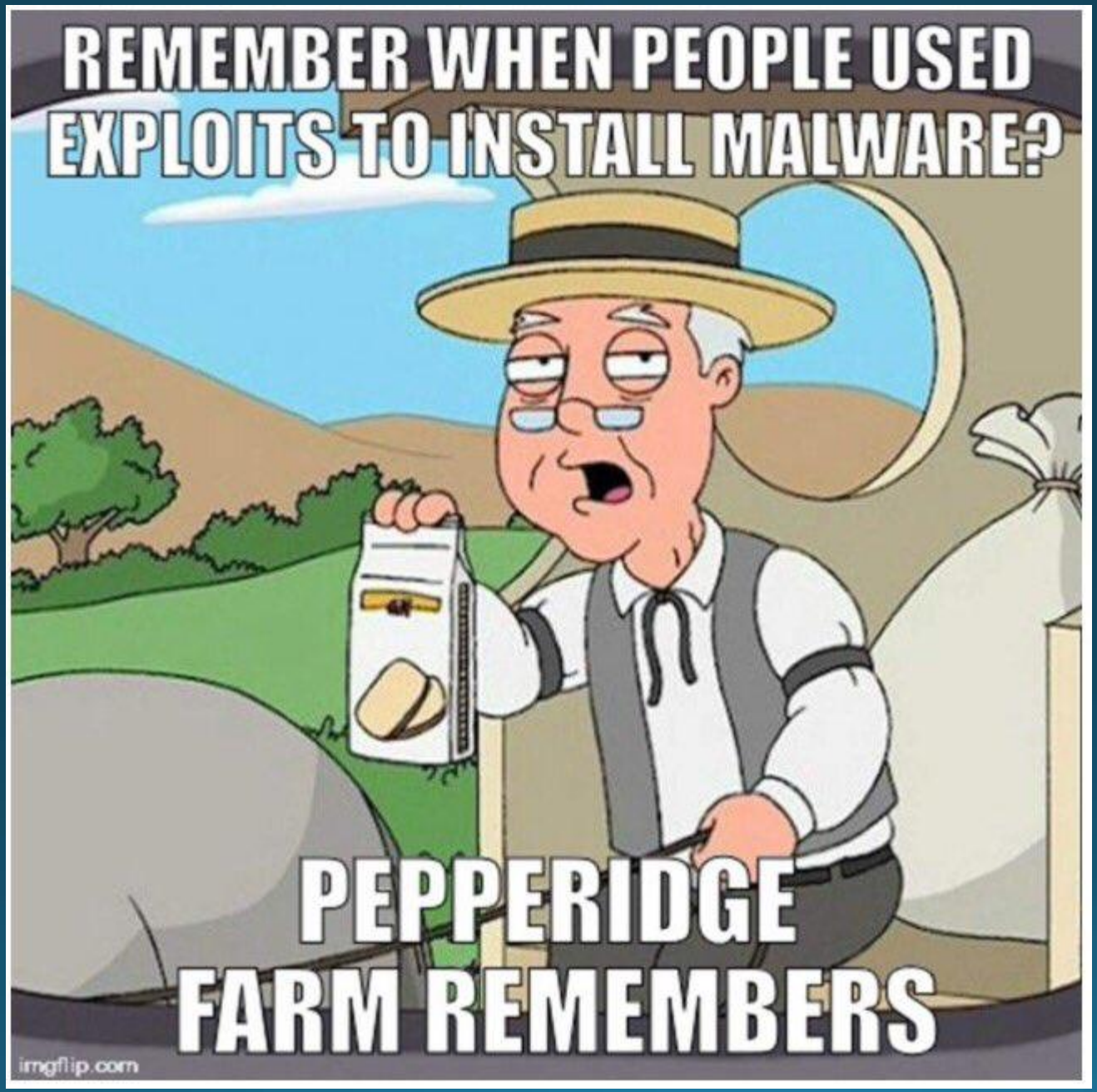

Marlboro
Smoking seriously harms you and others around you
Smoking seriously harms you and others around you
RICHMOND
Smoking seriously harms you and others around you
Vogue
Smok-ing kills

I Agree"

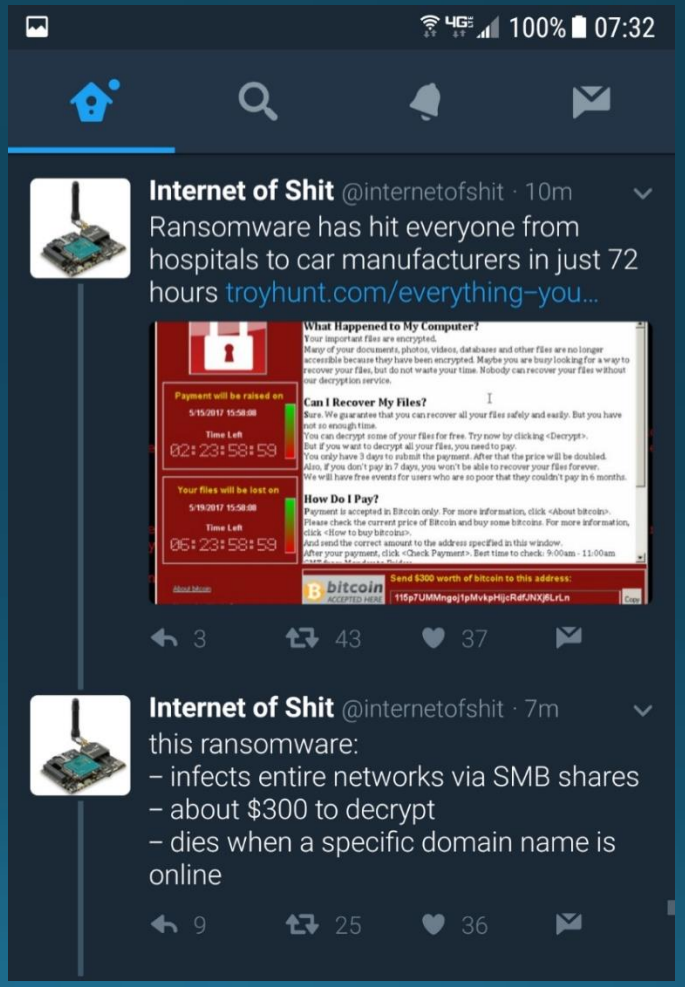
By
Dima Yarovinsky's

I Agree"

By
Dima Yarovinsky's


REMEMBER WHEN PEOPLE USED EXPLOITS TO INSTALL MALWARE?
PEPPERIDGE FARM REMEMBERS
imgflip.com

WannaCry – a Brief History of Crime



Boeing hit by WannaCry cyber attack

- [...] causing panic as concerns were raised that it would spread to automated assembly tools on the 777 production line, the *Seattle Times* reported.
- Concerns were also raised the virus could affect equipment used to test aeroplanes ready to roll off the production line, and could potentially spread to aeroplane software.
- Among the victims were **FedEx, Deutsche Post, Nissan** and the **NHS**. The attack disrupted ***more than a third of NHS trusts*** in England, as well as **hundreds of GP surgeries.**

https://www.cips.org/supply-management/news/2018/march/boeing-hit-by-wannacry-cyber-attack/

Renault

- *When workers arrived at a Renault plant in Sandouville, in northern France, on Saturday morning, TV screens that usually update staff on company productivity had a different message: A demand, in French, for $300 in ransom. The screens also showed two clocks counting down the time Renault had to deliver the payments before the factory's files were deleted.*
- *An early sign of trouble at the Renault plant in Sandouville came when the assembly line's alarm system stopped working early Saturday—right after the demand for ransom appeared on TV screens. Tanguy Deschamps, a 38-year-old who was working at the factory when the virus hit, said the alarms were failing to sound whenever workers tried to alert others to crooked or improperly welded parts.*

https://talkinglogistics.com/2017/05/15/the-wannacry-cyberattack-another-warning-for-supply-chain-executives/

NotPetya History

- **Piggybacks on Wannacry/EternalBlue & leverages Mimikatz**
- **Initial target was Ukrainian Tax Software firm MEDoc (QuickBooks for Ukraine – use mandated by law)**
- **Spread VERY QUICKLY outside Ukraine**

https://www.theregister.co.uk/2017/06/28/petya_notpetya_ransomware/

NotPetya Impact

- Exploded in 64 countries
- Took down Ukraine Power Grid
- Crippled shipping around the world for weeks
- Impacted airplanes, medicine, candy manufacturers

NotPetya Costs & Impact

- **Exploded in 64 countries**
- **Took down Ukraine Power Grid**

- **Maersk - $275 million** - which warned investors in August that it would lose **between $200 million and $300 million** in third-quarter revenue as a result of NotPetya.
- **FedEx/TNT** - $300 Million in losses
- **Mondelez International** (Cadbury, Oreo, Trident Gum)- $150M
- **Reckitt Benckiser** (Durex, Lysol, Clearasil, etc.) - $129M
- Merck - $300M

https://www.cybereason.com/blog/notpetya-costs-companies-1.2-billion-in-revenue

16:18 **'Carnage today': A dark verdict from London**

An anonymous NHS staffer tells us:

"Absolute carnage in the NHS today. Two Hyperacute stroke centres (the field I work in) in London have closed as of this afternoon. Patients will almost certainly suffer and die because of this.

"Had a patient that needed urgent neurosurgery referred, but unable to look at scans - stroke care is absolutely dependent on IT systems and joined up systems."

CCleaner

- Cisco Talos team discovered CCleaner had been hacked for months
- 2.3 Million infected downloads installed around the world
- Avast bought Piriform WHILE the infection was active

https://www.wired.com/story/ccleaner-malware-supply-chain-software-security/

https://thehackernews.com/2018/04/ccleaner-malware-attack.html

CCleaner – HIGH PRECISION MALWARE

- At least 40 PCs infected by a backdoored version of the CCleaner disk-maintenance utility received an **advanced second-stage payload** that researchers are still scrambling to understand, officials from CCleaner's parent company said.
- The 40 PCs, belonging to 12 technology companies, including **Samsung**, **Asus**, **Fujitsu**, **Sony** and **Intel**, is double the number previously known to have received the advanced follow-on infection. They still represent a minuscule percentage—more precisely, about 0.0018 percent—of the 2.27 million PCs that downloaded the booby-trapped CCleaner update. Avast notified most of the companies that received the stage-two malware and was attempting to contact the remaining victims.

https://arstechnica.com/information-technology/2017/09/ccleaner-backdoor-infecting-millions-delivered-mystery-payload-to-40-pcs/

75% of cars stolen in France…hacked

- Three quarters of cars stolen in France are targeted using electronic hacking, it was claimed on Thursday, prompting calls for urgent security improvements in a range of vehicles sold across Europe.

- The Smart Fortwo model was France's most-stolen car, with the Ford Fiesta and Peugeot 406 models also popular among thieves

- The astonishing figures come two months after computer scientists in the UK warned that thousands of cars – including high-end brands such as Porsches and Maseratis - are at risk of electronic hacking. **Their research was suppressed for two years by a court injunction for fear it would help thieves steal vehicles to order.**

http://www.telegraph.co.uk/news/worldnews/europe/france/11964140/Three-quarters-of-cars-stolen-in-France-electronically-hacked.html

Vehicles – No Keys For YOU!

64% 9:08 PM

Tweet

You Retweeted

Joseph Cox
@josephfcox

Crazy: because of legal restrictions, American farmers are downloading Ukrainian firmware for their tractors motherboard.vice.com/en_us/article/ ...

> To avoid the draconian locks that John Deere puts on the tractors they buy, farmers throughout America's heartland have started hacking their equipment with firmware that's cracked in Eastern Europe and traded on invite-only, paid online forums.

Reply to Joseph Cox

You Retweeted

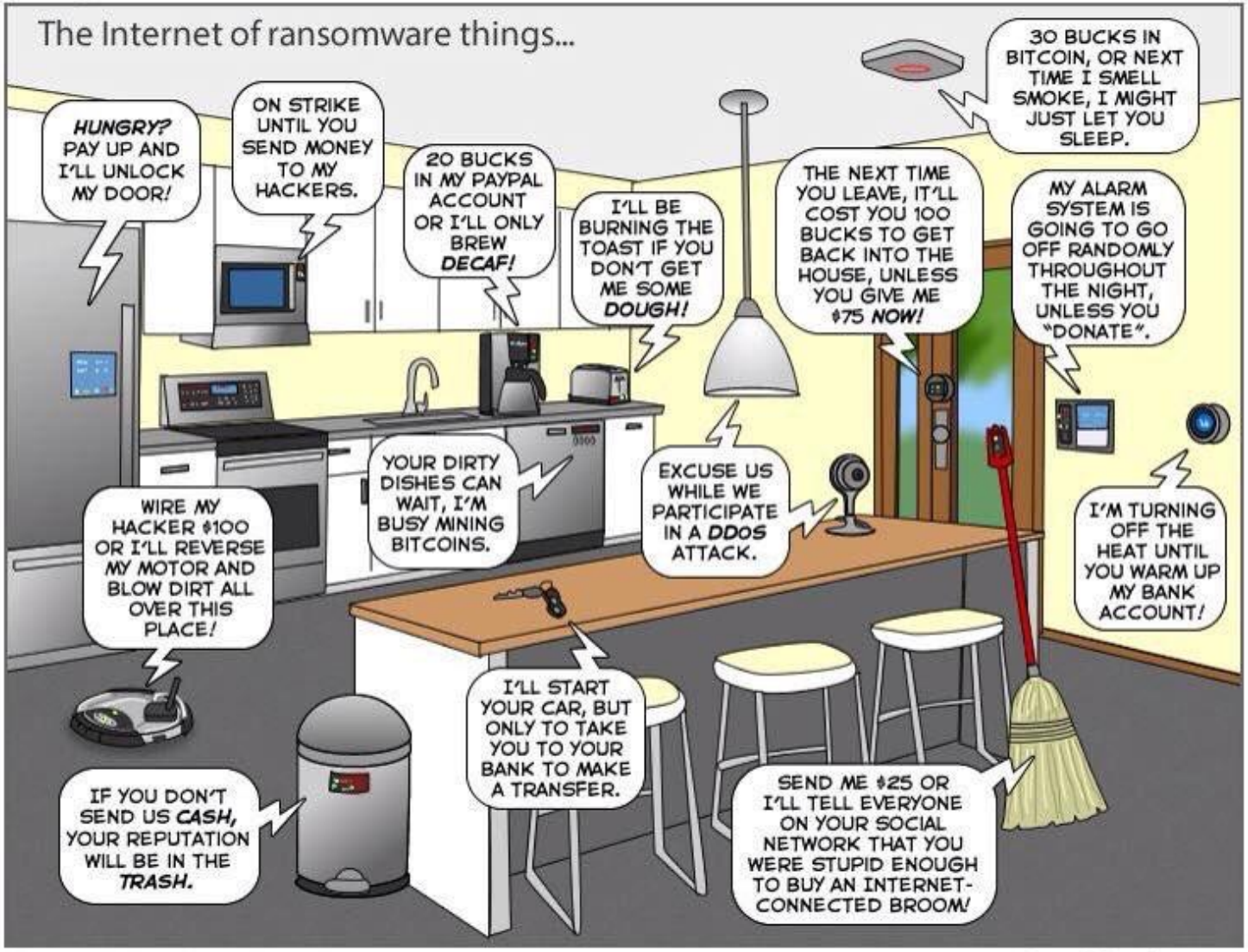
Adam Savage
@donttrythis

It's not hacking, it's called fixing. And we should all have the right to work on and fix things we bought.

Why American Farmers Are Hacking Their Tractors With Ukrainian Firmware
motherboard.vice.com

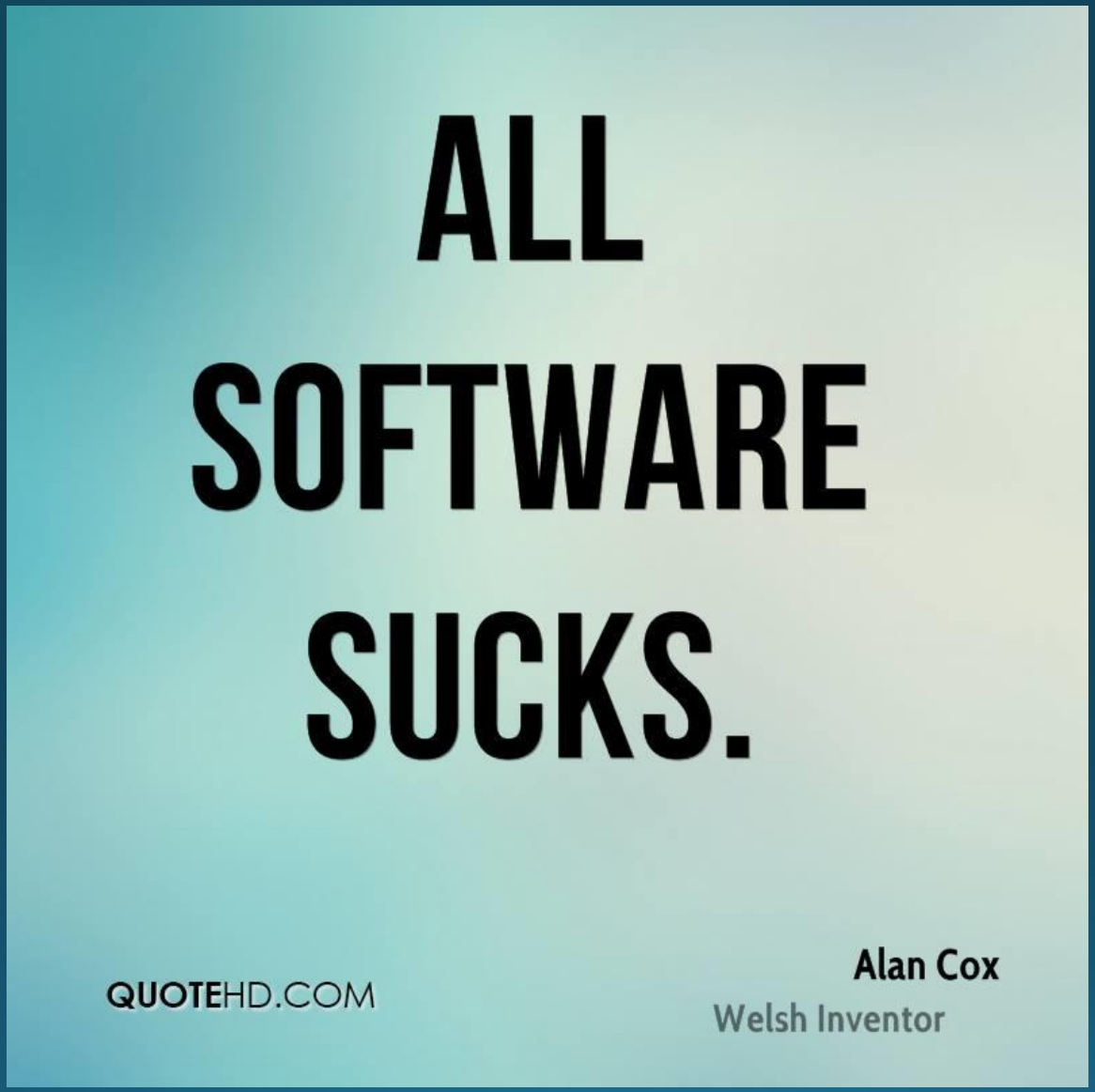
6:49 PM · 22 Mar 17

The Joy of Tech™ by Nitrozac & Snaggy



You can help us keep the comics coming by becoming a patron!
www.patreon/joyoftech

joyoftech.com


ALL
SOFTWARE
SUCKS.
QUOTEHD.COM
Alan Cox
Welsh Inventor

100% 18:09

Tweet

One thing they found is, "8,000 known vulns in 3rd–party libraries across 4 different pacemaker programmer from 4 different manufacturers."

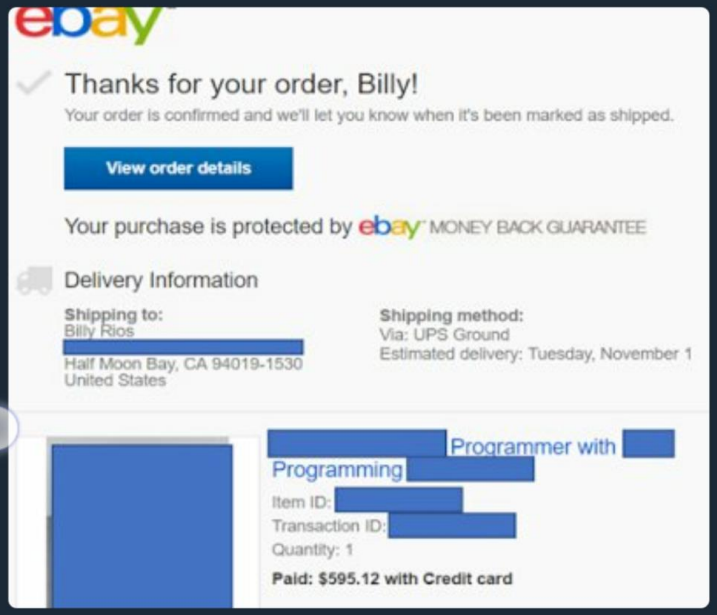
> **Billy Rios** @XSSniper
> We spent the last few months tearing apart various pacemaker systems... here is what we found! blog.whitescope.io/2017/05/unders...

6:00 PM · 25 May 17

Tweet

Jeremiah Grossman
@jeremiahg

And just how did they acquire pacemaker systems, which are supposed to be 'controlled', you might ask? eBay of course!




HELLO, WELCOME TO OUR HOUSE!
THANKS FOR INVITING US!
ALEXA, ORDER TWO TONS OF CREAMED CORN.
ALEXA, CONFIRM PURCHASE.
WHEN VISITING A NEW HOUSE, IT'S GOOD TO CHECK WHETHER THEY HAVE AN ALWAYS-ON DEVICE TRANSMITTING YOUR CONVERSATIONS SOMEWHERE.


I learned the name of the Amazon Echo and placed an order without asking permission.
- Larry Bird

Software, Food, Medicine, Cars

- I see strong parallels between software & food; and software & cars.
- Between 1870 & 1906, the quality of food and medicine sold in the US was frankly, terrible. There were no safety or sanitary practices.
- After the muckrakers agitated, and Upton Sinclair published INTO THE JUNGLE, American society was appalled by the unsanitary food and medicine production practices.

Lessons from FDA

- Congress passed the PURE FOOD AND DRUG ACT (1906)– which led to the creation of the FDA, regulation of FOOD , Medicine, etc.
- A lot of companies died because they could not meet new requirements for cleanliness, safety testing, inspections, etc.
- The net result, however, is that food and medicine in the US became the safest in the world, and influenced food & medical practices worldwide.
- I truly believe that the PURE FOOD & DRUG ACT saved more lives in human history than any other act of Congress.

Lessons from IIHS

- Another parallel to software is the automobile.
- When the automobile was invented, there were no regulations. And for the first few decades, it was seen as a fad; an expensive toy and very much resembled the dotcom economy.
- As cars became central to our lives, the National Highway Safety Commission, driver licensing requirements, mandatory driver's insurance requirements, seat belts, anti-lock brakes, and other safety features were mandated.
- The automakers hated this, and argued that building safer, more efficient cars would destroy the automobile industry.
- What we saw instead, is that some manufacturers died; the industry consolidated into a handful of big brands, and cars produced in 2016 are much safer, more efficient and frankly better than anything produced in 1950, 1970 or even 1990.

Dr. A rolled his eyes.

It was last October, and he had just come across a triage note tha

Dr. A — we're not using his name or identifying his hospital, whi
protect patient safety — is 28 years old, a resident and about as g

And he's got a patient who claims she's got a GPS tracking device

"When you work on the east side of our hospital, psychiatric pati

But this patient is different. She's put together. She's lucid. She's

A group crowded around the computer to see her x-ray.

"Embedded in the right side of her flank is a small metallic objec
rice," he said. "But it's there. It's unequivocally there. She has a tr
speaking for like five seconds — and in a busy ER that's saying something."

Patrick O'Neill ✓
@HowellONeill

A tracking chip was removed from a patient who was a victim of human trafficking marketplace.org/2016/03/02/hea...

Dr. A rolled his eyes.

It was last October, and he had just come across a triage note that said, "I have a tracker in me."

Dr. A — we're not using his name or identifying his hospital, which is in a major American city, to protect patient safety — is 28 years old, a resident and about as green as they come.

And he's got a patient who claims she's got a GPS tracking device implanted in her side.

"When you work on the east side of our hospital, psychiatric patients are a dime a dozen," he said.

But this patient is different. She's put together. She's lucid. She's got an incision.

A group crowded around the computer to see her x-ray.

"Embedded in the right side of her flank is a small metallic object only a little bit larger than a grain of rice," he said. "But it's there. It's unequivocally there. She has a tracker in her. And no one was speaking for like five seconds — and in a busy ER that's saying something."

12:15 PM · 21 Mar 17

Keep that in mind as you examine the secret ISR study, and you'll see that the Pentagon's drone program uses data analytics in almost precisely the same way IBM encourages corporations to use it to track customers. The only significant difference comes at the very end of the drone process, when the customer is killed.

Summary

- Every other industry has had BAD INSIDERS (Ford, Toyota, VW)
- Other industries have had MISALIGNED EXECUTIVE COMPENSATION (Ford, VW)
- Other industries have successfully dealt with HACKERS & ZERODAY attacks (Tylenol)

- Software isn't a special flower – it's time for us to treat Software like a mature industry.

Recommendations

- **REVOKE EULAs**
- **Pass SOFTWARE SAFETY laws**
- **Hold vendors accountable for shoddy software and pass minimum or mandatory safety standards.**
- **What we CAN do is make it harder for criminals to steal by building better defenses; making companies and management more liable for breaches; and demanding safer software.**

Contact Information

Raj Goel, CISSP

Chief Technology Officer

Brainlink International, Inc.

C: 917-685-7731

raj@brainlink.com

www.RajGoel.com

www.linkedin.com/in/rajgoel

@rajgoel_ny

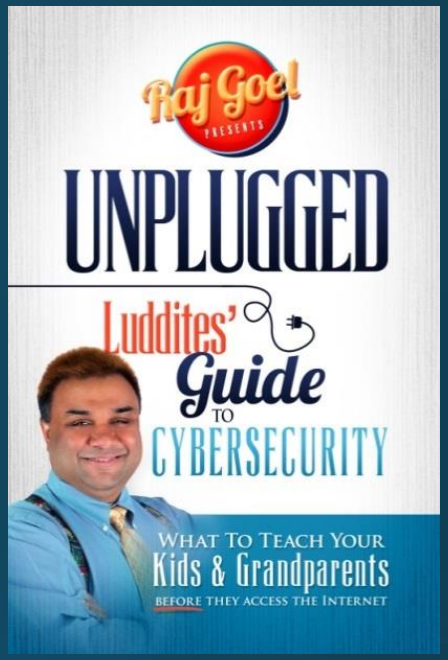
Author of

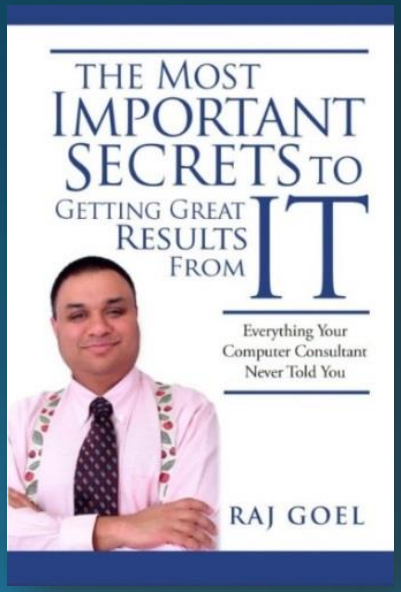
UNPLUGGED Luddites Guide To Cybersecurity

http://www.amazon.com/UNPLUGGED-Luddites-Guide-CyberSecurity-Grandparents/dp/0984424830/

The Most Important Secrets To Getting Great Results From IT

http://www.amazon.com/gp/product/0984424814





Questions?


OSLO
"We have time for just one long-winded, self-indulgent question that relates to nothing we've been talking about."