RiskBased SECURITY

Cyber, Cyber, Cyber..

Jake Kouns

Chief Information Security Officer (CISO)

Risk Based Security

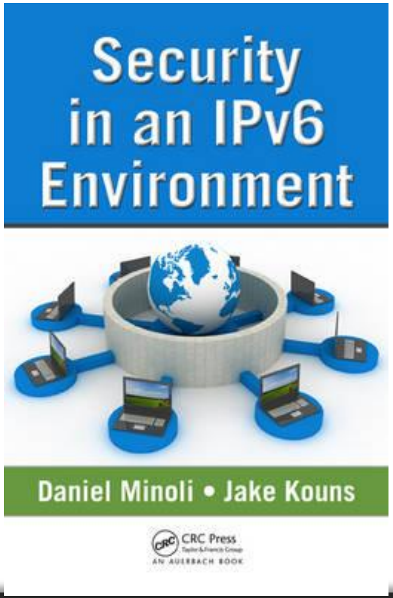
jake@riskbasedsecurity.com

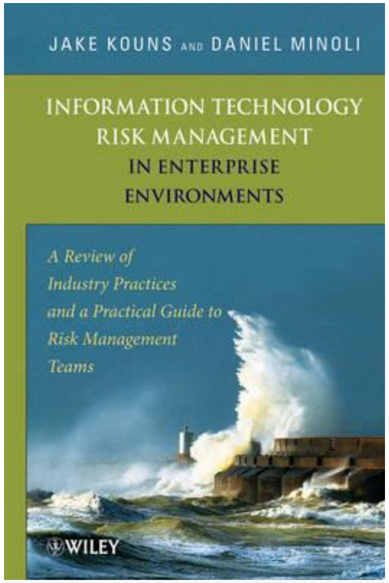
@jkouns

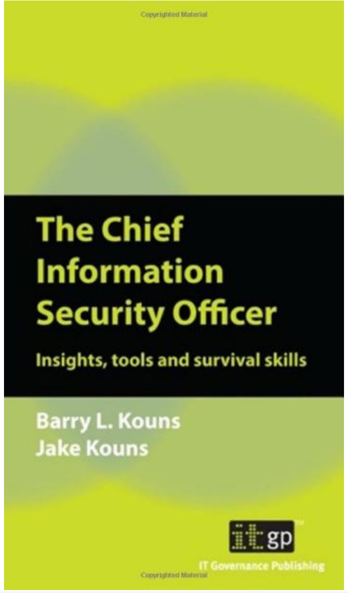
December 13, 2017

Why Should You Listen?

- CISO / Risk Based Security
- OSVDB / DataLossDB
- Founder of RVAsec conference
  - Yearly Conference in June hosted at VCU (June 7-8, 2018)
- James Madison University – MBA Information Security
- Spoke at Black Hat, DEF CON, RSA, FIRST, and many more!
- Spoke at DHS & Pentagon about Cyber Insurance




JAKE KOUNS AND DANIEL MINOLI
INFORMATION TECHNOLOGY RISK MANAGEMENT IN ENTERPRISE ENVIRONMENTS
A Review of Industry Practices and a Practical Guide to Risk Management Teams
WILEY


The Chief Information Security Officer
Insights, tools and survival skills
Barry L. Kouns
Jake Kouns
itgp
IT Governance Publishing

April 2010 Issue of SCMagazine

Are You Tired Of Hearing About Cyber Yet?

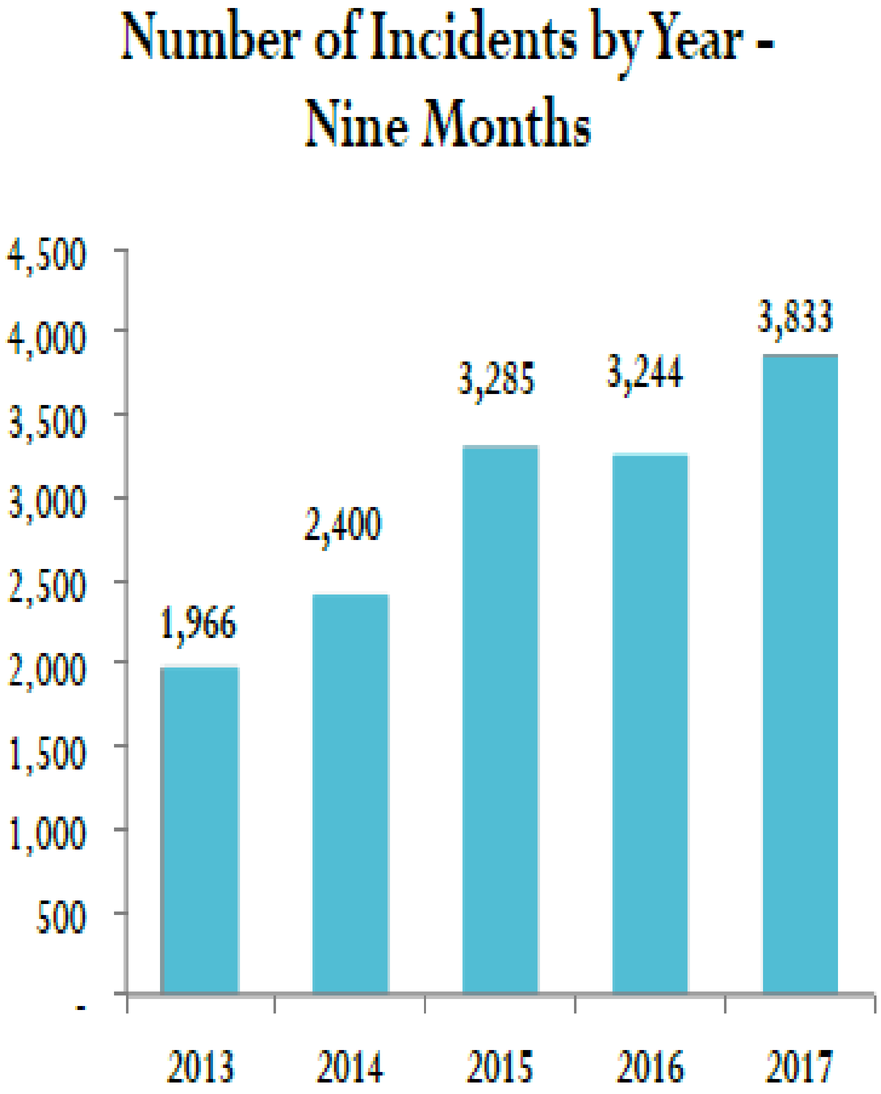
Cyber,

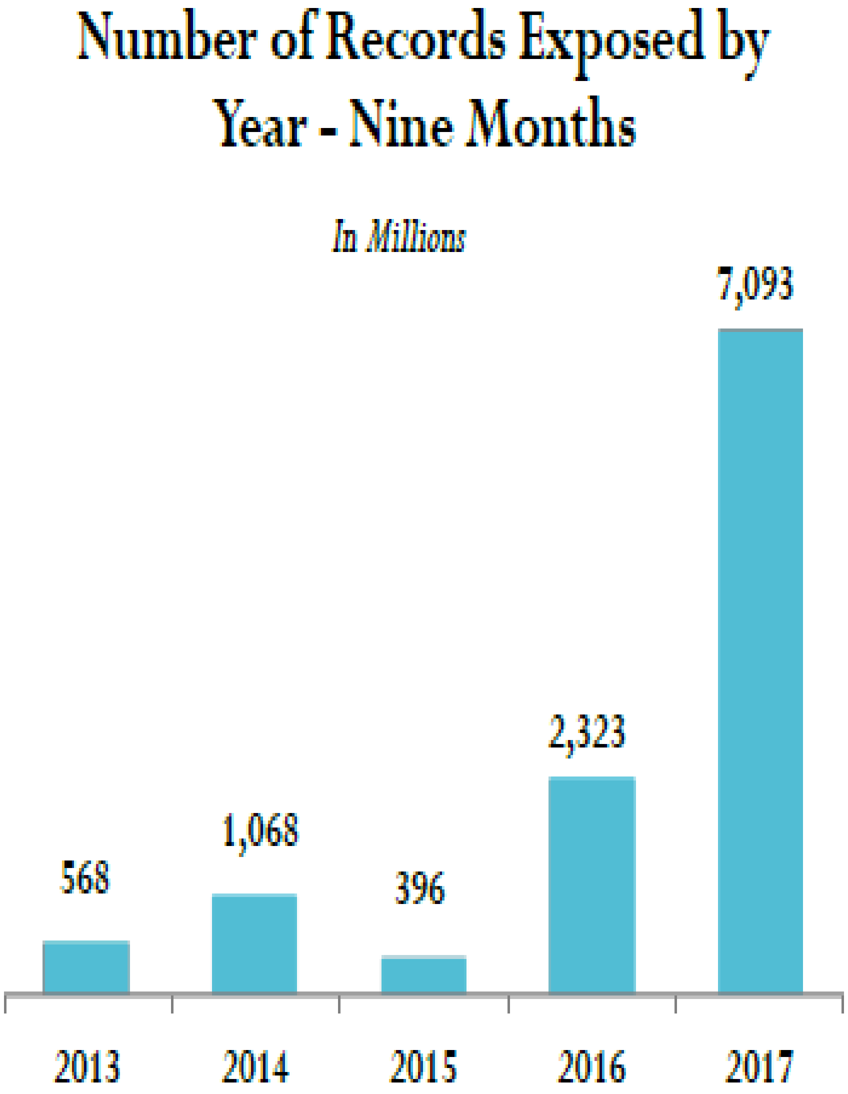
Cyber

Cyber……

cyber

Looking Back At The Last Five Years

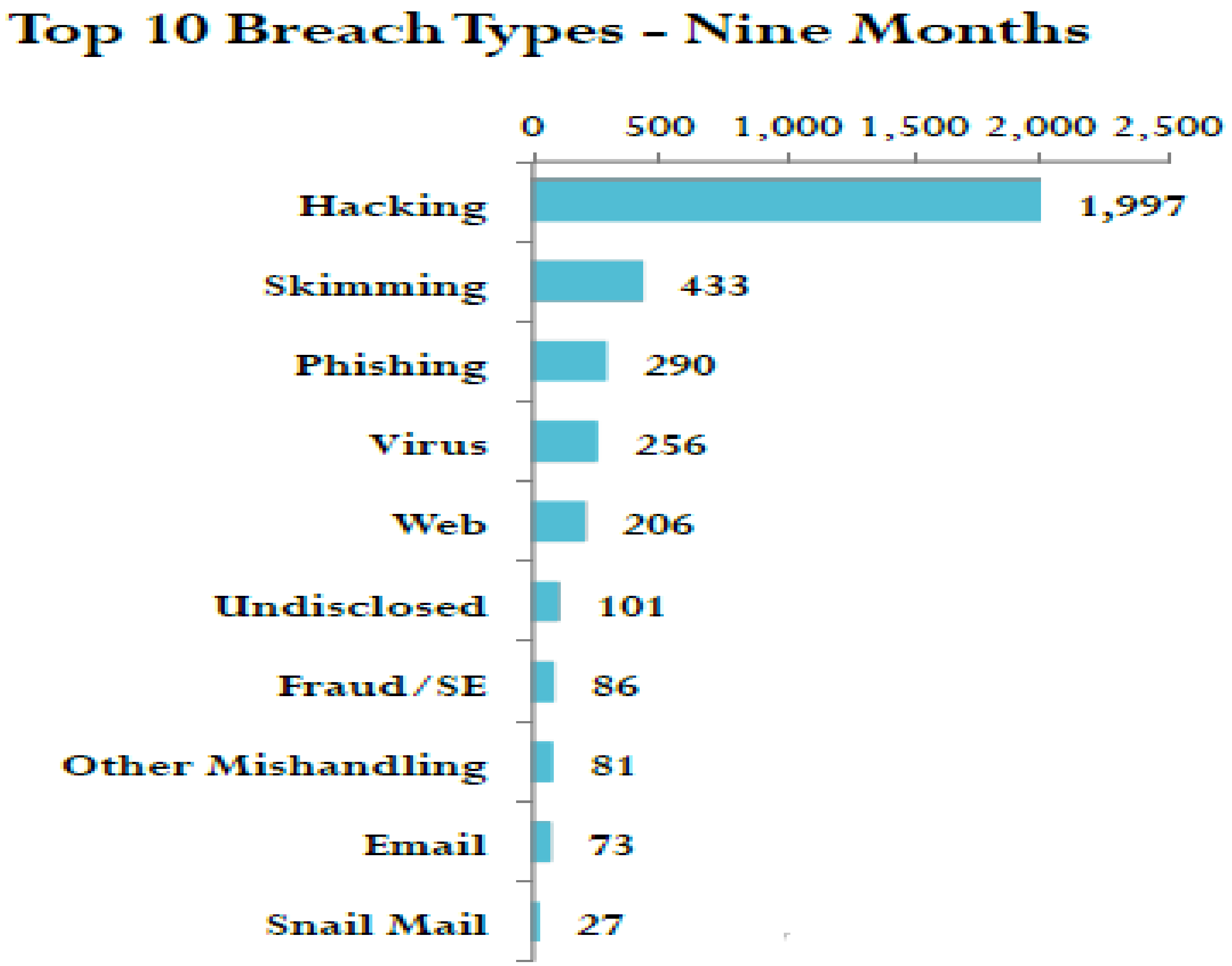




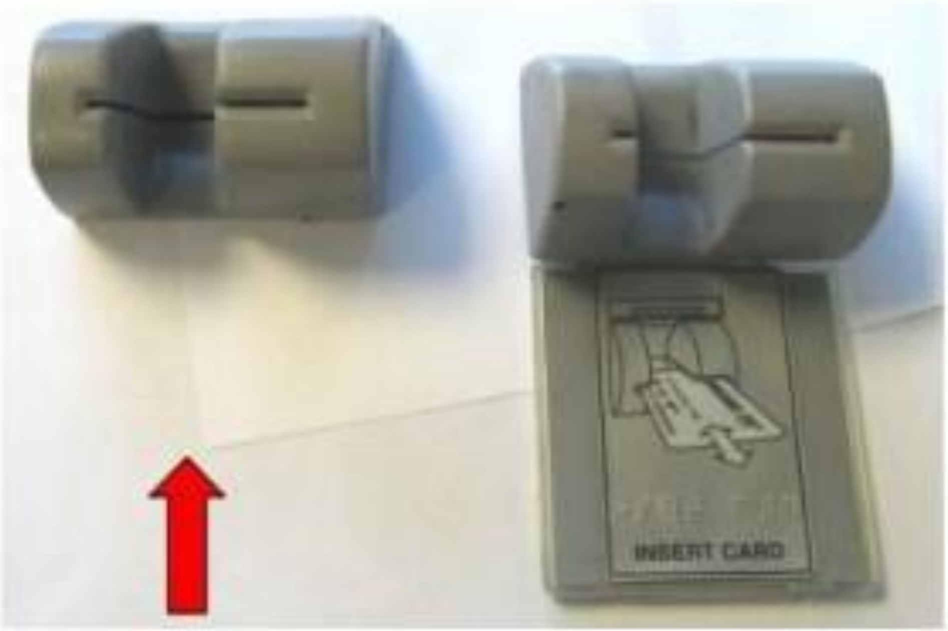
2017 YTD Data Breaches

Statistics

2017 YTD - Breach Types

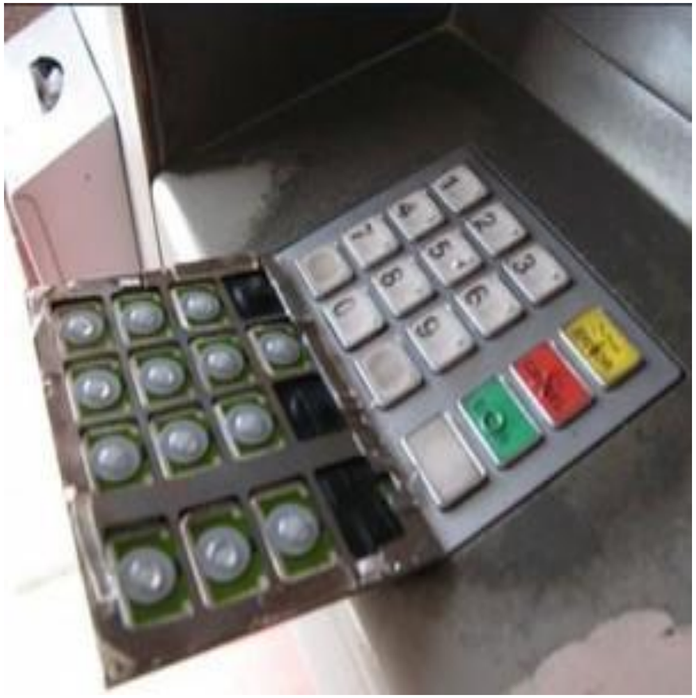


Skimmers

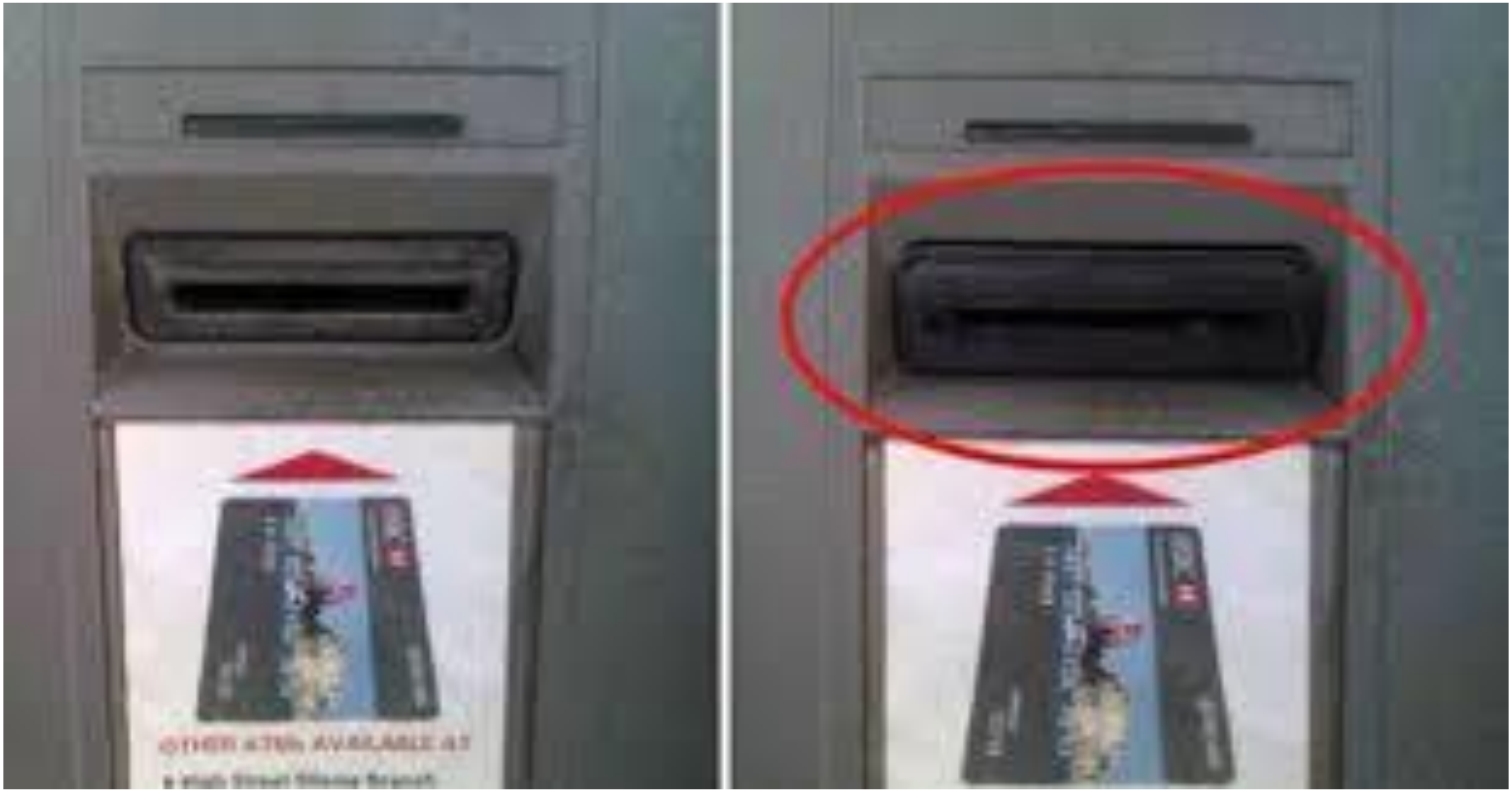


The real card reader slot.

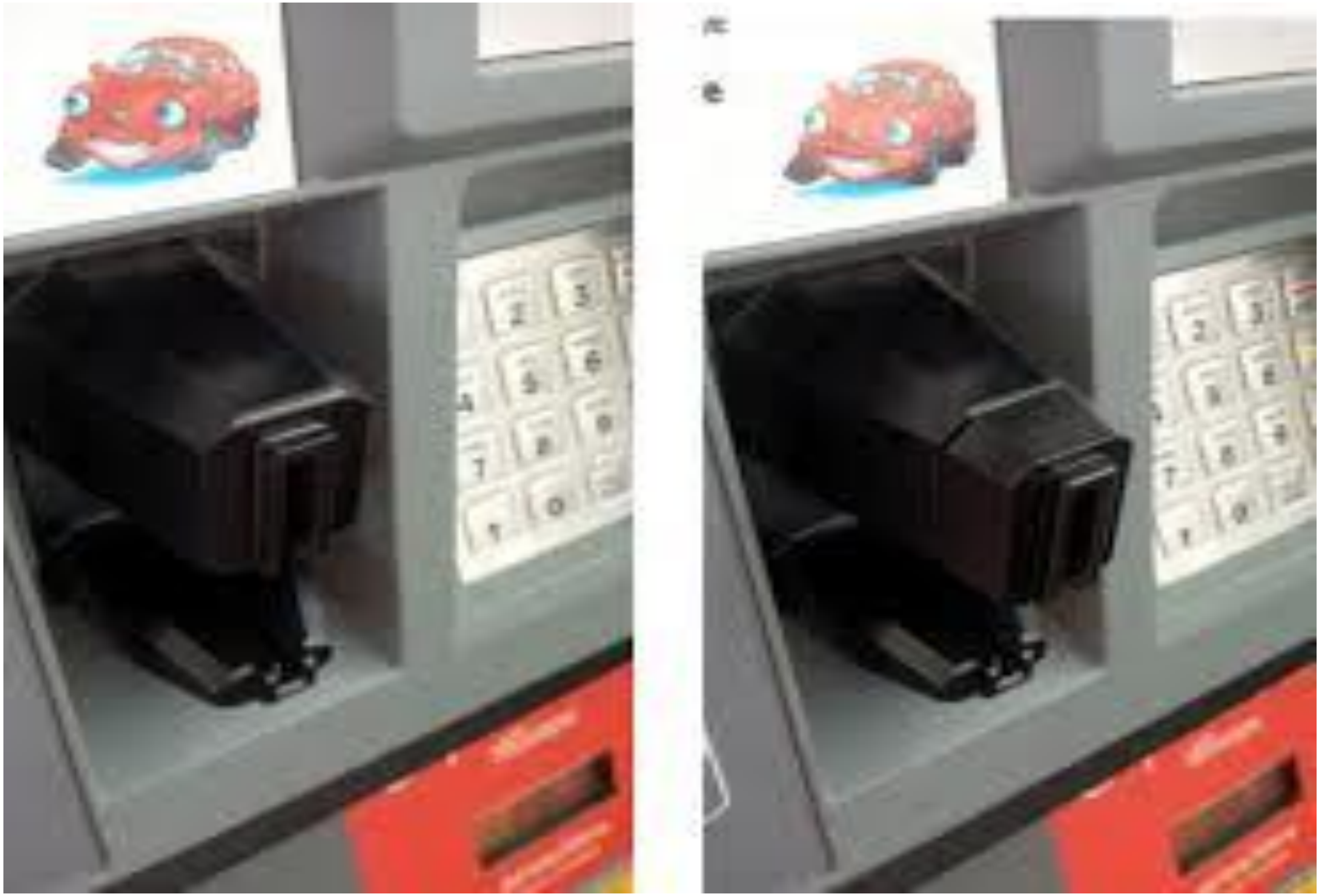
The capture device



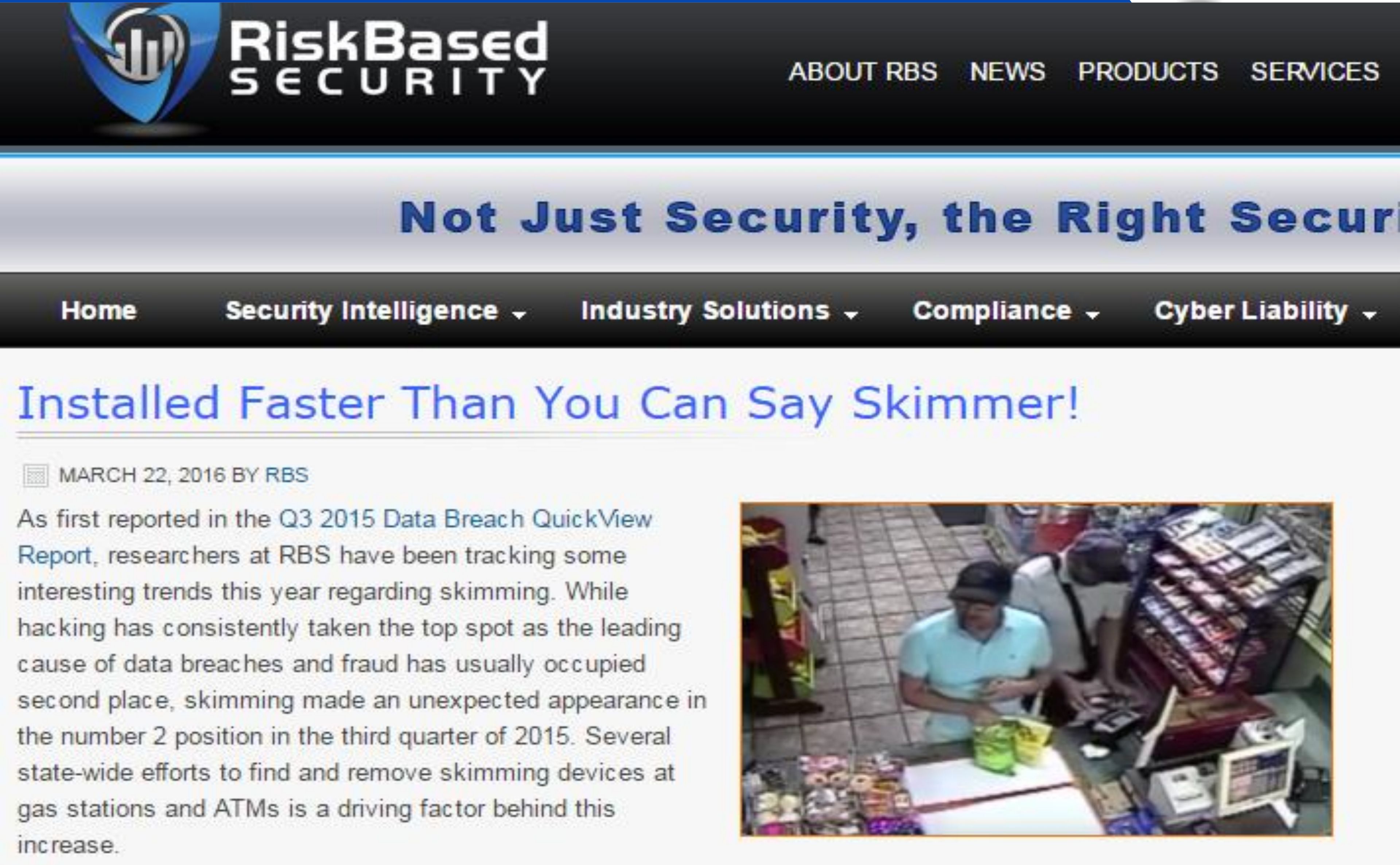
Skimmers



Skimmers



2017 YTD - Skimming



RiskBased SECURITY

ABOUT RBS NEWS PRODUCTS SERVICES

Not Just Security, the Right Securi

Home Security Intelligence Industry Solutions Compliance Cyber Liability

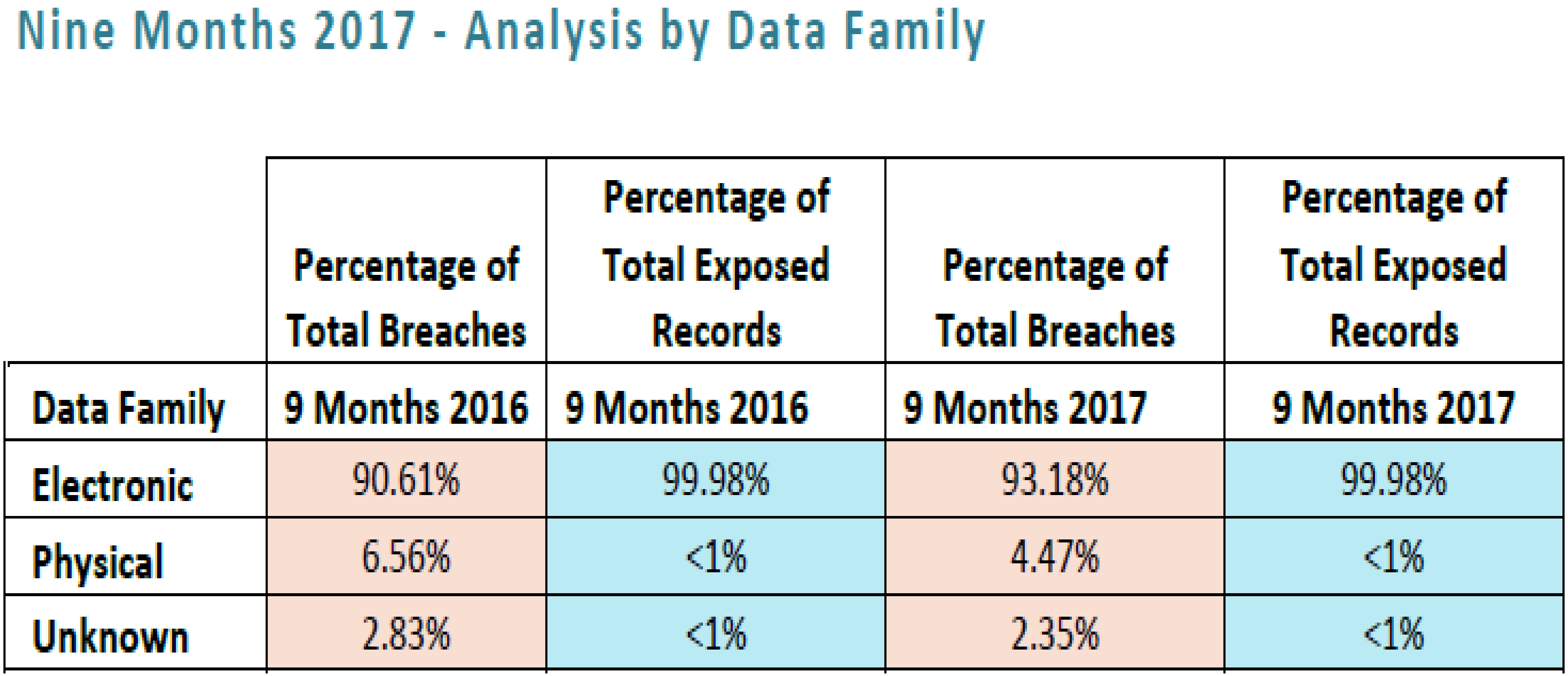
Installed Faster Than You Can Say Skimmer!

MARCH 22, 2016 BY RBS

As first reported in the Q3 2015 Data Breach QuickView Report, researchers at RBS have been tracking some interesting trends this year regarding skimming. While hacking has consistently taken the top spot as the leading cause of data breaches and fraud has usually occupied second place, skimming made an unexpected appearance in the number 2 position in the third quarter of 2015. Several state-wide efforts to find and remove skimming devices at gas stations and ATMs is a driving factor behind this increase.

Watch The Installation!

2017 YTD Analysis – Data Family



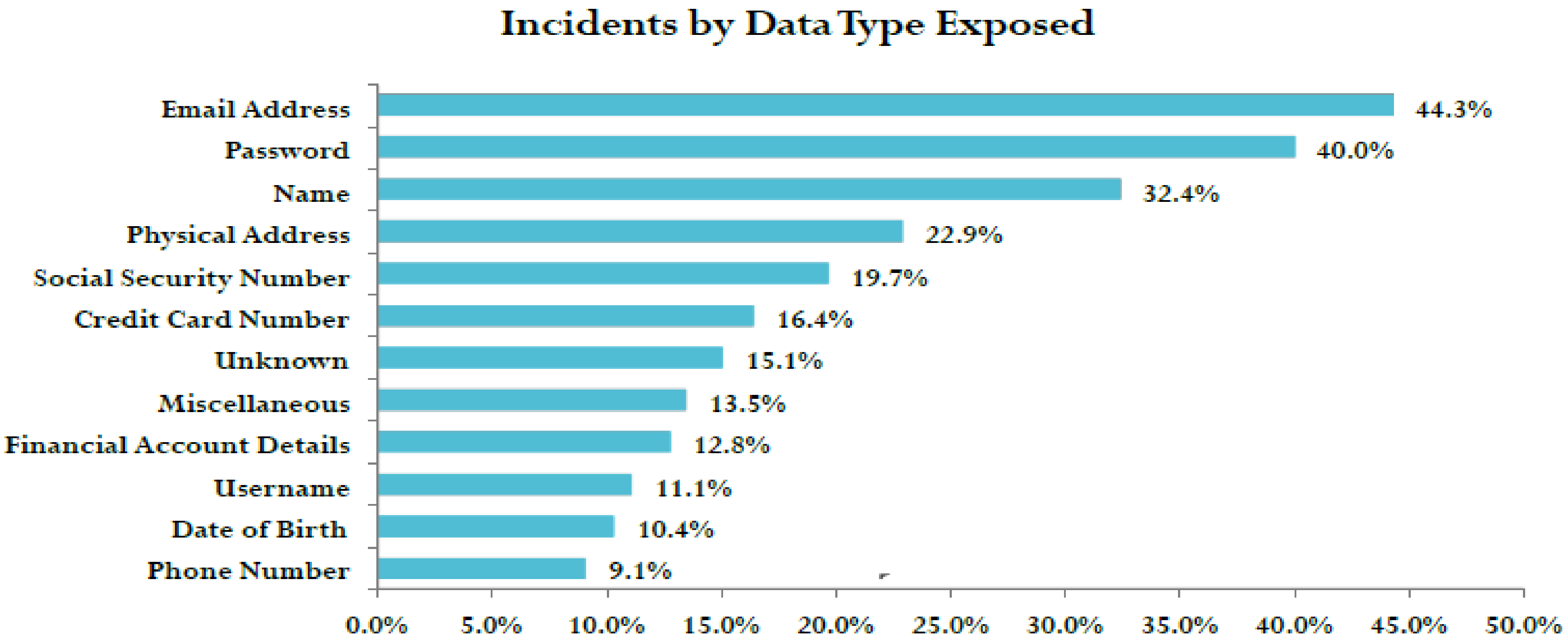
Nine Months 2017 - Analysis by Data Family

	Percentage of Total Breaches	Percentage of Total Exposed Records	Percentage of Total Breaches	Percentage of Total Exposed Records
Data Family	**9 Months 2016**	**9 Months 2016**	**9 Months 2017**	**9 Months 2017**
Electronic	90.61%	99.98%	93.18%	99.98%
Physical	6.56%	<1%	4.47%	<1%
Unknown	2.83%	<1%	2.35%	<1%

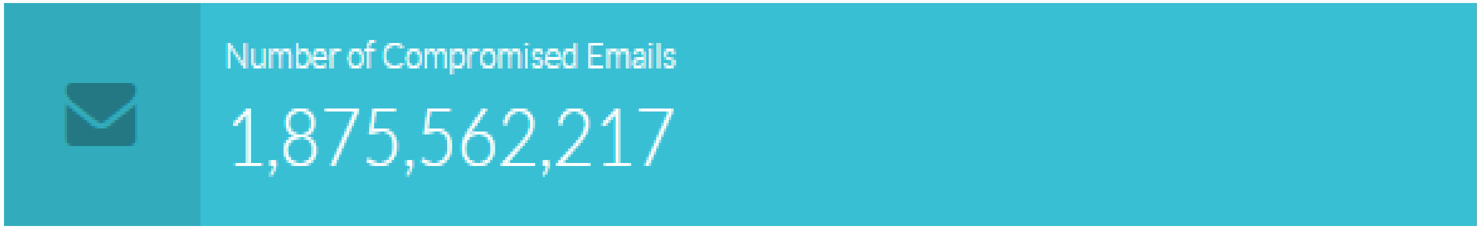
- 93.18% of all incidents involved electronic data
- Nearly 100% of the exposed records were in electronic form.
- This is a constant theme year over year.

2017 YTD – Data Types

Nine Months 2017 - Analysis by Data Type



The percentage of breaches impacting names dropped 8.2% from the midyear point. Similarly, the number of breaches impacting physical addresses and Social Security numbers dropped 7.5% and 6.4% respectively since the midyear point. Once again, access credentials in the form of email addresses and passwords are the top two most compromised data types.



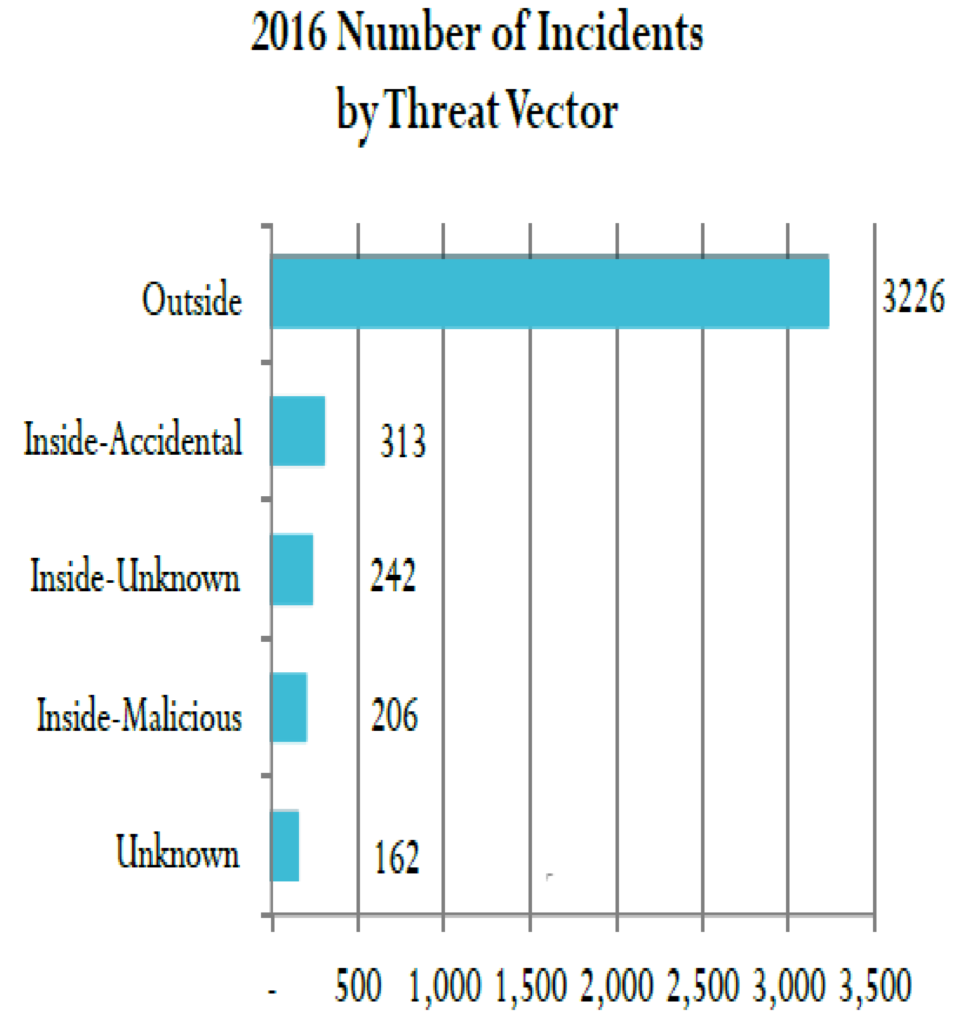
Number of Compromised Emails

1,875,562,217

Continuing trend of targeting user names, e-mail addresses, and passwords.

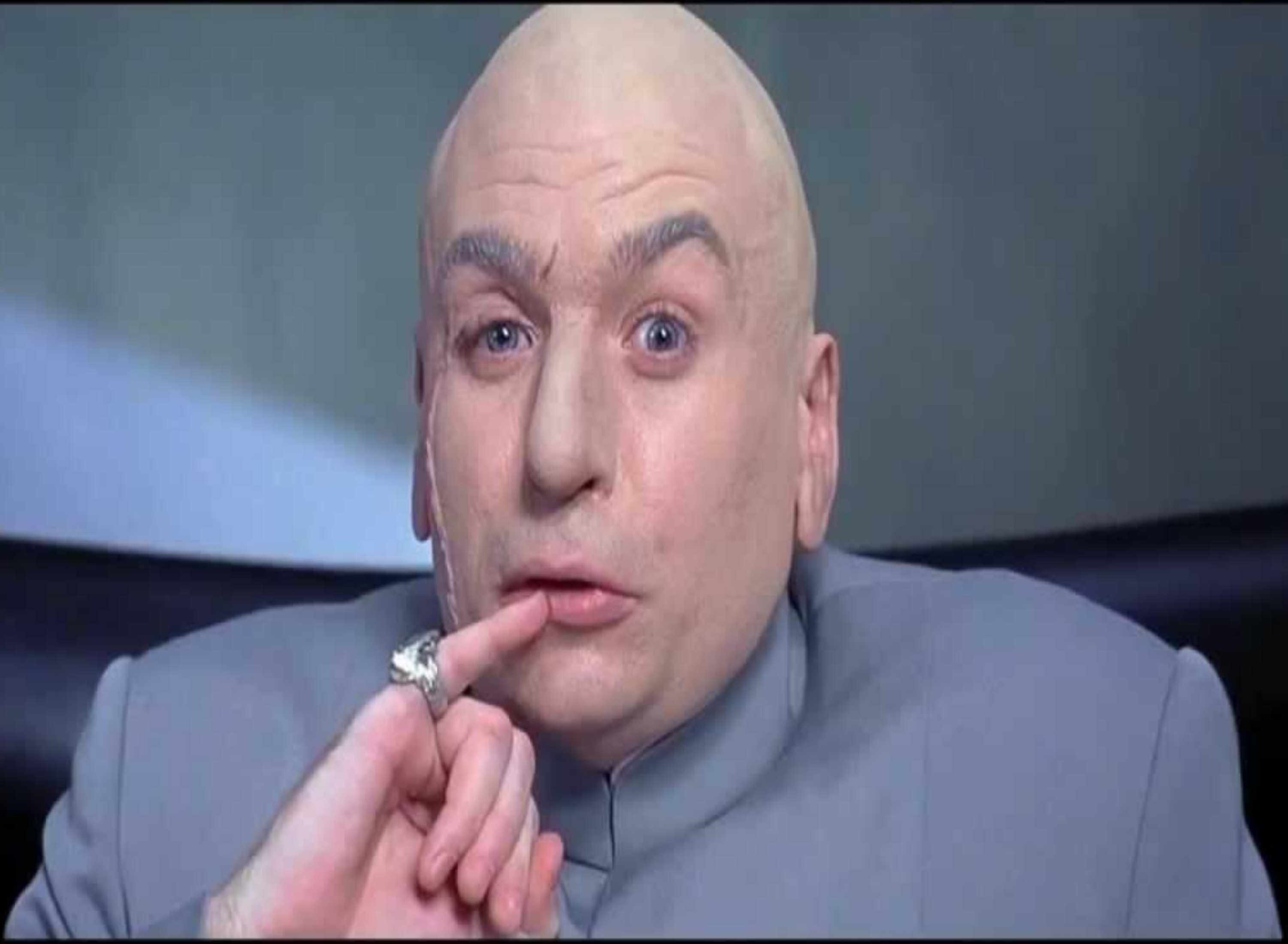
2017 YTD – Threat Vector

2016 Data Breach Analysis by Threat Vector



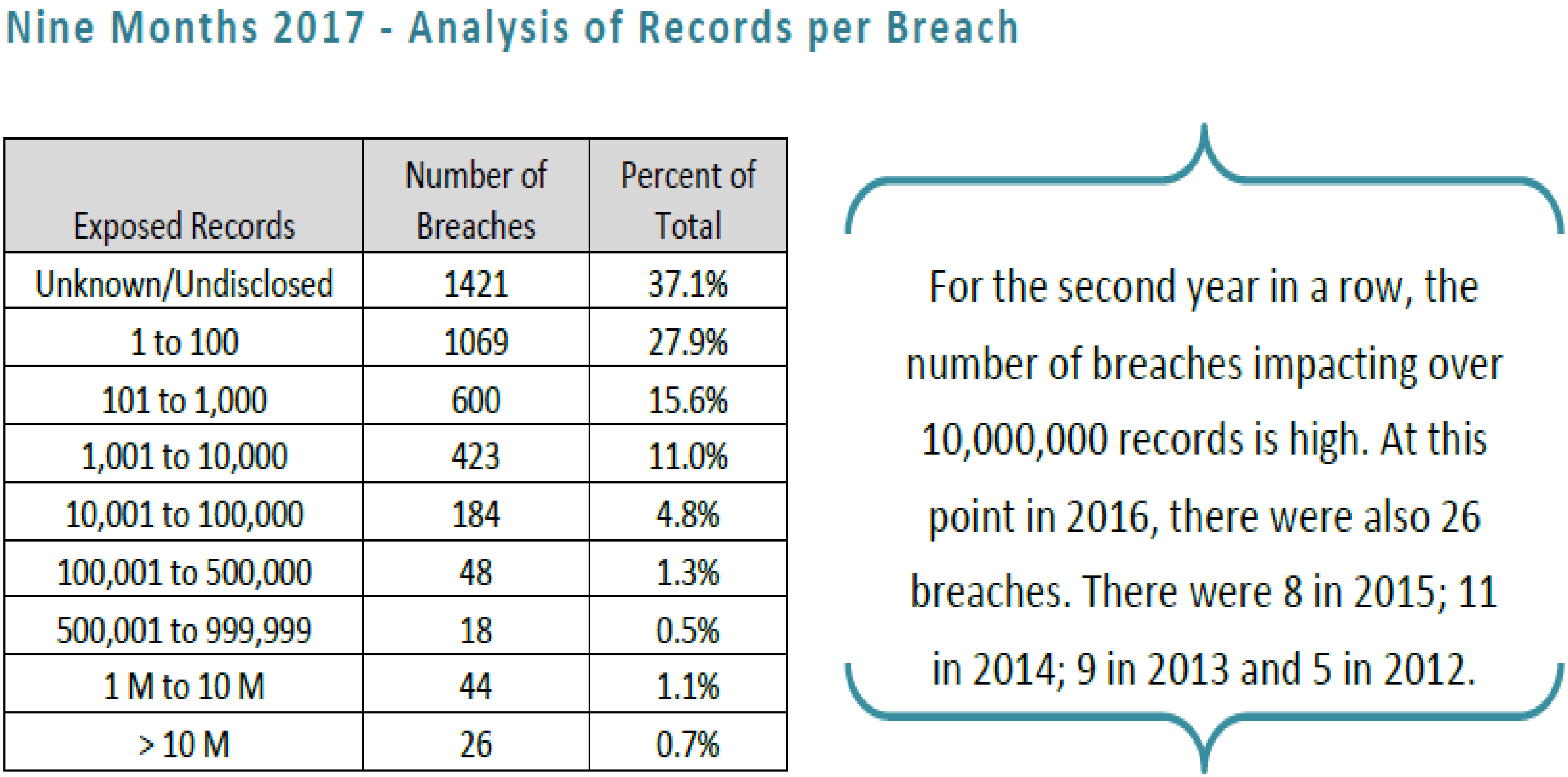
Only 18.3% of incidents were the result of insider activity

70 breaches exposed at least



ONE MILLION RECORDS

2016 Analysis Of Records Per Breach



Nine Months 2017 - Analysis of Records per Breach

Exposed Records	Number of Breaches	Percent of Total
Unknown/Undisclosed	1421	37.1%
1 to 100	1069	27.9%
101 to 1,000	600	15.6%
1,001 to 10,000	423	11.0%
10,001 to 100,000	184	4.8%
100,001 to 500,000	48	1.3%
500,001 to 999,999	18	0.5%
1 M to 10 M	44	1.1%
> 10 M	26	0.7%

For the second year in a row, the number of breaches impacting over 10,000,000 records is high. At this point in 2016, there were also 26 breaches. There were 8 in 2015; 11 in 2014; 9 in 2013 and 5 in 2012.

43.5% of incidents exposed between 1 and 1000 records (50.4% in 2016)

Data Breaches All Time

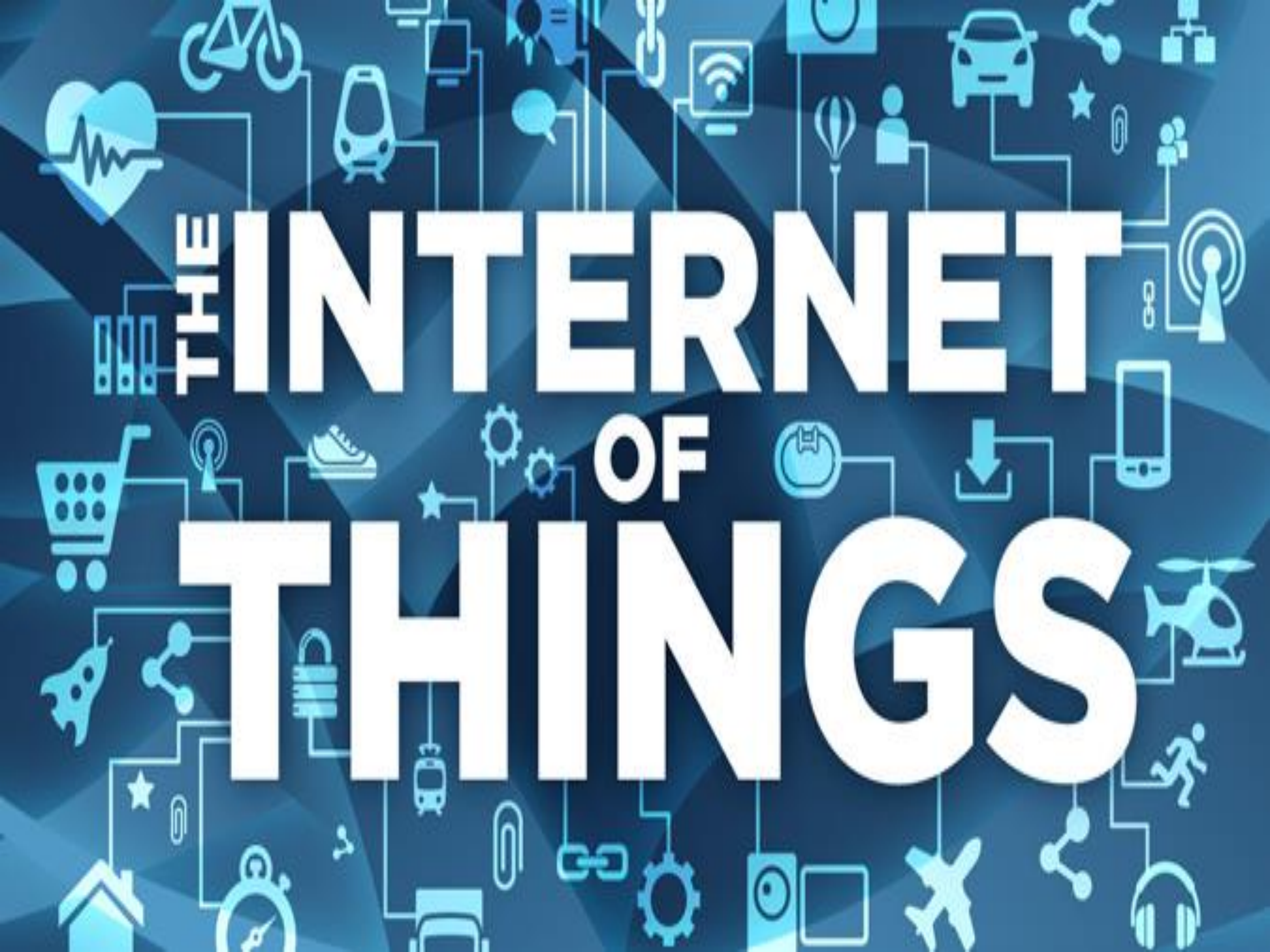
28,000+

reported incidents

19+ billion

exposed records

What’s The New Problem?


THE
INTERNET
OF
THINGS

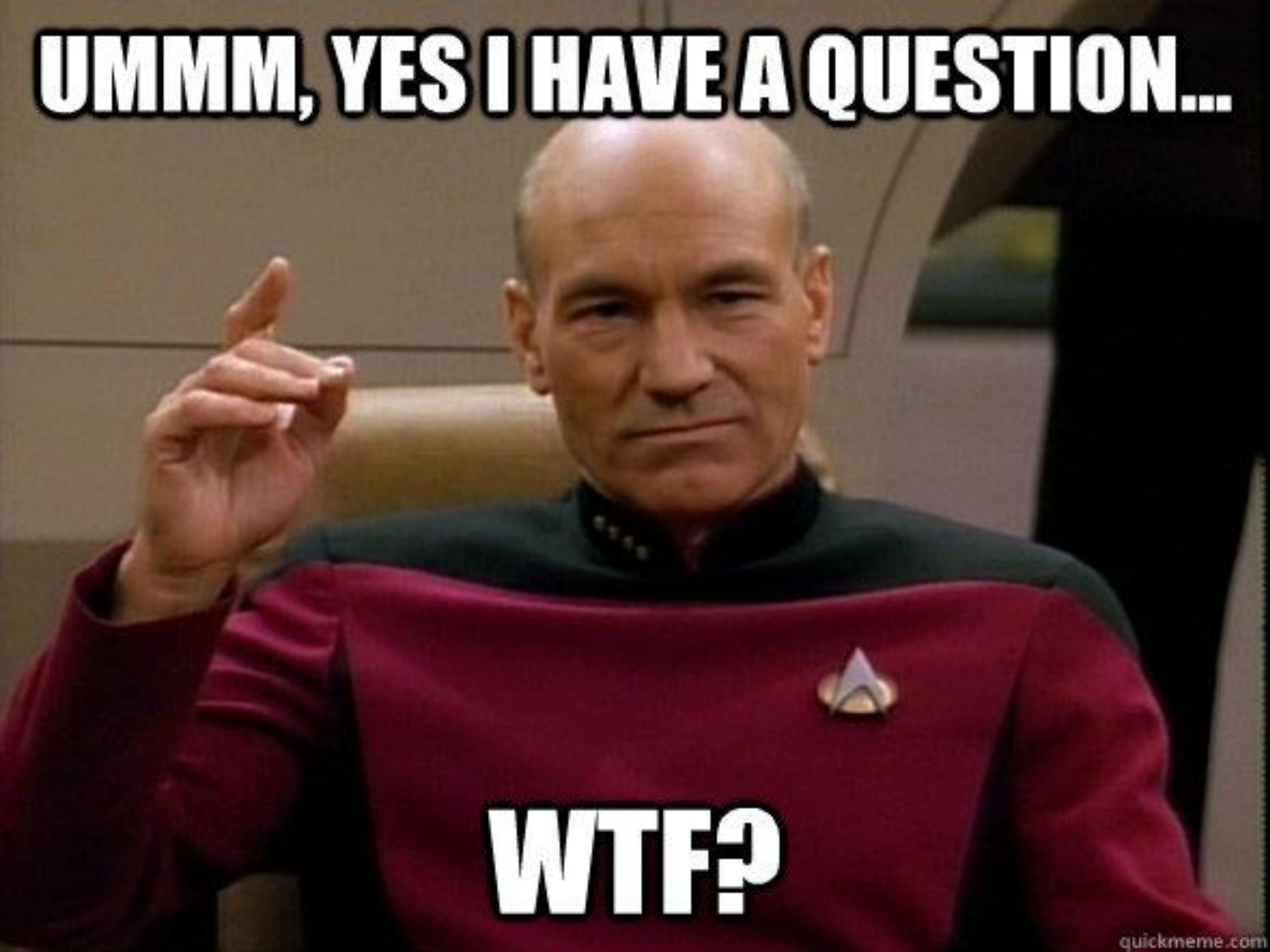
Internet of Things – Definition (Techopedia.com)

“The Internet of Things (IoT) is a computing concept that describes a future where everyday physical objects will be connected to the Internet and be able to identify themselves to other devices. The term is closely identified with RFID as the method of communication, although it also may include other sensor technologies, wireless technologies or QR codes.

The IoT is significant because an object that can represent itself digitally becomes something greater than the object by itself. No longer does the object relate just to you, but is now connected to surrounding objects and database data. When many objects act in unison, they are known as having "ambient intelligence.“”

”The Internet of Things is a difficult concept to define precisely.”

- Techopedia.com


UMMM, YES I HAVE A QUESTION...
WTF?
quickmeme.com

Internet of Things – Definition

1. Needs to be networked / connected
2. Some capability of sensing and decision making without human interaction/control

Many products have the word ”Smart” in their name or to describe its function

Internet of Things – Examples (Everyday Life)

Internet of Things – Examples
(Just because we can...)

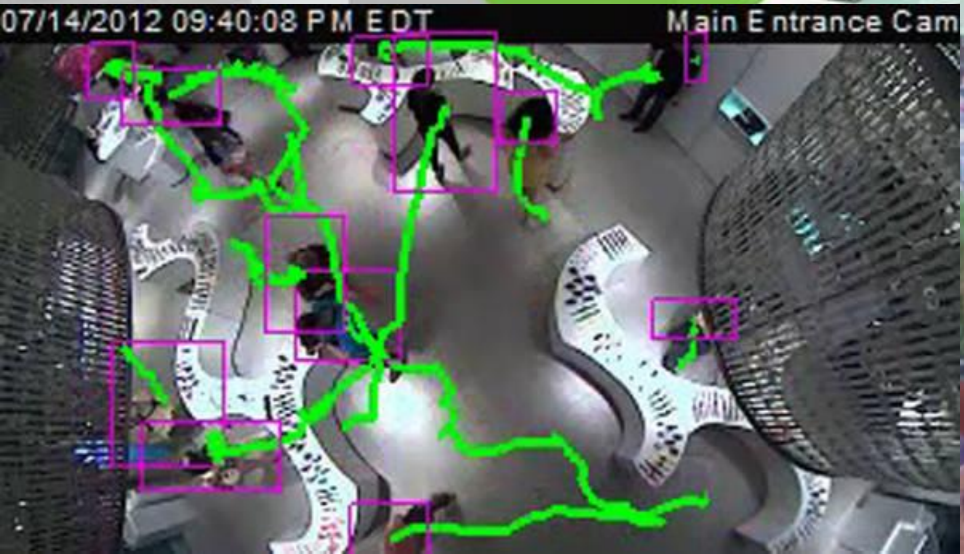
Internet of Things - Definition

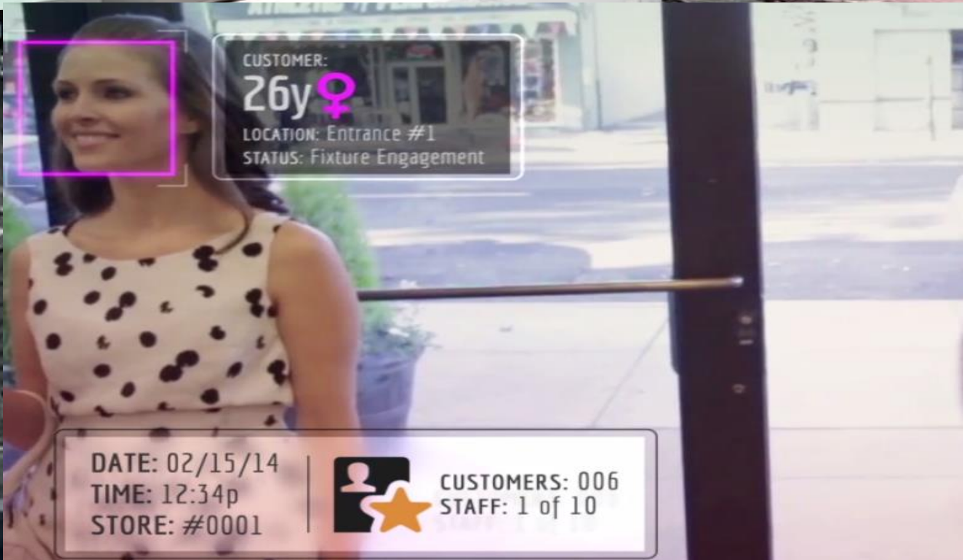
Looking past all the hype, IoT does not just pertain to consumers.

From a business perspective, it can:

- Help to cut costs
- Save time
- Improve productivity and efficiency.

Internet of Things – Examples (Retail)




CUSTOMER:
26y ♀
LOCATION: Entrance #1
STATUS: Fixture Engagement

DATE: 02/15/14
TIME: 12:34p
STORE: #0001

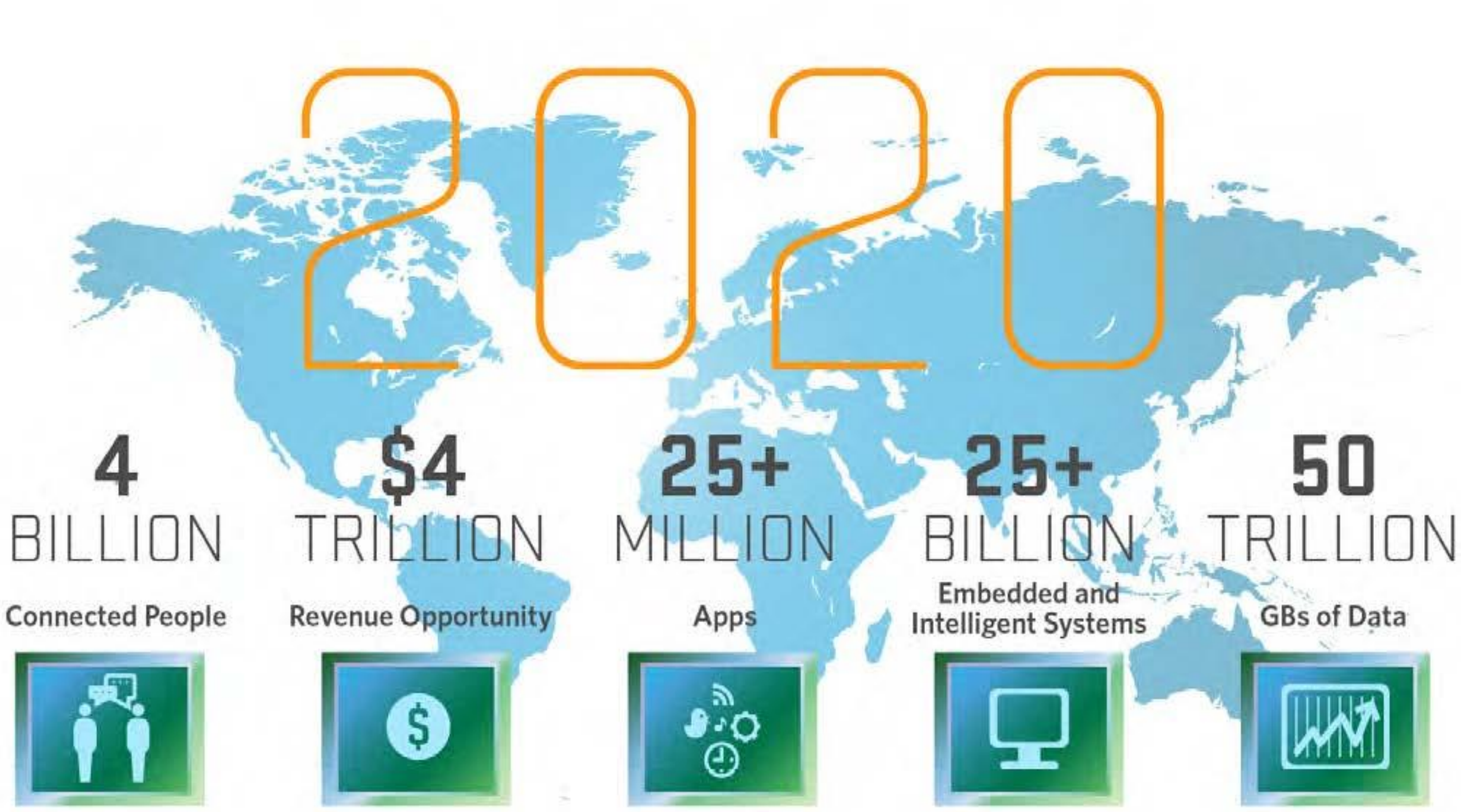
CUSTOMERS: 006
STAFF: 1 of 10

Internet of Things – Examples (Environmental)

Internet of Things – Examples (Your Home & Company Network)

Internet of Things – Examples (Your Home & Company Network)

Internet of Things – Why Should You Care?



2020

4 BILLION Connected People

$4 TRILLION Revenue Opportunity

25+ MILLION Apps

25+ BILLION Embedded and Intelligent Systems

50 TRILLION GBs of Data

Source: Mario Morales, IDC

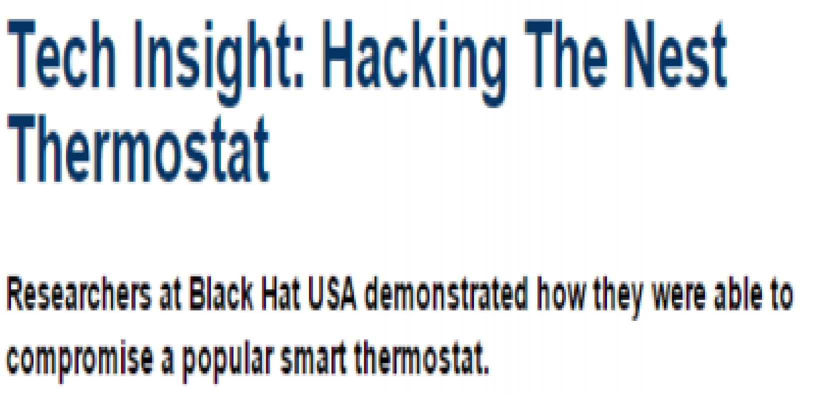
Internet of Things – How Is This Different?

BI/PD (Bodily Injury, Property Damage) – People can get hurt, and property can be damaged

Real world impact - no longer 1s and 0s

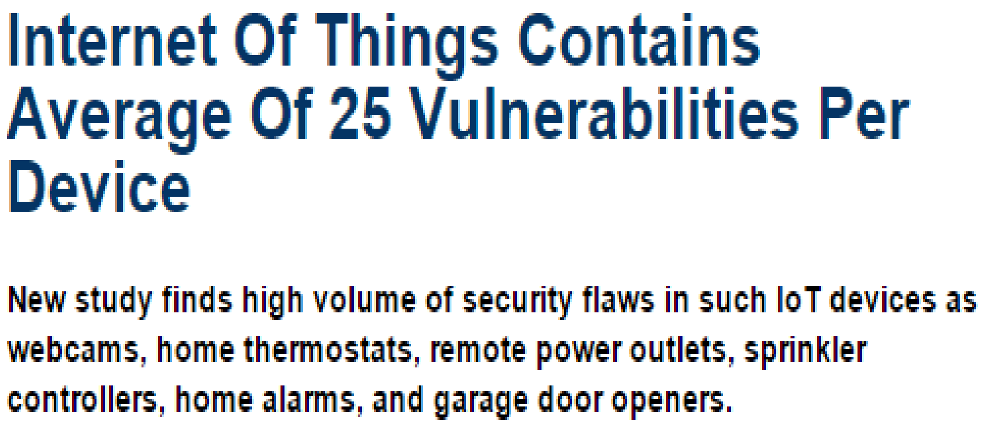
Internet of Things – Is There An Impact?

Internet of Things – IoT Vulns So Far?



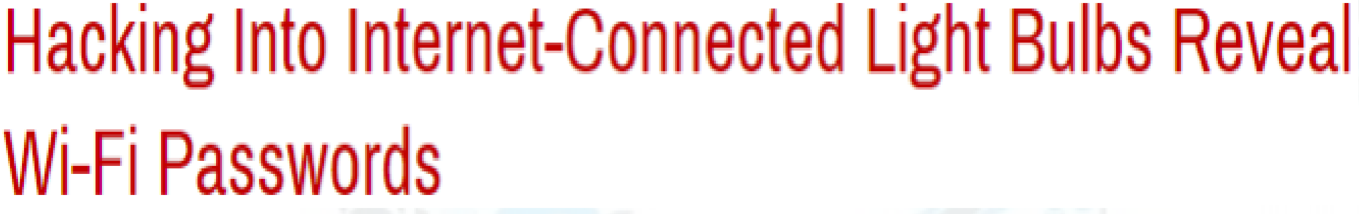
Tech Insight: Hacking The Nest Thermostat

Researchers at Black Hat USA demonstrated how they were able to compromise a popular smart thermostat.

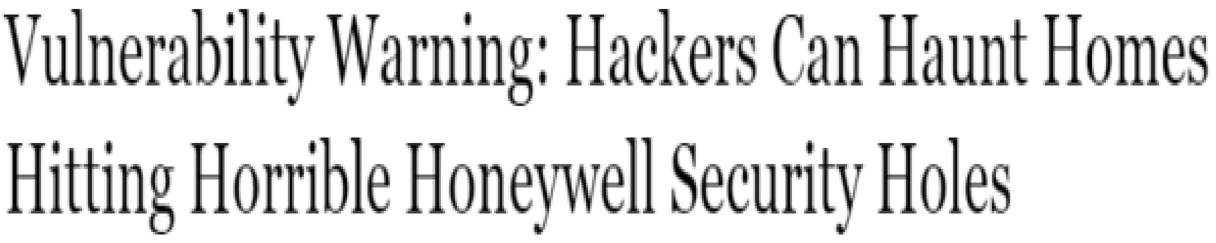


Internet Of Things Contains Average Of 25 Vulnerabilities Per Device

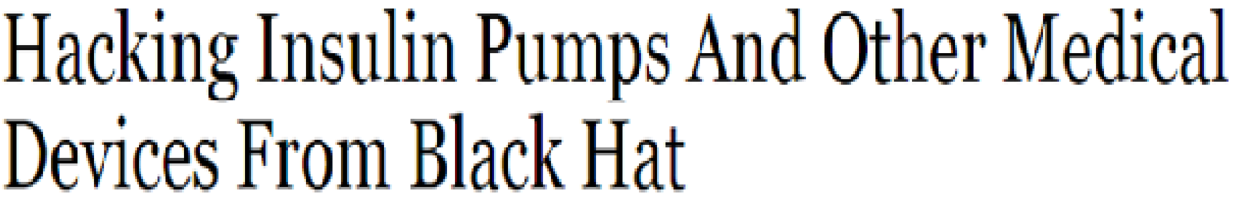
New study finds high volume of security flaws in such IoT devices as webcams, home thermostats, remote power outlets, sprinkler controllers, home alarms, and garage door openers.



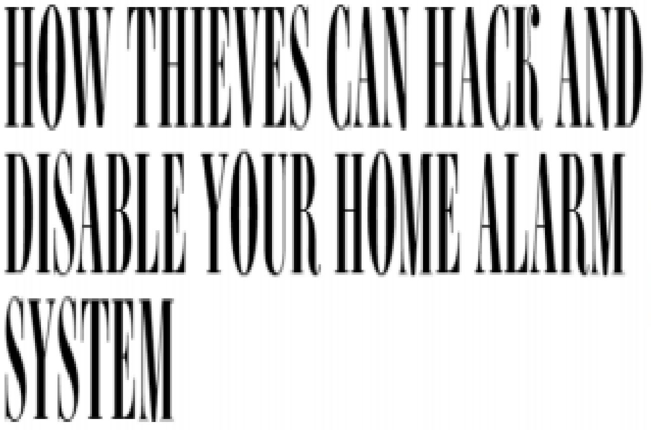
Hacking Into Internet-Connected Light Bulbs Reveal Wi-Fi Passwords



Vulnerability Warning: Hackers Can Haunt Homes Hitting Horrible Honeywell Security Holes

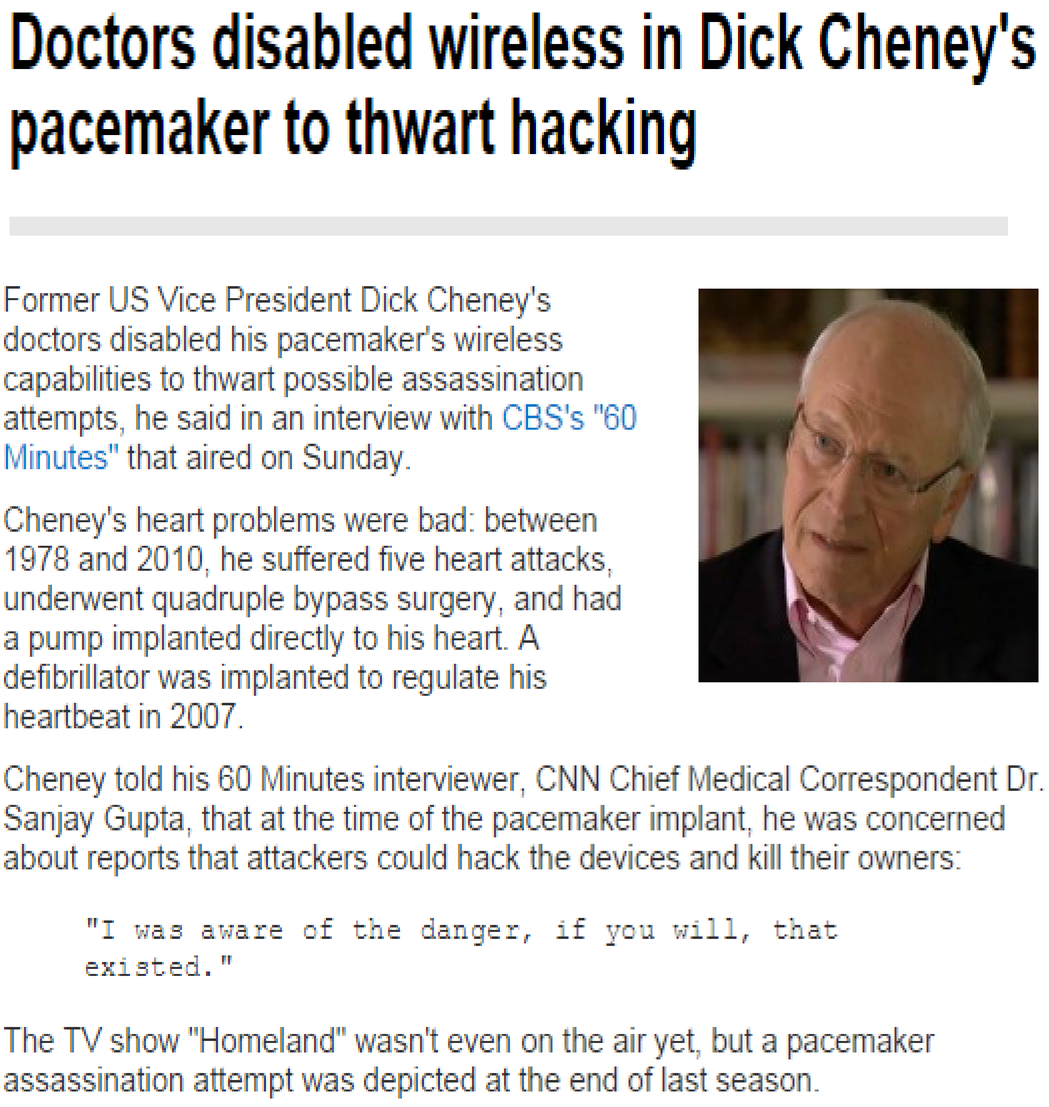


Hacking Insulin Pumps And Other Medical Devices From Black Hat



HOW THIEVES CAN HACK AND DISABLE YOUR HOME ALARM SYSTEM

Internet Of Things - Medical



Doctors disabled wireless in Dick Cheney's pacemaker to thwart hacking

Former US Vice President Dick Cheney's doctors disabled his pacemaker's wireless capabilities to thwart possible assassination attempts, he said in an interview with CBS's "60 Minutes" that aired on Sunday.

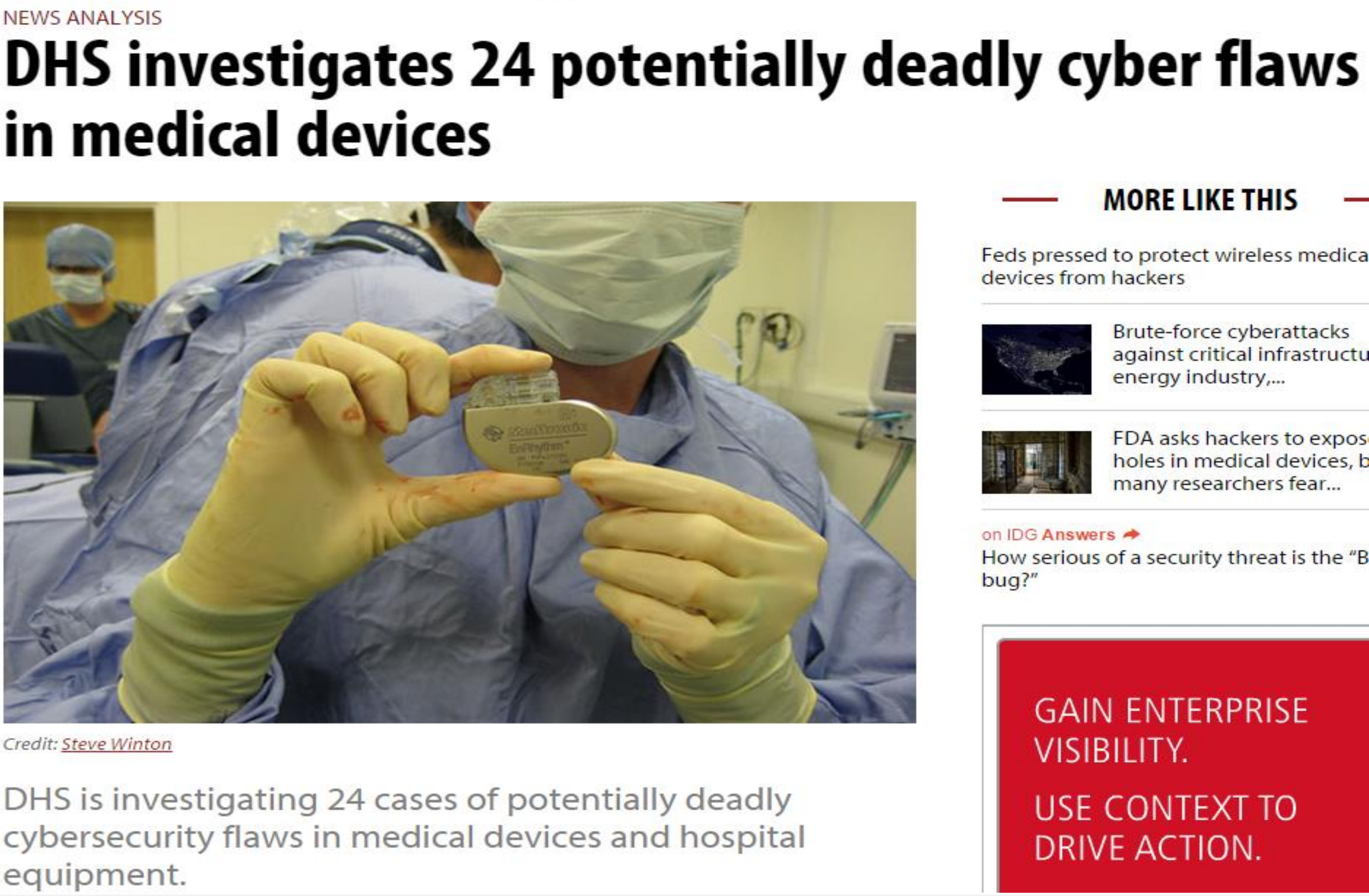
Cheney's heart problems were bad: between 1978 and 2010, he suffered five heart attacks, underwent quadruple bypass surgery, and had a pump implanted directly to his heart. A defibrillator was implanted to regulate his heartbeat in 2007.

Cheney told his 60 Minutes interviewer, CNN Chief Medical Correspondent Dr. Sanjay Gupta, that at the time of the pacemaker implant, he was concerned about reports that attackers could hack the devices and kill their owners:

> "I was aware of the danger, if you will, that existed."

The TV show "Homeland" wasn't even on the air yet, but a pacemaker assassination attempt was depicted at the end of last season.

Internet of Things – What's In The News?



NEWS ANALYSIS

DHS investigates 24 potentially deadly cyber flaws in medical devices

Credit: Steve Winton

DHS is investigating 24 cases of potentially deadly cybersecurity flaws in medical devices and hospital equipment.

MORE LIKE THIS

Feds pressed to protect wireless medica devices from hackers

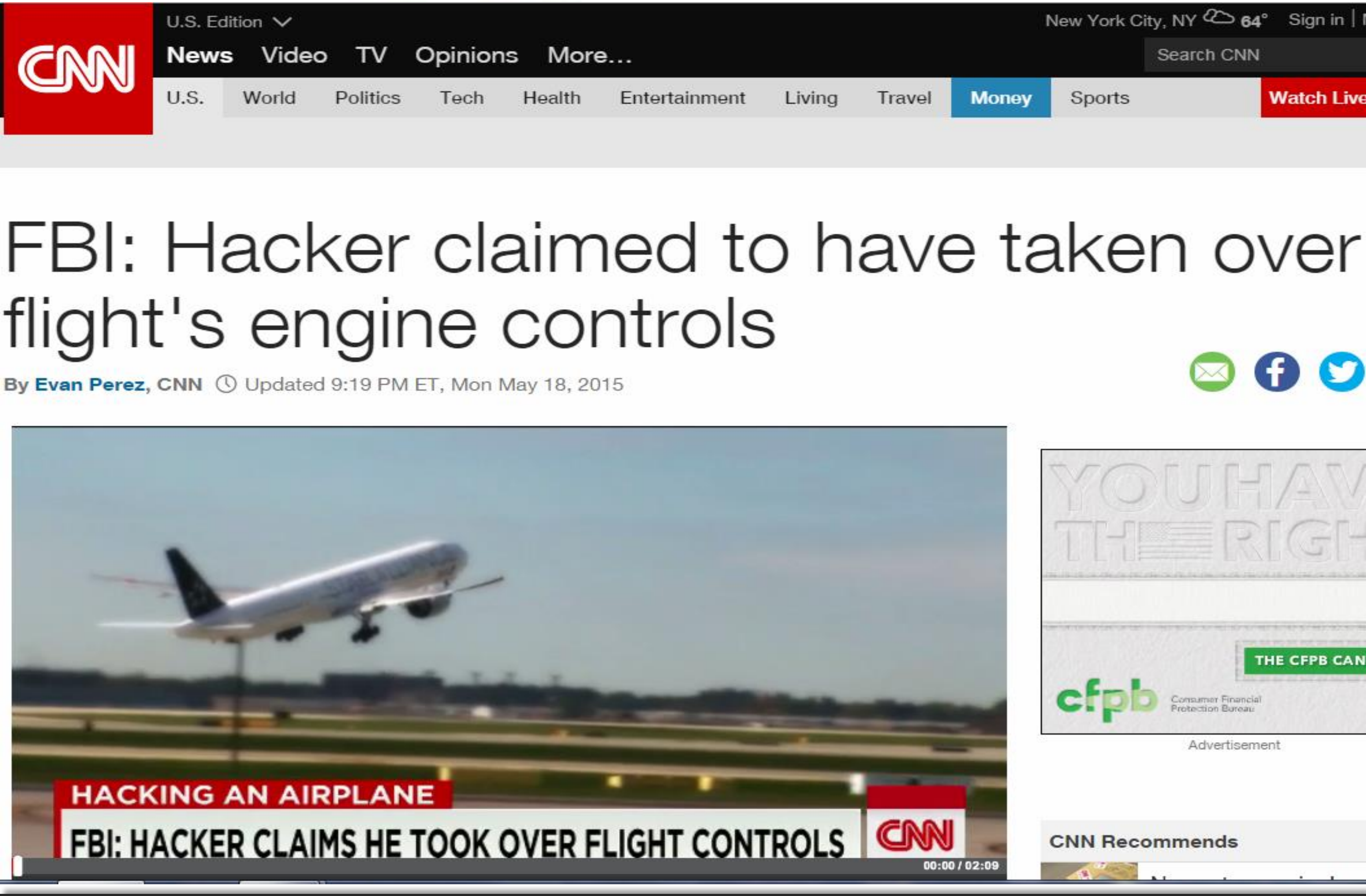
Brute-force cyberattacks against critical infrastructu energy industry,...

FDA asks hackers to expos holes in medical devices, b many researchers fear...

on IDG Answers

How serious of a security threat is the "B bug?"

Internet of Things – What's In The News?



FBI: Hacker claimed to have taken over flight's engine controls

By Evan Perez, CNN Updated 9:19 PM ET, Mon May 18, 2015

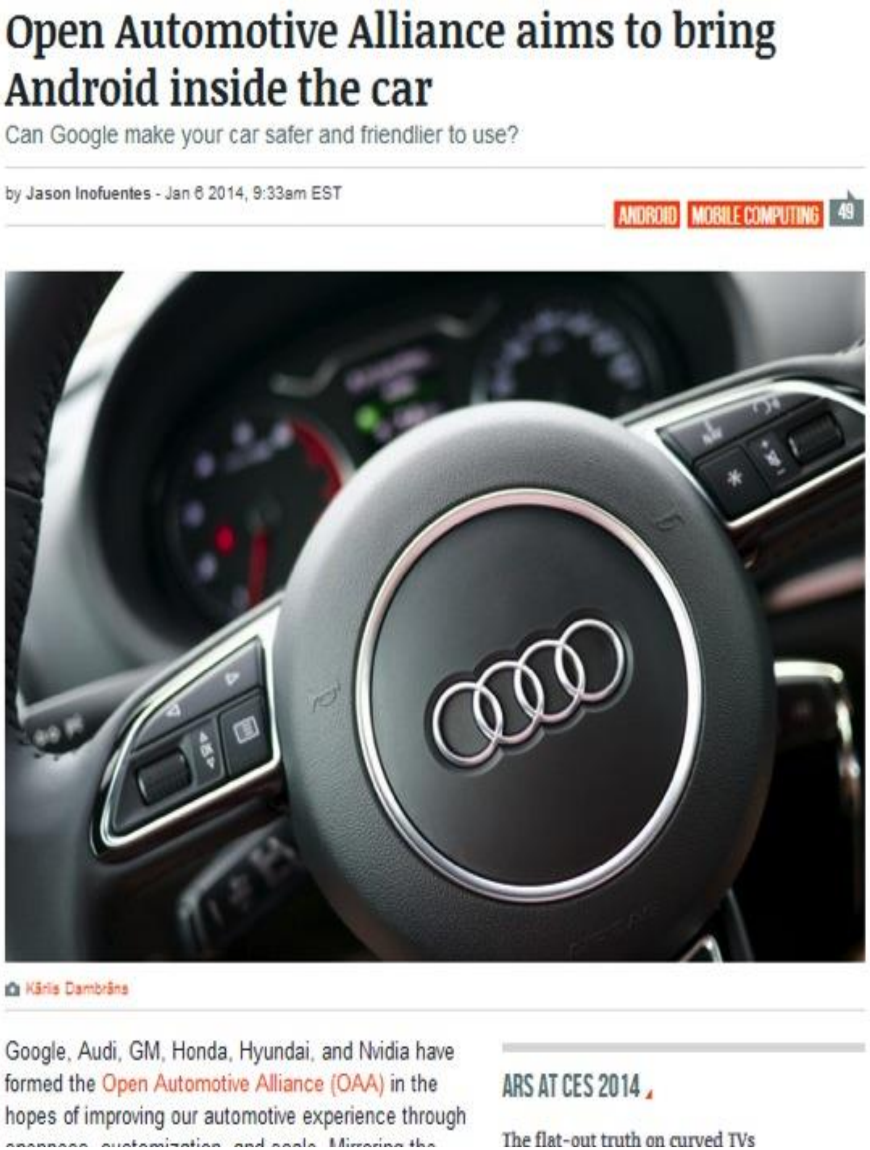
HACKING AN AIRPLANE

FBI: HACKER CLAIMS HE TOOK OVER FLIGHT CONTROLS

00:00 / 02:09

CNN Recommends

Internet Of Things - Cars



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

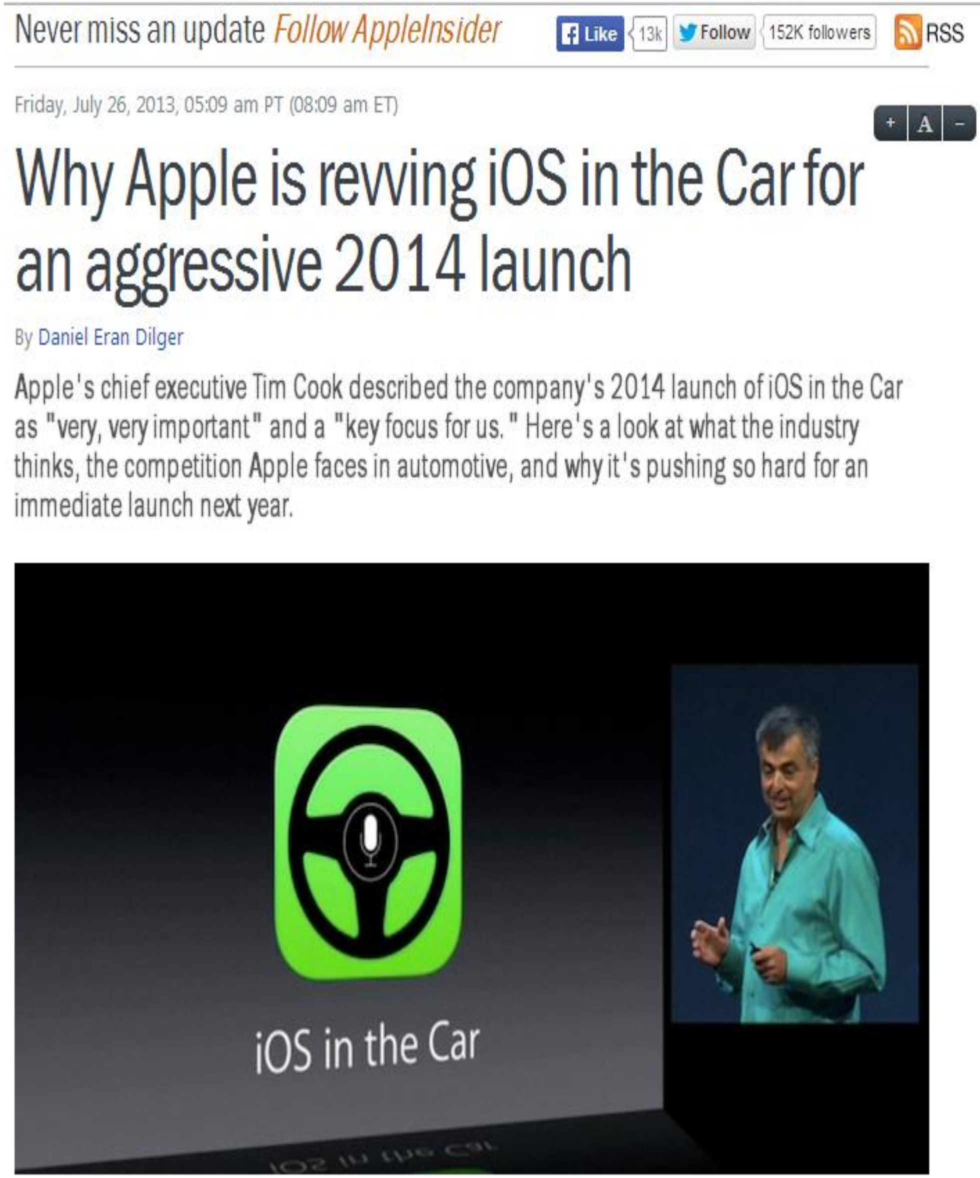
ANDROID MOBILE COMPUTING 49

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 openness, customization, and scale. Mirroring the

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)

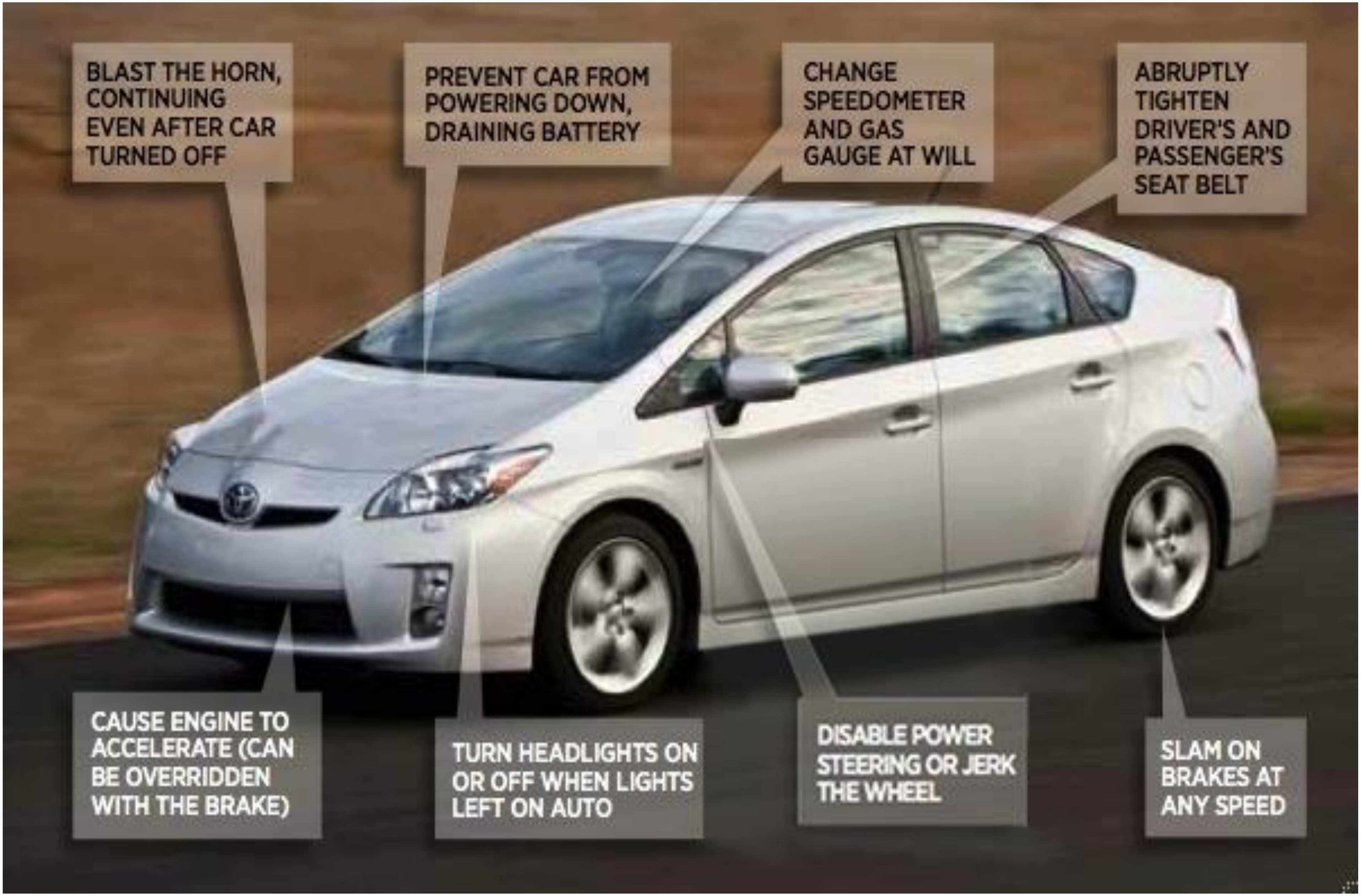
+ A −

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

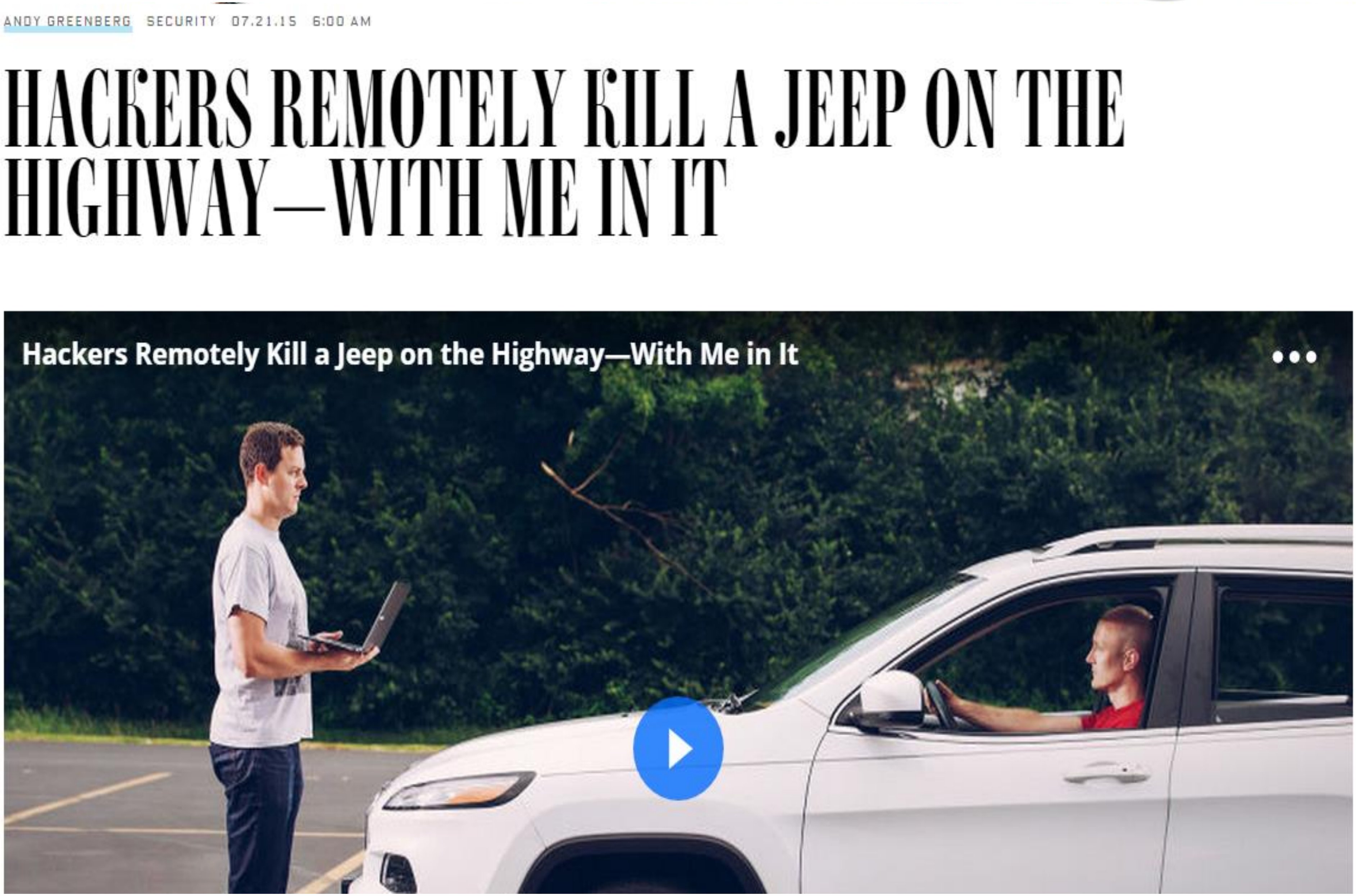
By Daniel Eran Dilger

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.

Internet Of Things - Cars


BLAST THE HORN, CONTINUING EVEN AFTER CAR TURNED OFF
PREVENT CAR FROM POWERING DOWN, DRAINING BATTERY
CHANGE SPEEDOMETER AND GAS GAUGE AT WILL
ABRUPTLY TIGHTEN DRIVER'S AND PASSENGER'S SEAT BELT
CAUSE ENGINE TO ACCELERATE (CAN BE OVERRIDDEN WITH THE BRAKE)
TURN HEADLIGHTS ON OR OFF WHEN LIGHTS LEFT ON AUTO
DISABLE POWER STEERING OR JERK THE WHEEL
SLAM ON BRAKES AT ANY SPEED

Internet of Things – What’s In The News?

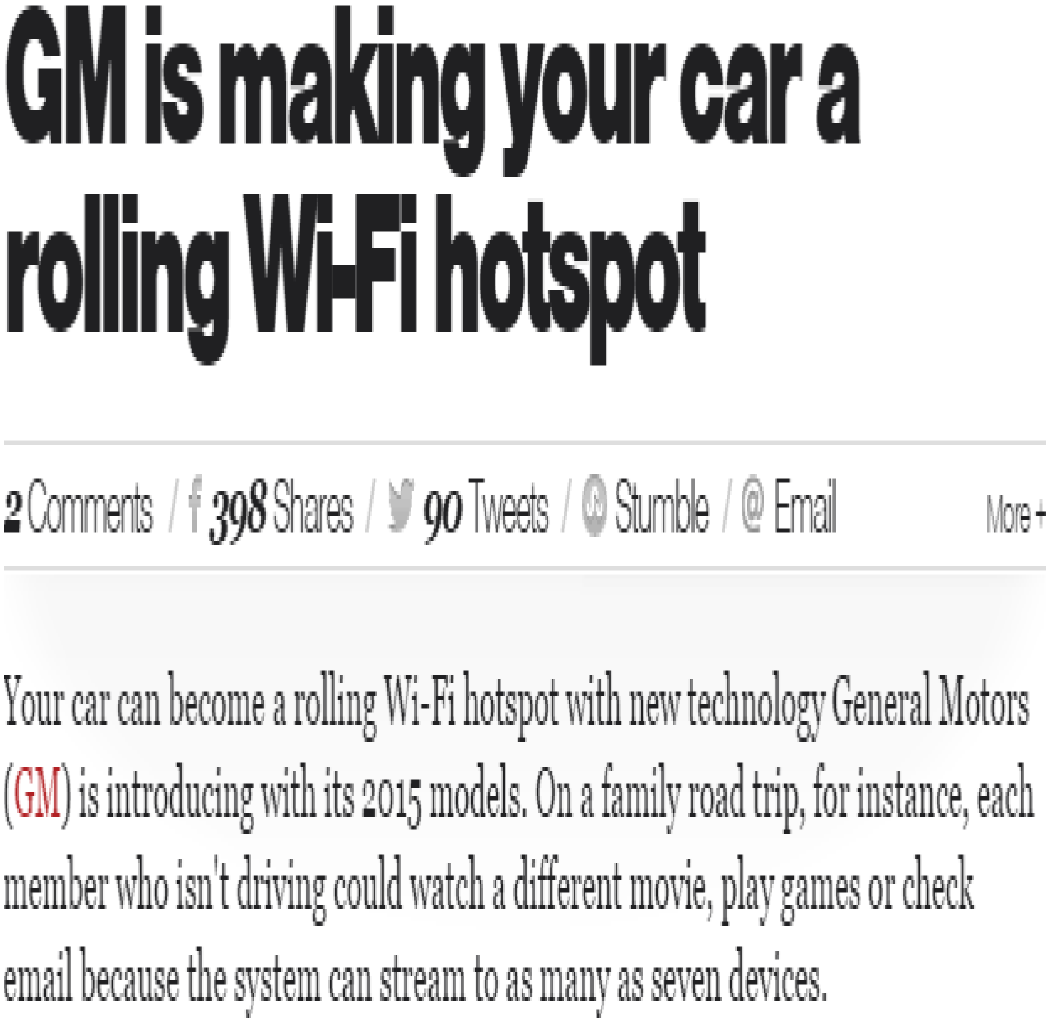


ANDY GREENBERG SECURITY 07.21.15 6:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

Hackers Remotely Kill a Jeep on the Highway—With Me in It

Internet of Things – IoT Connected



GM is making your car a rolling Wi-Fi hotspot

2 Comments / 398 Shares / 90 Tweets / Stumble / @ Email More +

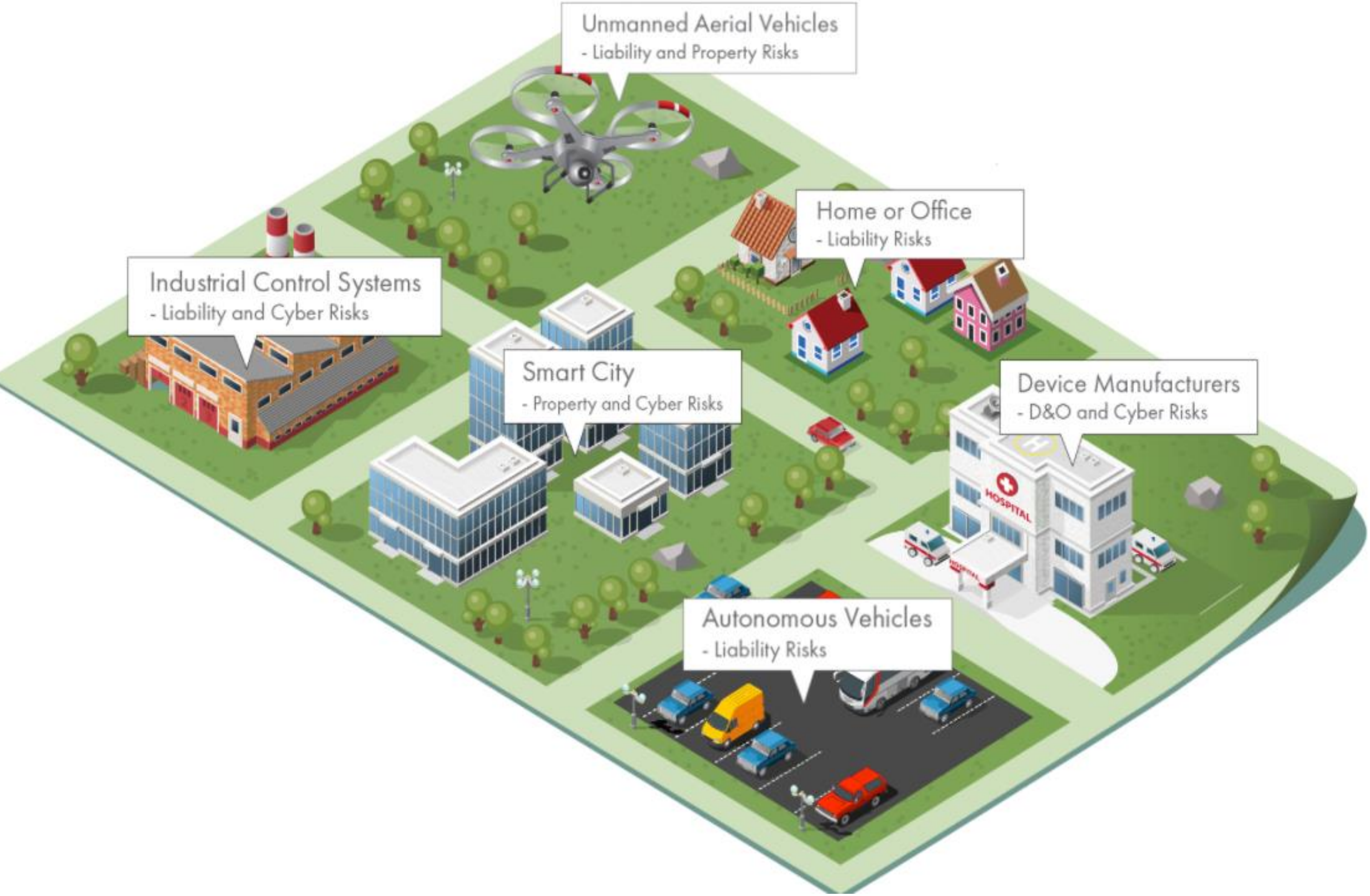
Your car can become a rolling Wi-Fi hotspot with new technology General Motors (GM) is introducing with its 2015 models. On a family road trip, for instance, each member who isn't driving could watch a different movie, play games or check email because the system can stream to as many as seven devices.

TESLA'S OVER-THE-AIR FIX: BEST EXAMPLE YET OF THE INTERNET OF THINGS?

CHANGE
AHEAD

Connected / Smart Cities

Connected / Smart Cities



Unmanned Aerial Vehicles
- Liability and Property Risks

Home or Office
- Liability Risks

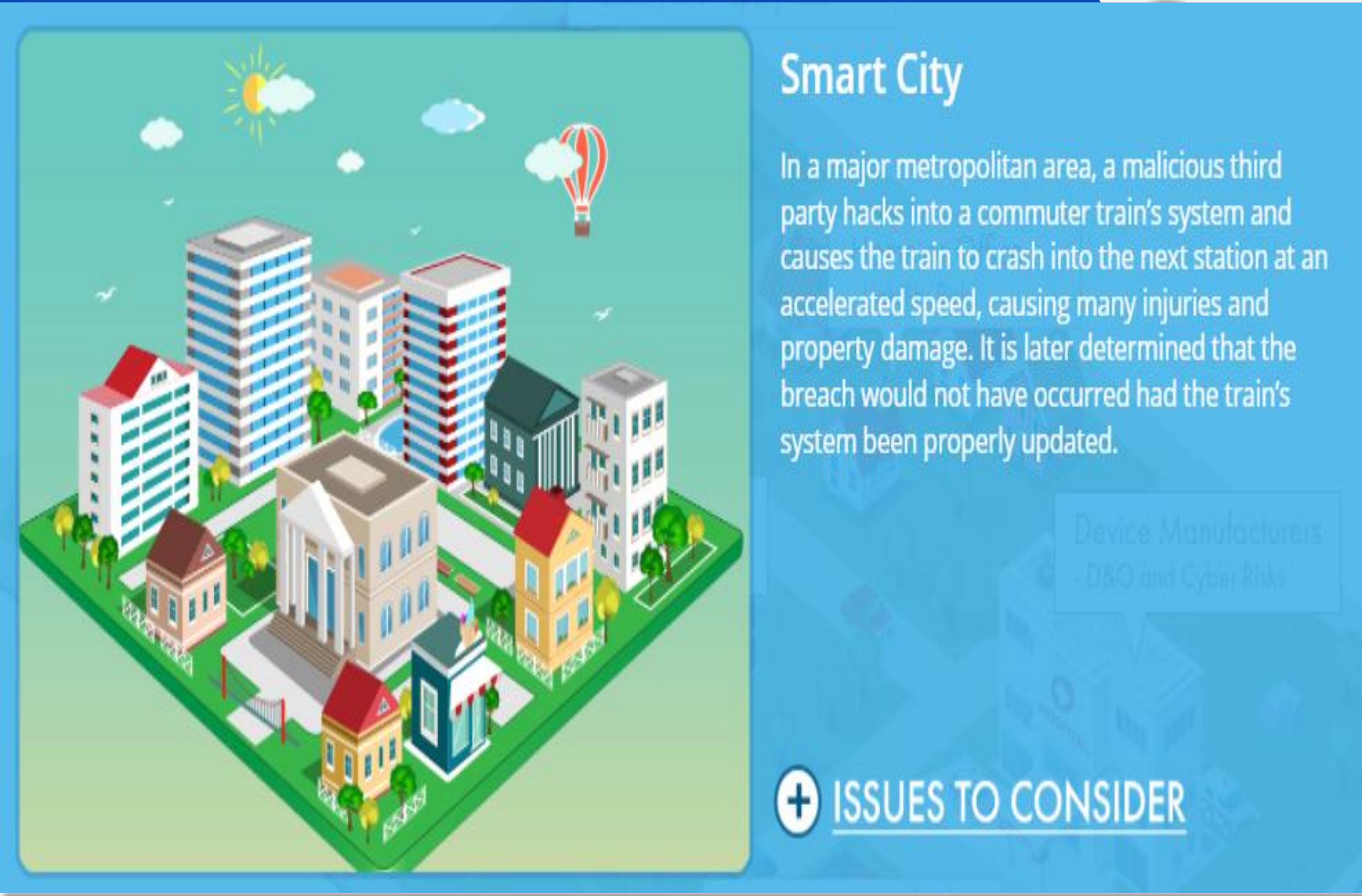
Industrial Control Systems
- Liability and Cyber Risks

Smart City
- Property and Cyber Risks

Device Manufacturers
- D&O and Cyber Risks

Autonomous Vehicles
- Liability Risks

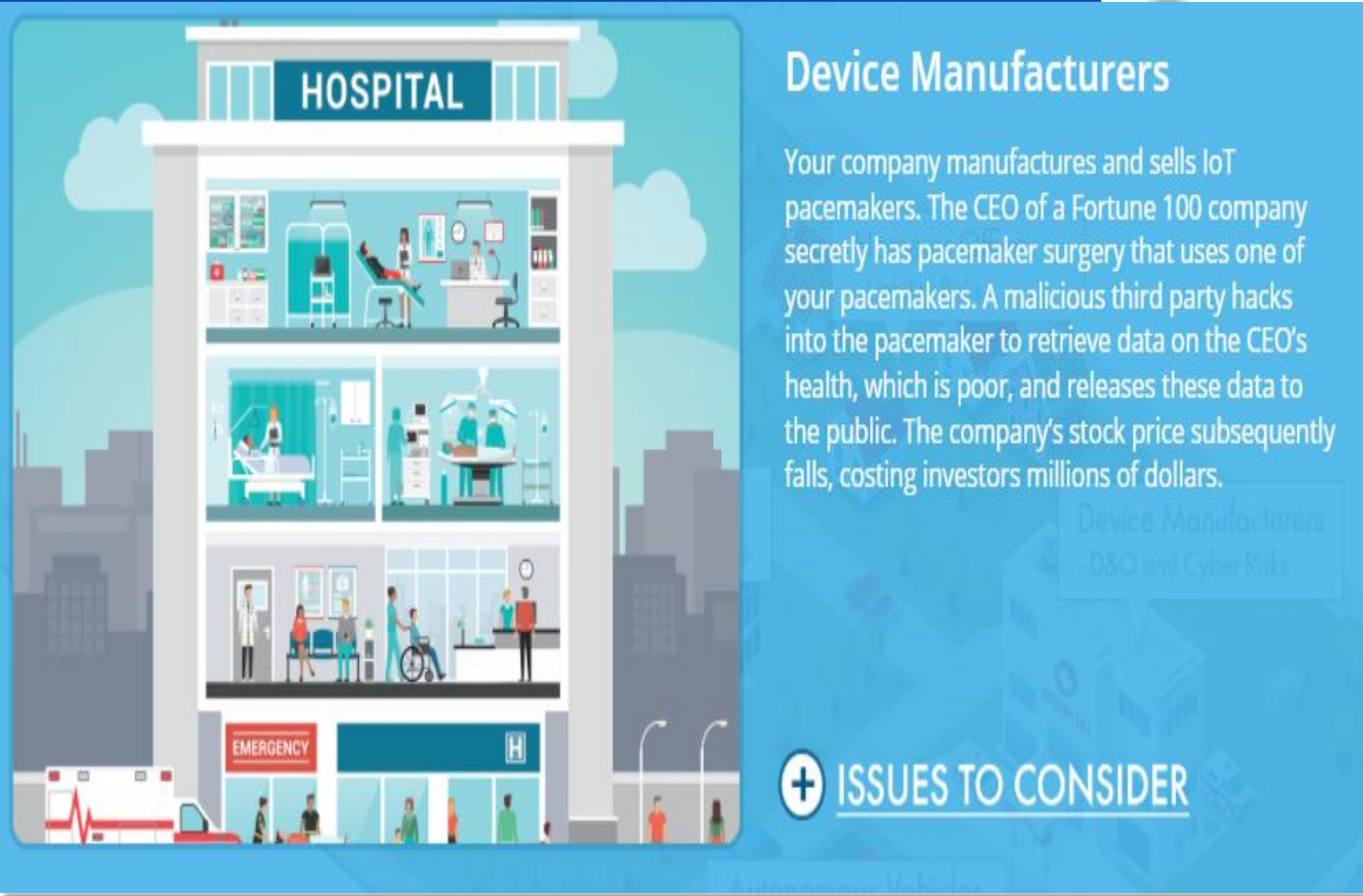
Areas That Must Be Considered



Smart City

In a major metropolitan area, a malicious third party hacks into a commuter train's system and causes the train to crash into the next station at an accelerated speed, causing many injuries and property damage. It is later determined that the breach would not have occurred had the train's system been properly updated.

Areas That Must Be Considered

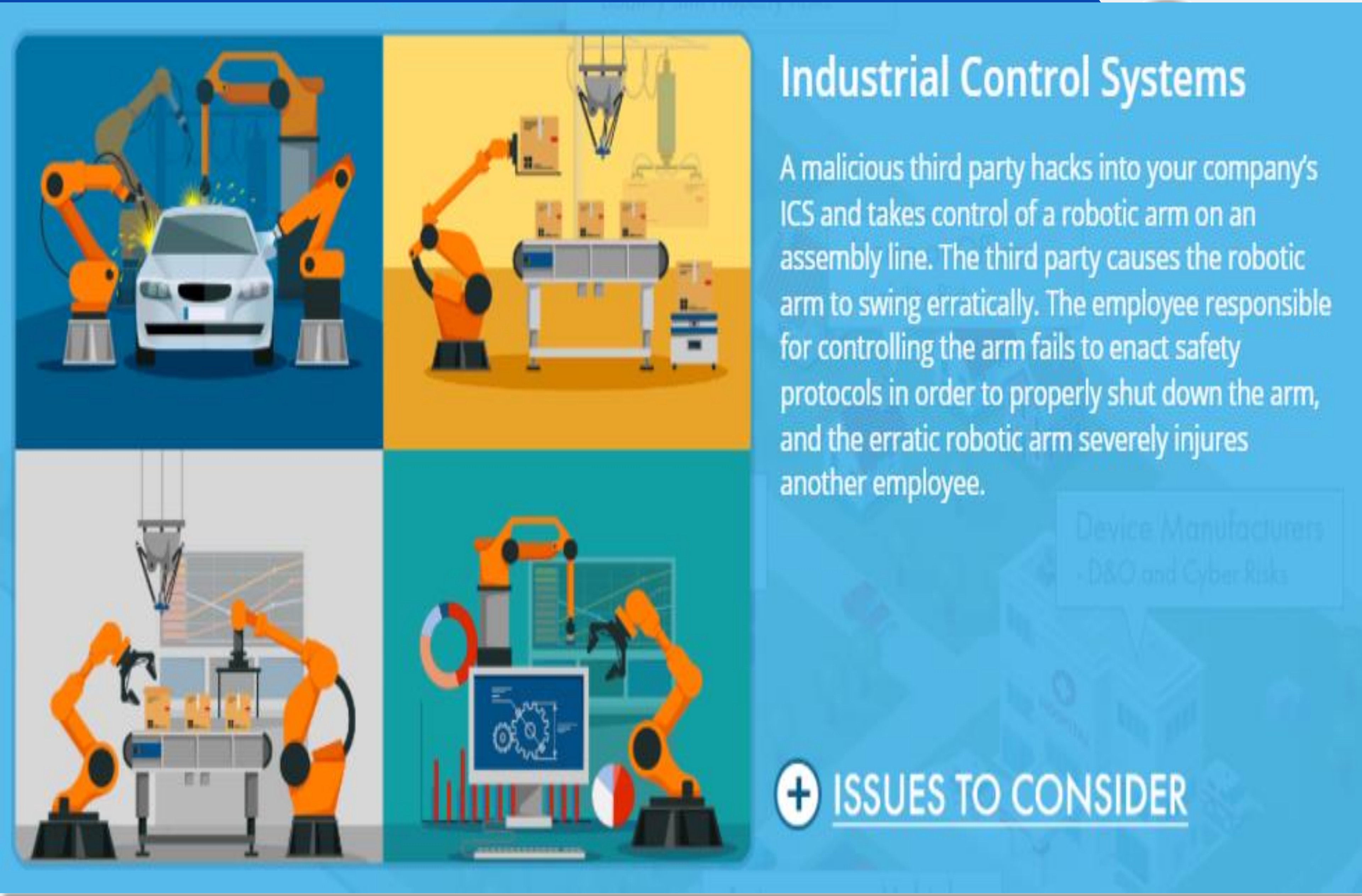


Device Manufacturers

Your company manufactures and sells IoT pacemakers. The CEO of a Fortune 100 company secretly has pacemaker surgery that uses one of your pacemakers. A malicious third party hacks into the pacemaker to retrieve data on the CEO's health, which is poor, and releases these data to the public. The company's stock price subsequently falls, costing investors millions of dollars.

⊕ ISSUES TO CONSIDER

Areas That Must Be Considered

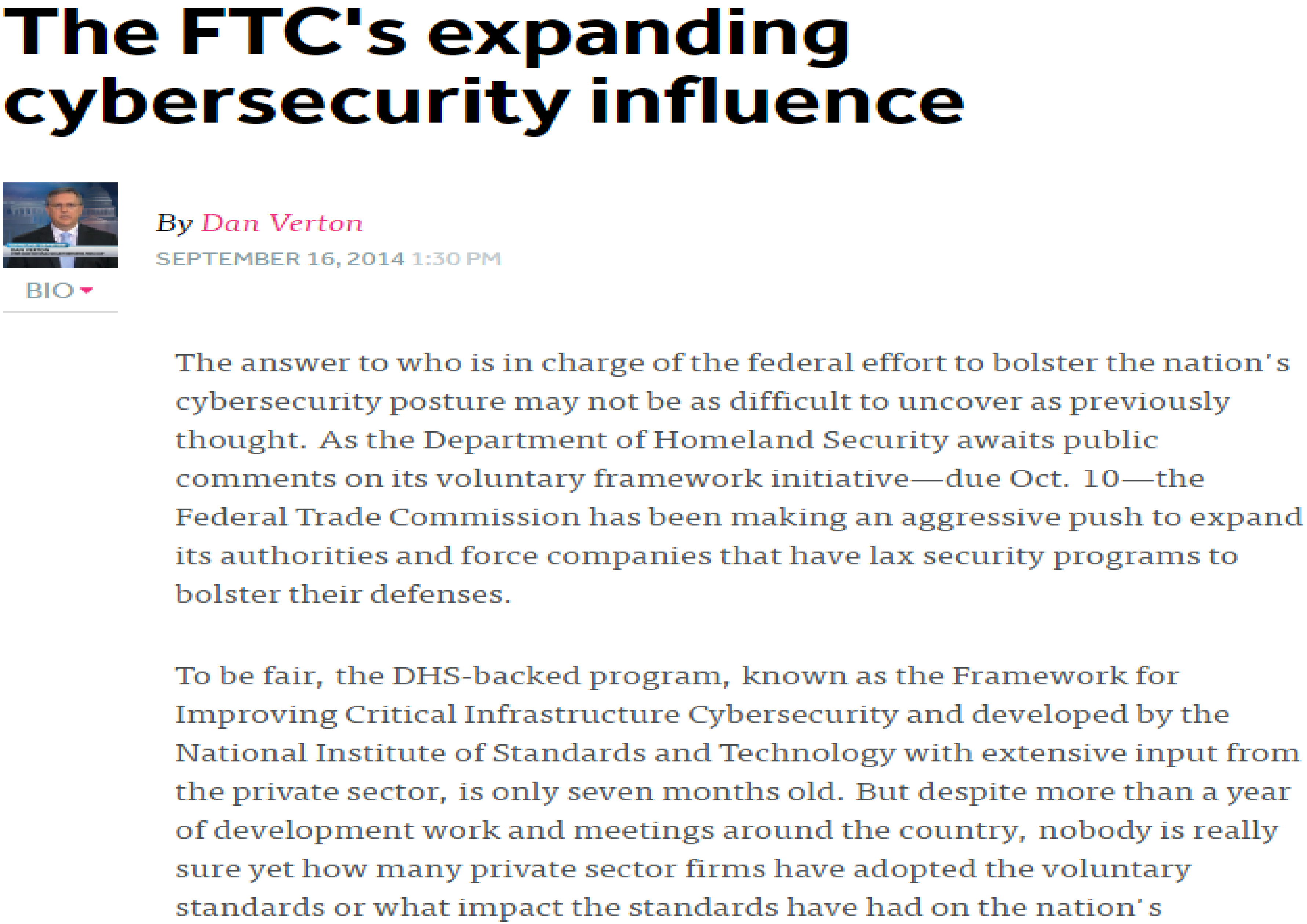


Industrial Control Systems

A malicious third party hacks into your company's ICS and takes control of a robotic arm on an assembly line. The third party causes the robotic arm to swing erratically. The employee responsible for controlling the arm fails to enact safety protocols in order to properly shut down the arm, and the erratic robotic arm severely injures another employee.

Critical Infrastructure

Liability – FTC Expanding Role



The FTC's expanding cybersecurity influence

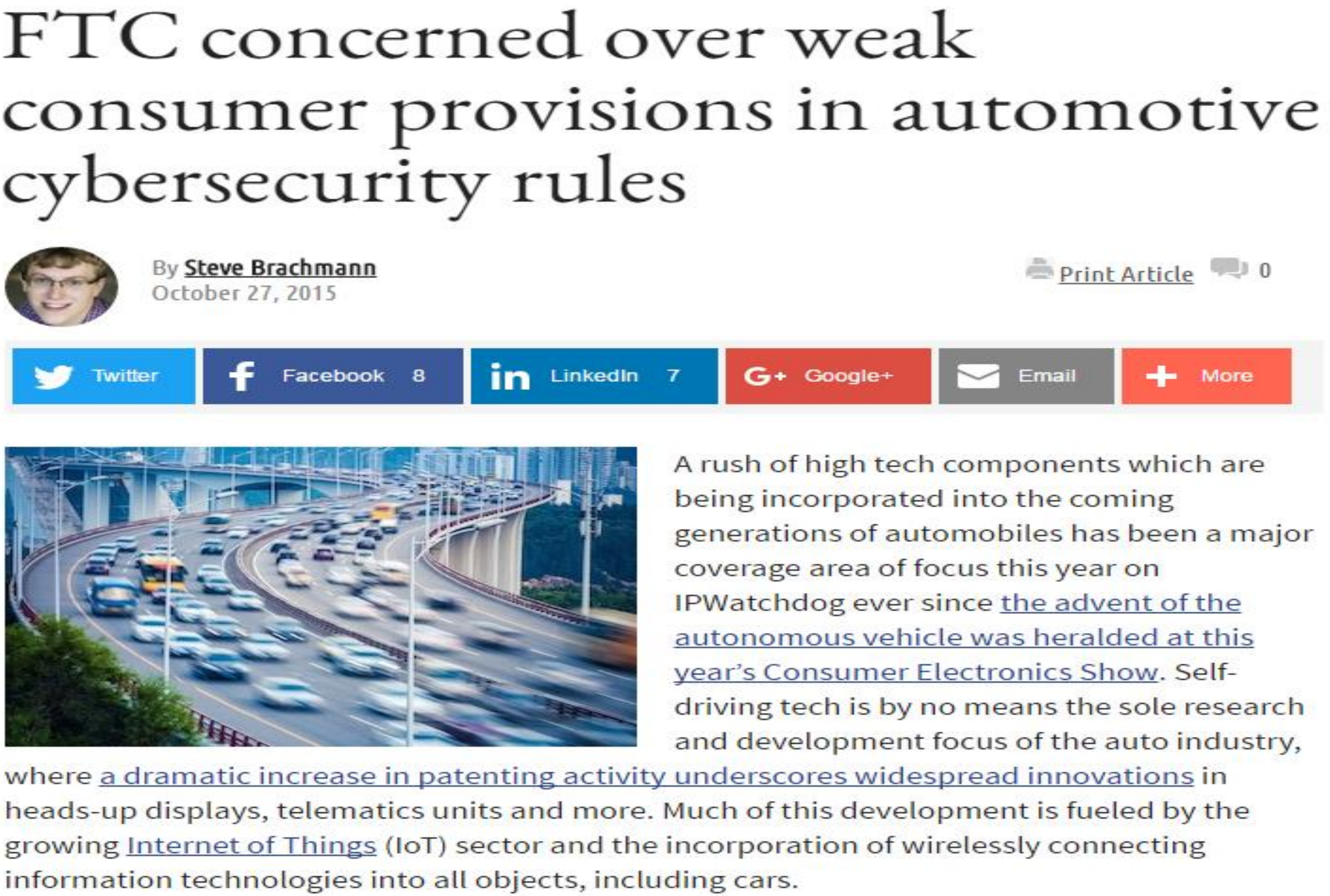
By *Dan Verton*

SEPTEMBER 16, 2014 1:30 PM

The answer to who is in charge of the federal effort to bolster the nation's cybersecurity posture may not be as difficult to uncover as previously thought. As the Department of Homeland Security awaits public comments on its voluntary framework initiative—due Oct. 10—the Federal Trade Commission has been making an aggressive push to expand its authorities and force companies that have lax security programs to bolster their defenses.

To be fair, the DHS-backed program, known as the Framework for Improving Critical Infrastructure Cybersecurity and developed by the National Institute of Standards and Technology with extensive input from the private sector, is only seven months old. But despite more than a year of development work and meetings around the country, nobody is really sure yet how many private sector firms have adopted the voluntary standards or what impact the standards have had on the nation's

Liability – FTC “concerned”

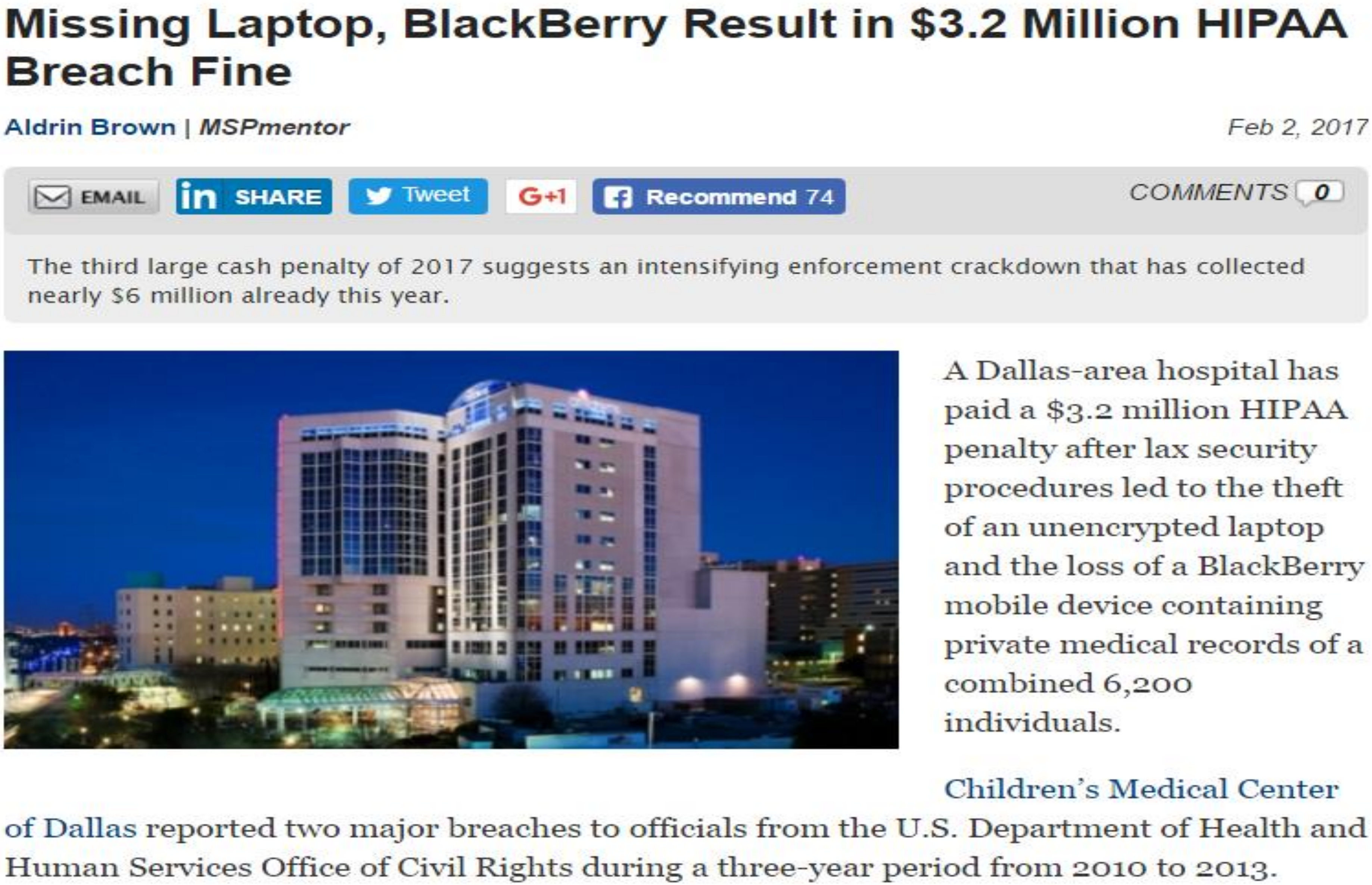


FTC concerned over weak consumer provisions in automotive cybersecurity rules

By Steve Brachmann
October 27, 2015

A rush of high tech components which are being incorporated into the coming generations of automobiles has been a major coverage area of focus this year on IPWatchdog ever since the advent of the autonomous vehicle was heralded at this year’s Consumer Electronics Show. Self-driving tech is by no means the sole research and development focus of the auto industry, where a dramatic increase in patenting activity underscores widespread innovations in heads-up displays, telematics units and more. Much of this development is fueled by the growing Internet of Things (IoT) sector and the incorporation of wirelessly connecting information technologies into all objects, including cars.

Repeat Breach = Big Fine



Missing Laptop, BlackBerry Result in $3.2 Million HIPAA Breach Fine

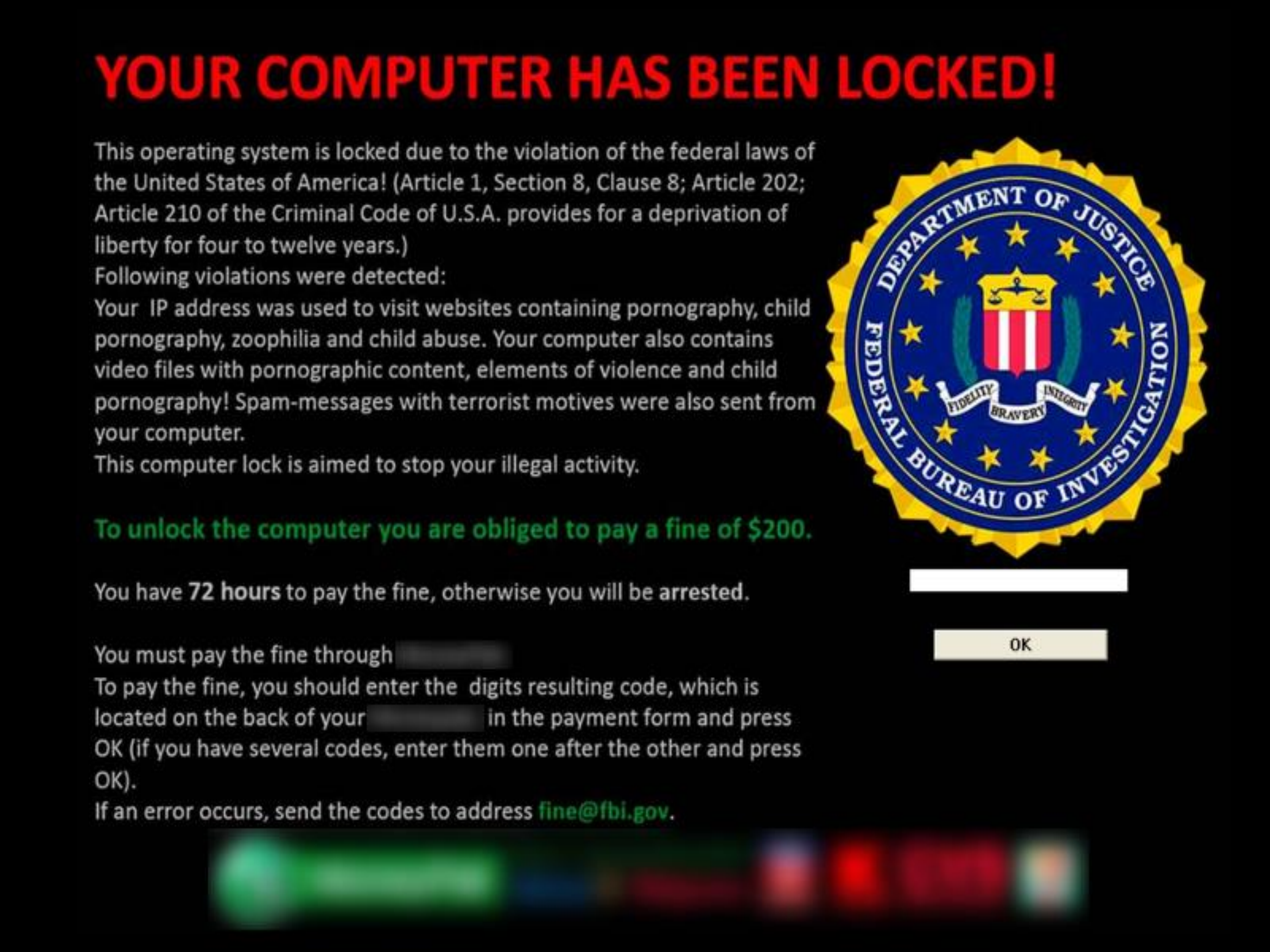
Aldrin Brown | *MSPmentor*

Feb 2, 2017

The third large cash penalty of 2017 suggests an intensifying enforcement crackdown that has collected nearly $6 million already this year.

A Dallas-area hospital has paid a $3.2 million HIPAA penalty after lax security procedures led to the theft of an unencrypted laptop and the loss of a BlackBerry mobile device containing private medical records of a combined 6,200 individuals.

Children's Medical Center of Dallas reported two major breaches to officials from the U.S. Department of Health and Human Services Office of Civil Rights during a three-year period from 2010 to 2013.



YOUR COMPUTER HAS BEEN LOCKED!

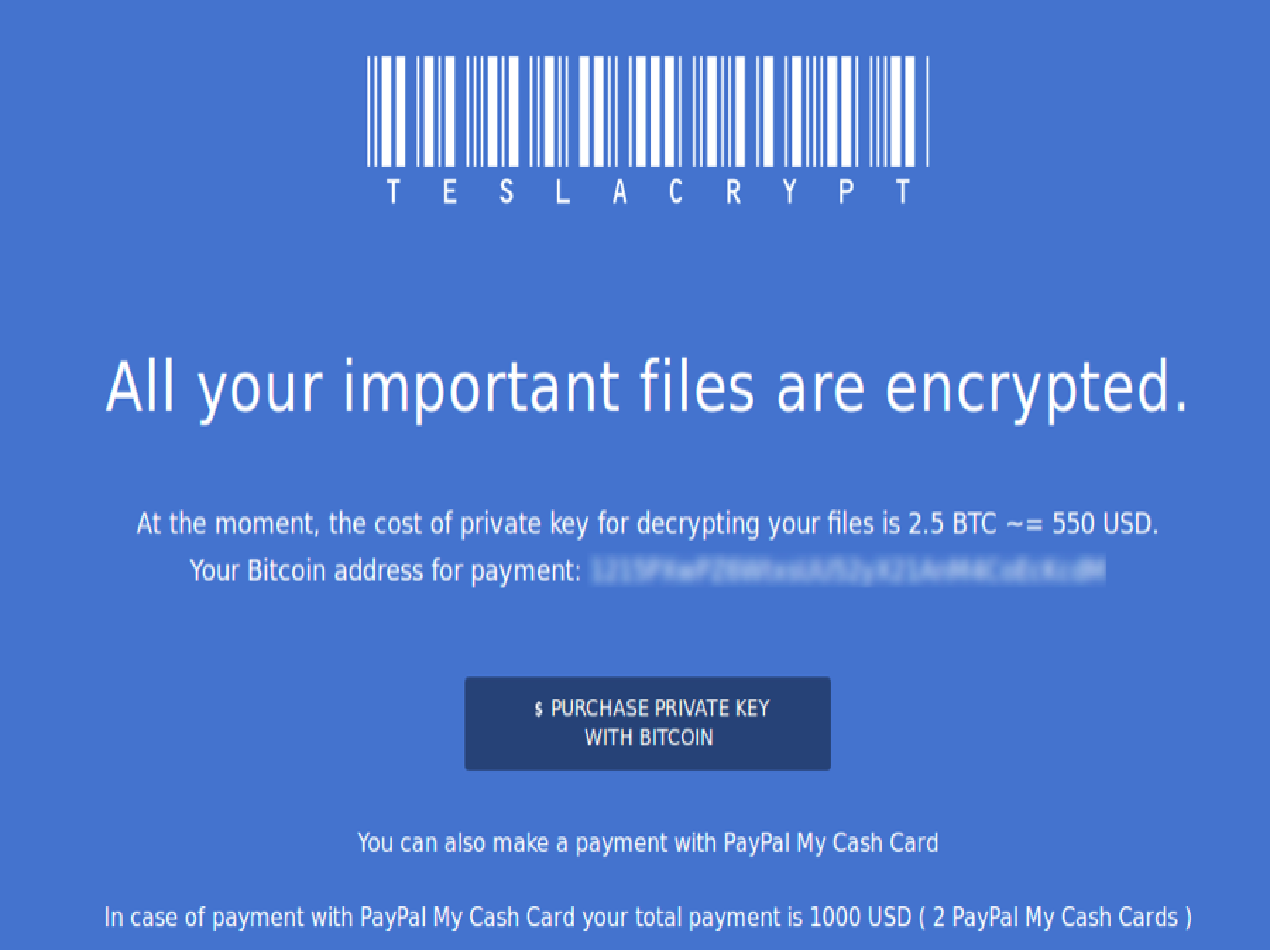
This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

You have **72 hours** to pay the fine, otherwise you will be **arrested**.

You must pay the fine through [redacted]
To pay the fine, you should enter the digits resulting code, which is located on the back of your [redacted] in the payment form and press OK (if you have several codes, enter them one after the other and press OK).
If an error occurs, send the codes to address fine@fbi.gov.

[redacted]



TESLACRYPT

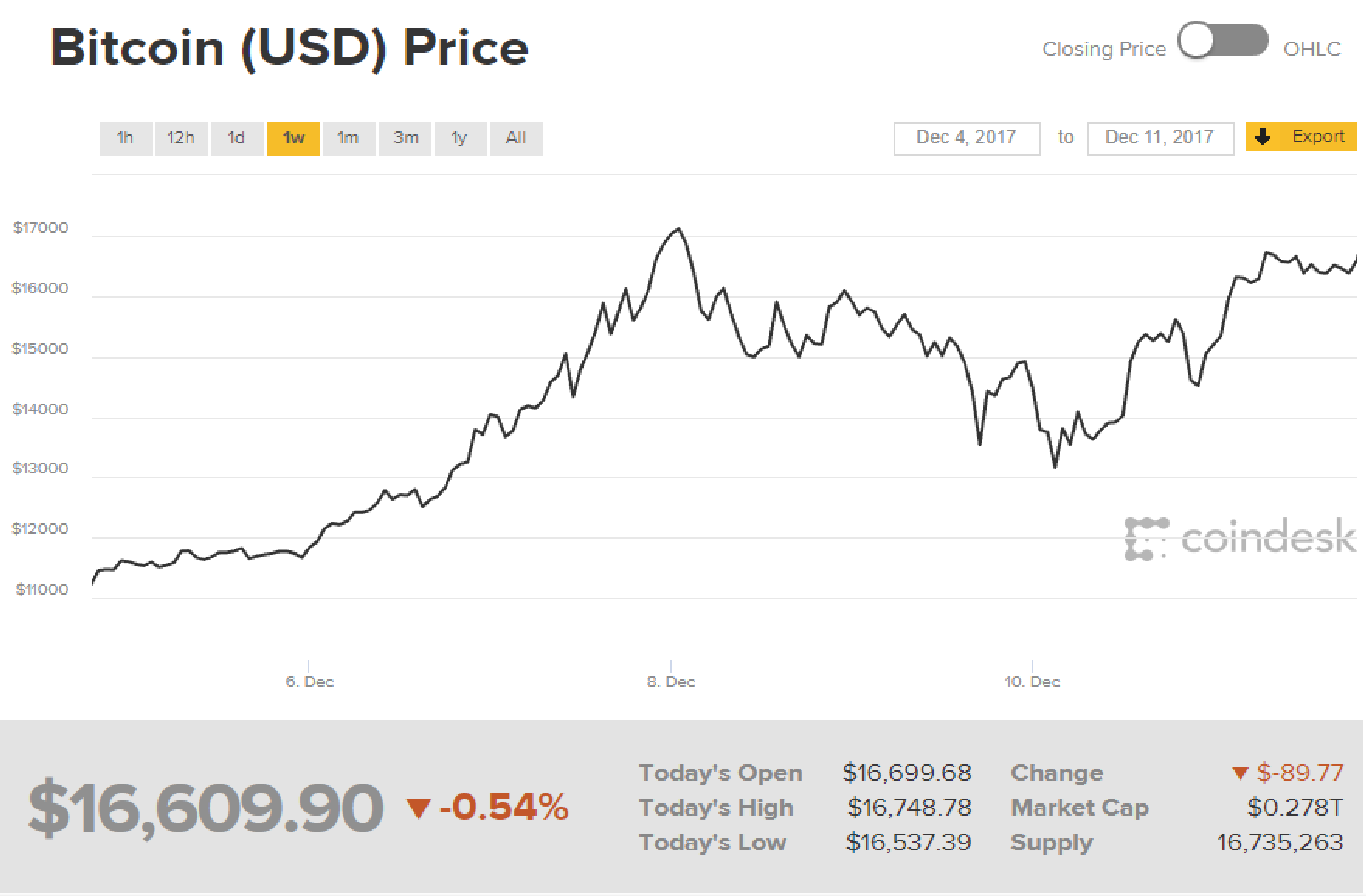
All your important files are encrypted.

At the moment, the cost of private key for decrypting your files is 2.5 BTC ~= 550 USD.
Your Bitcoin address for payment: [redacted]

You can also make a payment with PayPal My Cash Card

In case of payment with PayPal My Cash Card your total payment is 1000 USD (2 PayPal My Cash Cards)

Bitcoin – Trading @ $16,609 – 12/11/2017



Bitcoin (USD) Price

Closing Price ○ OHLC

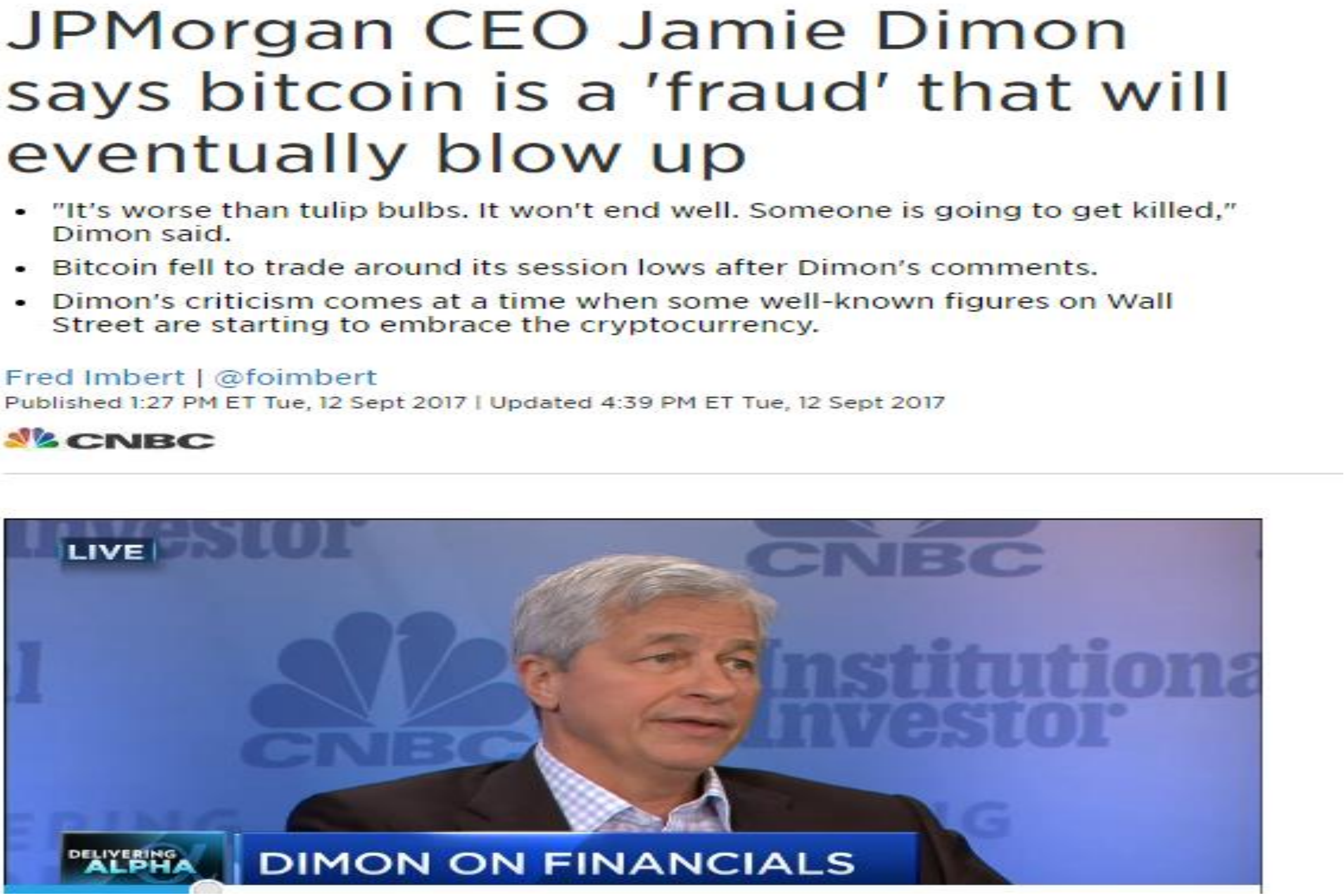
1h | 12h | 1d | **1w** | 1m | 3m | 1y | All

Dec 4, 2017 to Dec 11, 2017 Export

$16,609.90 ▼ -0.54%

Today's Open	$16,699.68	Change	▼ $-89.77
Today's High	$16,748.78	Market Cap	$0.278T
Today's Low	$16,537.39	Supply	16,735,263

Bitcoin – Trading @ $16,609 – 12/11/2017



JPMorgan CEO Jamie Dimon says bitcoin is a 'fraud' that will eventually blow up

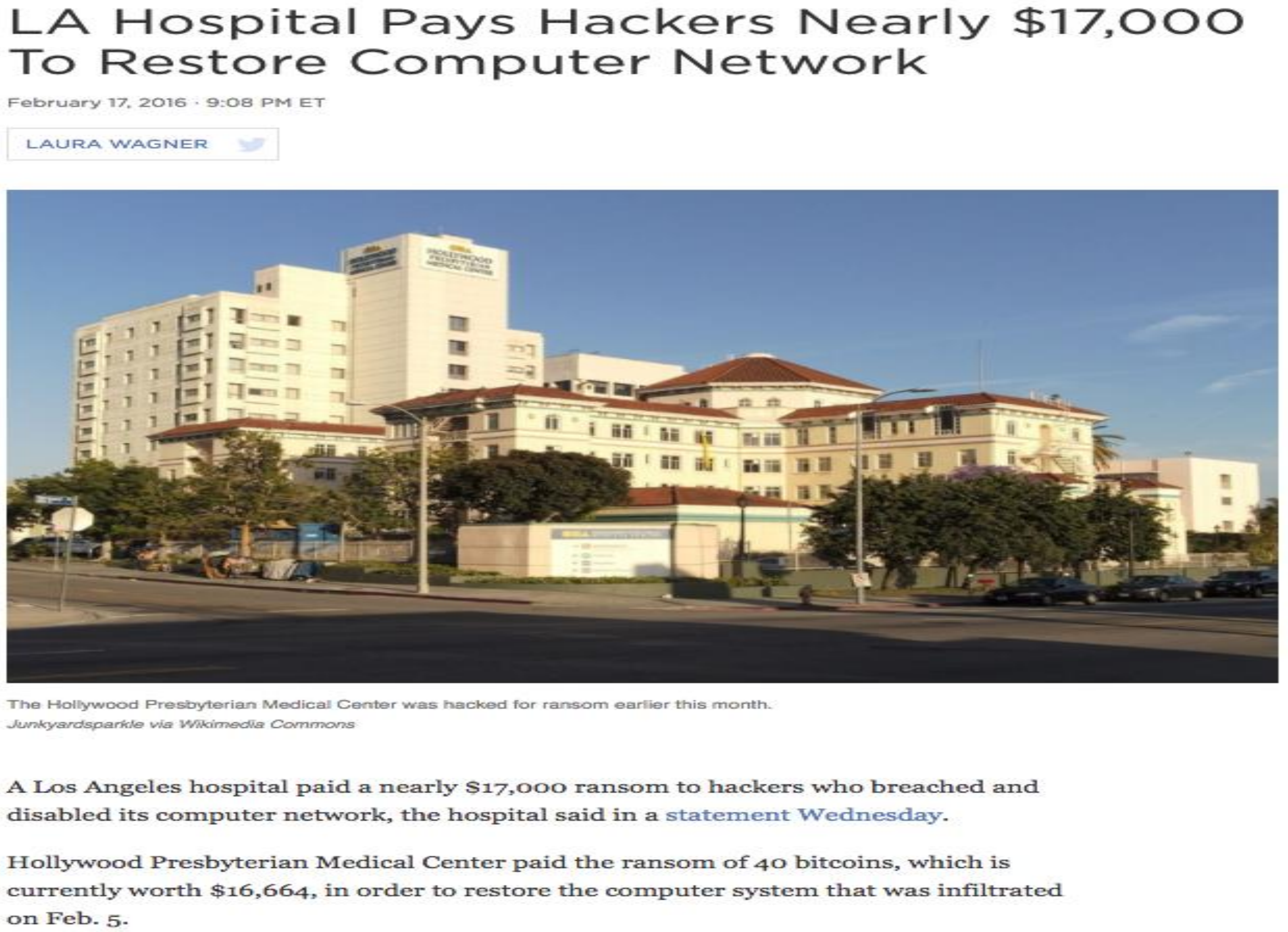
- "It's worse than tulip bulbs. It won't end well. Someone is going to get killed," Dimon said.
- Bitcoin fell to trade around its session lows after Dimon's comments.
- Dimon's criticism comes at a time when some well-known figures on Wall Street are starting to embrace the cryptocurrency.

Fred Imbert | @foimbert

Published 1:27 PM ET Tue, 12 Sept 2017 | Updated 4:39 PM ET Tue, 12 Sept 2017

CNBC

Ransomware



LA Hospital Pays Hackers Nearly $17,000 To Restore Computer Network

February 17, 2016 · 9:08 PM ET

LAURA WAGNER

The Hollywood Presbyterian Medical Center was hacked for ransom earlier this month.
Junkyardsparkle via Wikimedia Commons

A Los Angeles hospital paid a nearly $17,000 ransom to hackers who breached and disabled its computer network, the hospital said in a statement Wednesday.

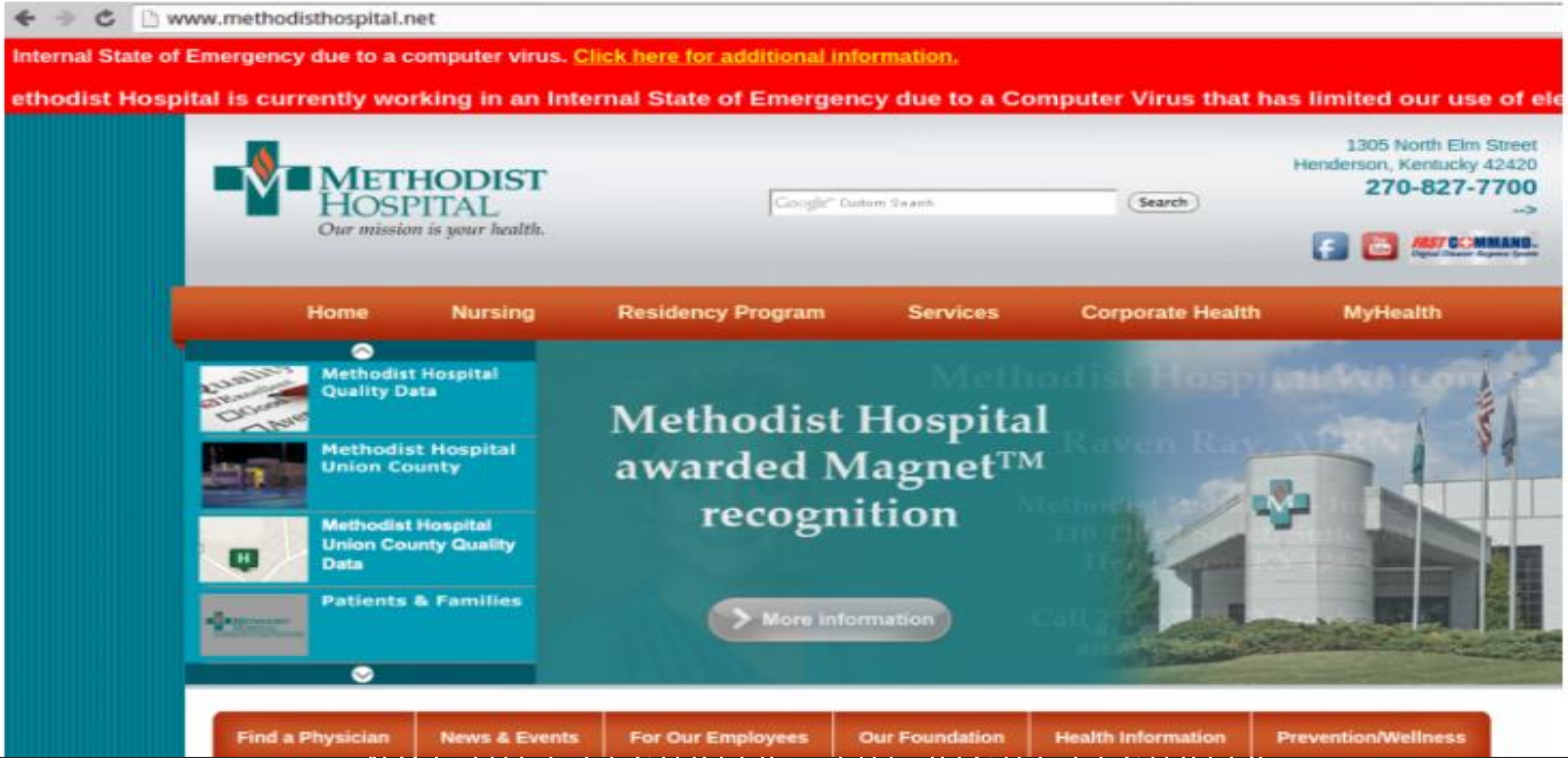
Hollywood Presbyterian Medical Center paid the ransom of 40 bitcoins, which is currently worth $16,664, in order to restore the computer system that was infiltrated on Feb. 5.

Ransomware

22 MAR 16

Hospital Declares 'Internal State of Emergency' After Ransomware Infection

A Kentucky hospital says it is operating in an "internal state of emergency" after a ransomware attack rattled around inside its networks, encrypting files on computer systems and holding the data on them hostage unless and until the hospital pays up.



www.methodisthospital.net

Internal State of Emergency due to a computer virus. Click here for additional information.

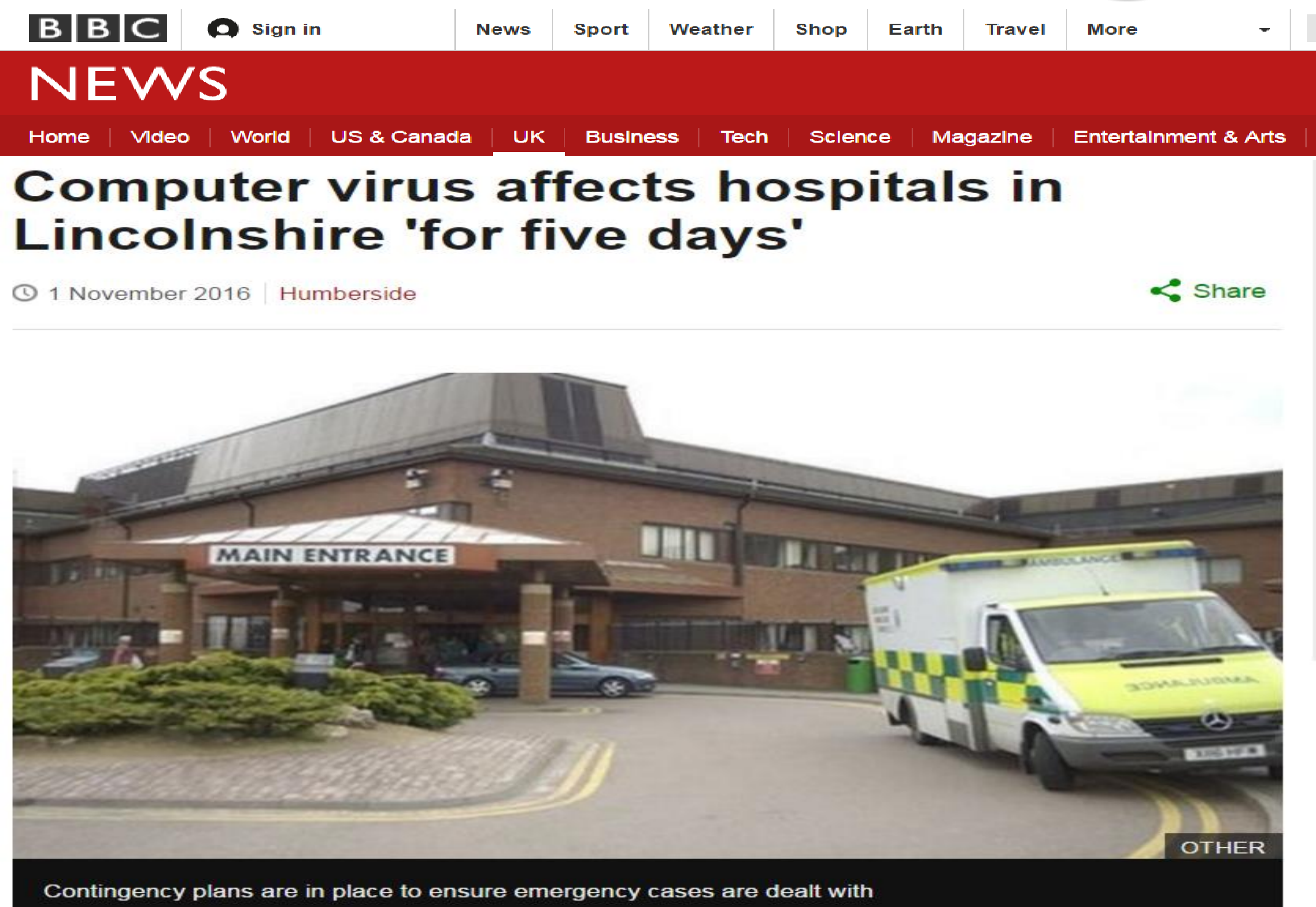
ethodist Hospital is currently working in an Internal State of Emergency due to a Computer Virus that has limited our use of ele

METHODIST HOSPITAL
Our mission is your health.

1305 North Elm Street
Henderson, Kentucky 42420
270-827-7700

Methodist Hospital awarded Magnet™ recognition

Ransomware

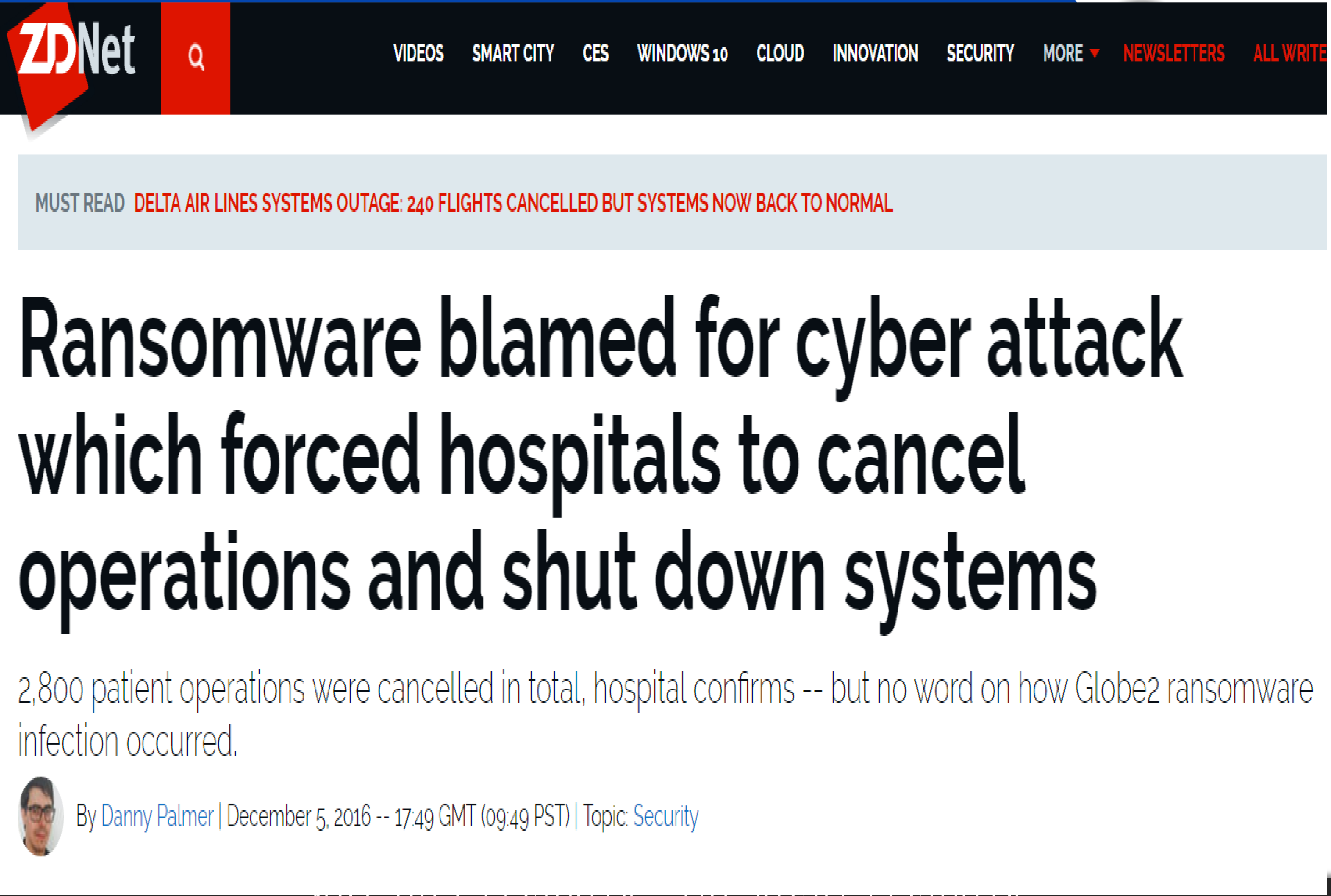


Computer virus affects hospitals in Lincolnshire 'for five days'

1 November 2016 | Humberside

Contingency plans are in place to ensure emergency cases are dealt with

Ransomware



MUST READ DELTA AIR LINES SYSTEMS OUTAGE: 240 FLIGHTS CANCELLED BUT SYSTEMS NOW BACK TO NORMAL

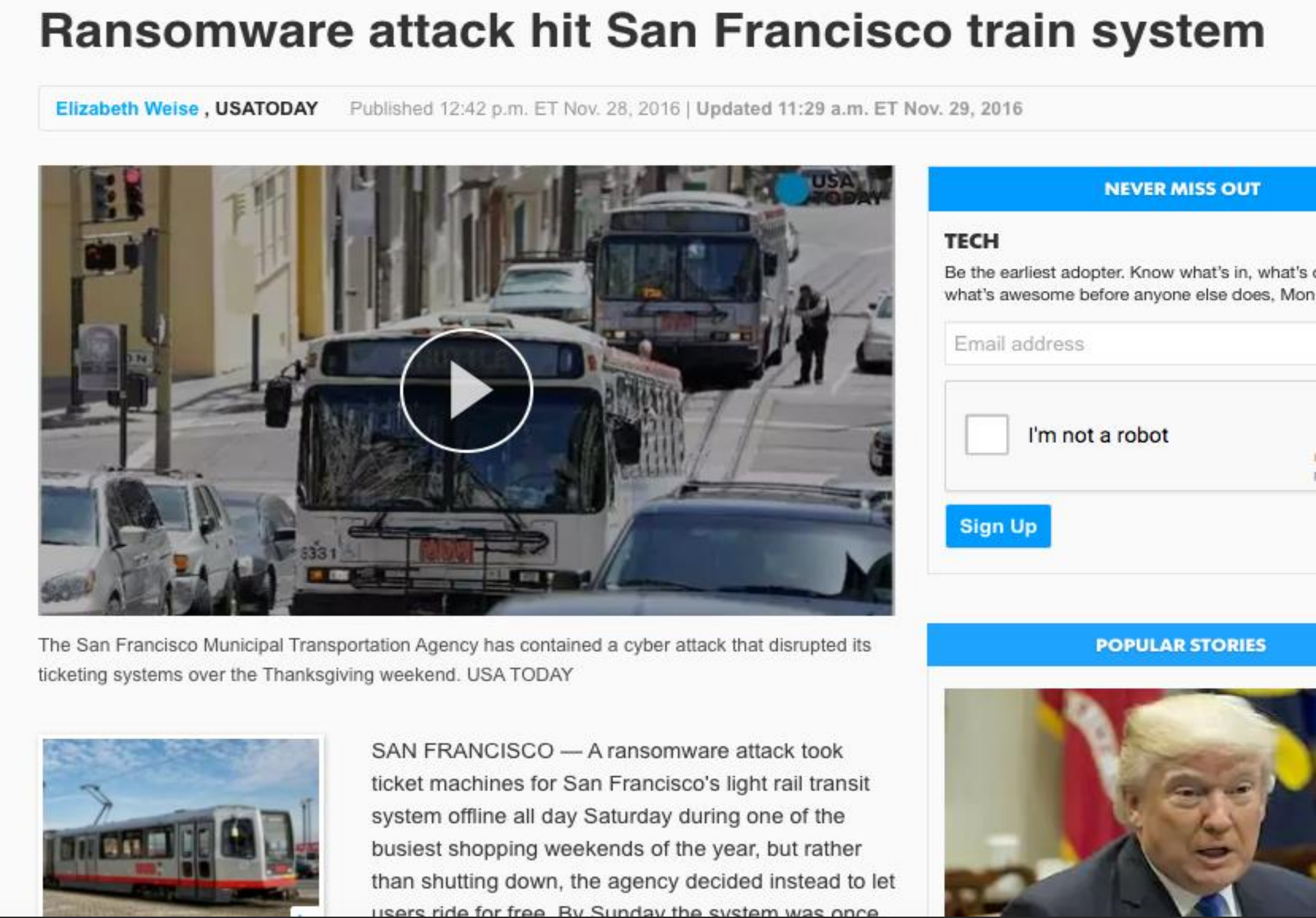
Ransomware blamed for cyber attack which forced hospitals to cancel operations and shut down systems

2,800 patient operations were cancelled in total, hospital confirms -- but no word on how Globe2 ransomware infection occurred.

By Danny Palmer | December 5, 2016 -- 17:49 GMT (09:49 PST) | Topic: Security

Ransomware – Not Just Hospitals!

RiskBased SECURITY



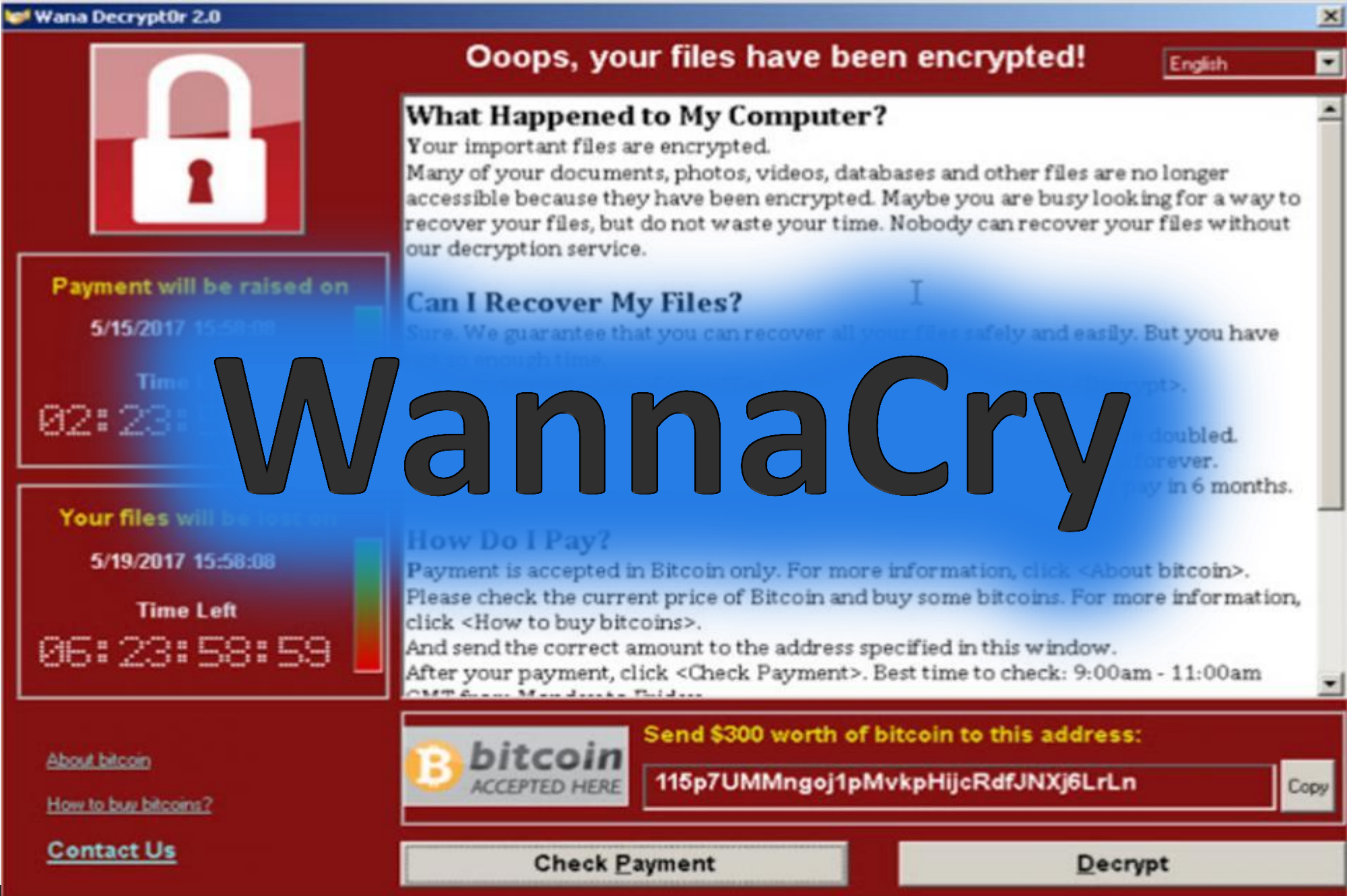
Ransomware attack hit San Francisco train system

Elizabeth Weise , USATODAY   Published 12:42 p.m. ET Nov. 28, 2016 | Updated 11:29 a.m. ET Nov. 29, 2016

The San Francisco Municipal Transportation Agency has contained a cyber attack that disrupted its ticketing systems over the Thanksgiving weekend. USA TODAY

SAN FRANCISCO — A ransomware attack took ticket machines for San Francisco's light rail transit system offline all day Saturday during one of the busiest shopping weekends of the year, but rather than shutting down, the agency decided instead to let users ride for free. By Sunday the system was once

Ransomware



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

crypt>.

doubled.

forever.

ay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on

5/15/2017 15:58:08

Time Left

02:23:

Your files will be lost on

5/19/2017 15:58:08

Time Left

06:23:58:59

About bitcoin

How to buy bitcoins?

Contact Us

bitcoin ACCEPTED HERE

Send $300 worth of bitcoin to this address:

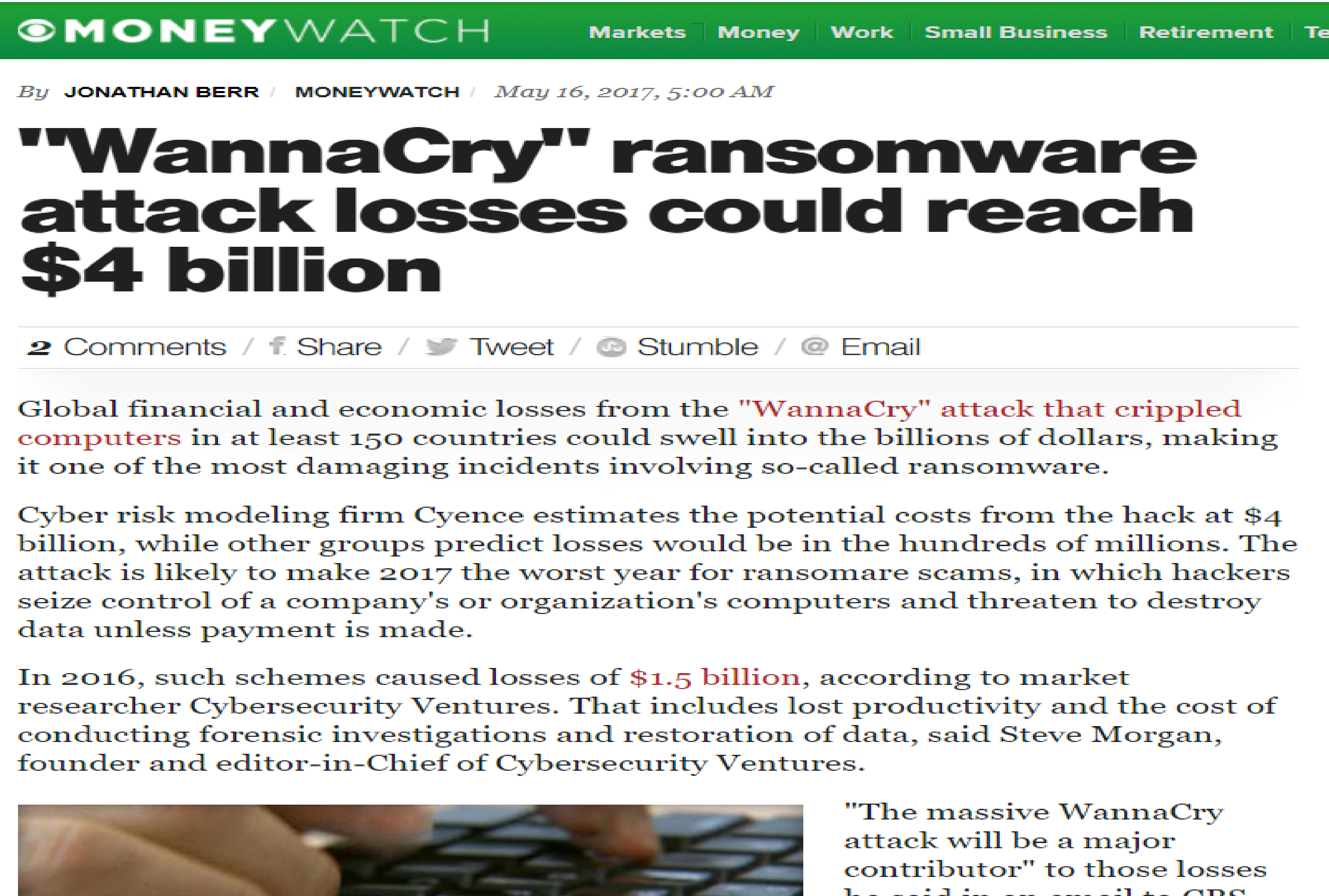
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

Copy

Check Payment

Decrypt

WannaCry Estimated Costs



By JONATHAN BERR / MONEYWATCH / *May 16, 2017, 5:00 AM*

"WannaCry" ransomware attack losses could reach $4 billion

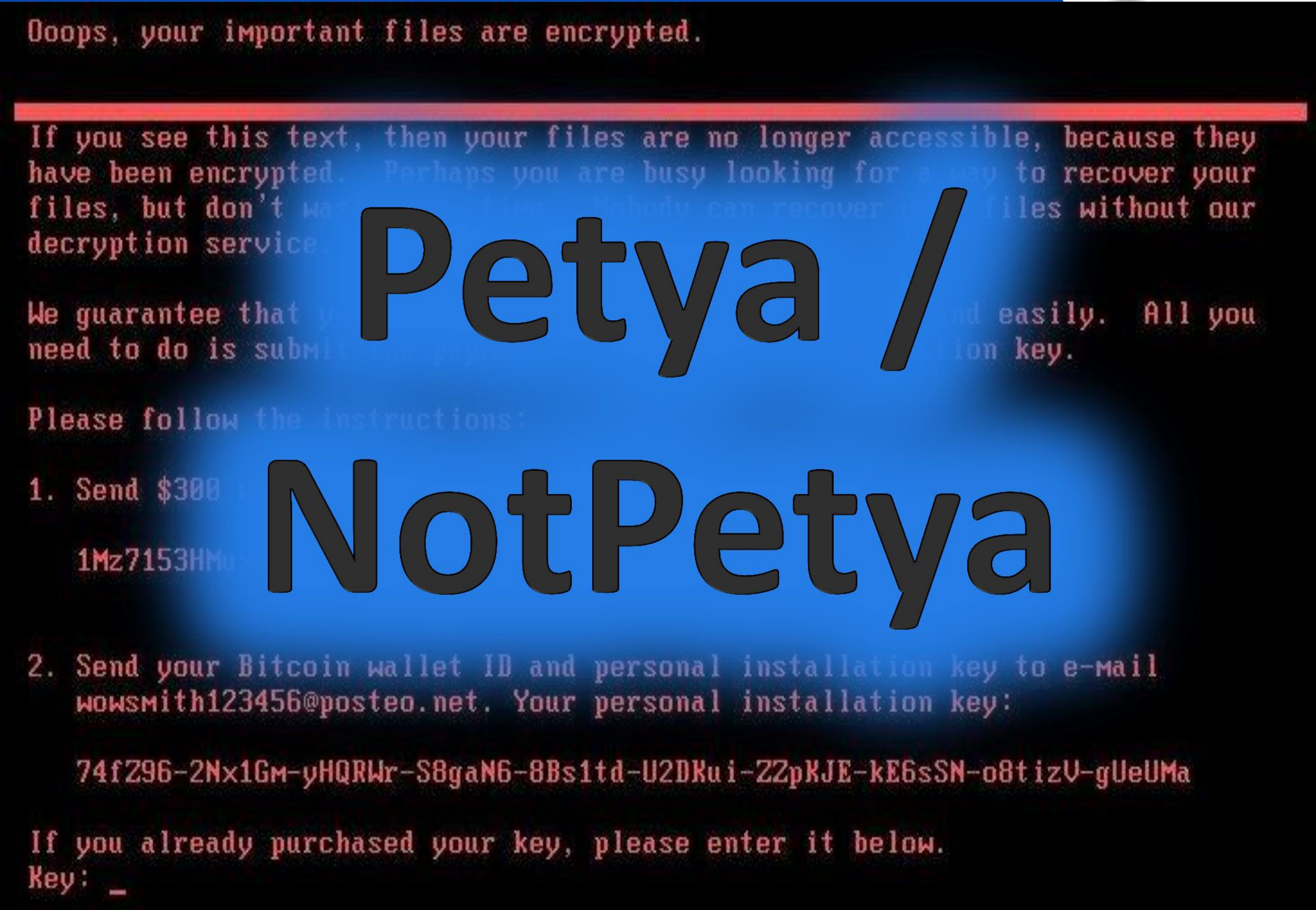
Global financial and economic losses from the "WannaCry" attack that crippled computers in at least 150 countries could swell into the billions of dollars, making it one of the most damaging incidents involving so-called ransomware.

Cyber risk modeling firm Cyence estimates the potential costs from the hack at $4 billion, while other groups predict losses would be in the hundreds of millions. The attack is likely to make 2017 the worst year for ransomare scams, in which hackers seize control of a company's or organization's computers and threaten to destroy data unless payment is made.

In 2016, such schemes caused losses of $1.5 billion, according to market researcher Cybersecurity Ventures. That includes lost productivity and the cost of conducting forensic investigations and restoration of data, said Steve Morgan, founder and editor-in-Chief of Cybersecurity Ventures.

"The massive WannaCry attack will be a major contributor" to those losses he said in an email to CBS

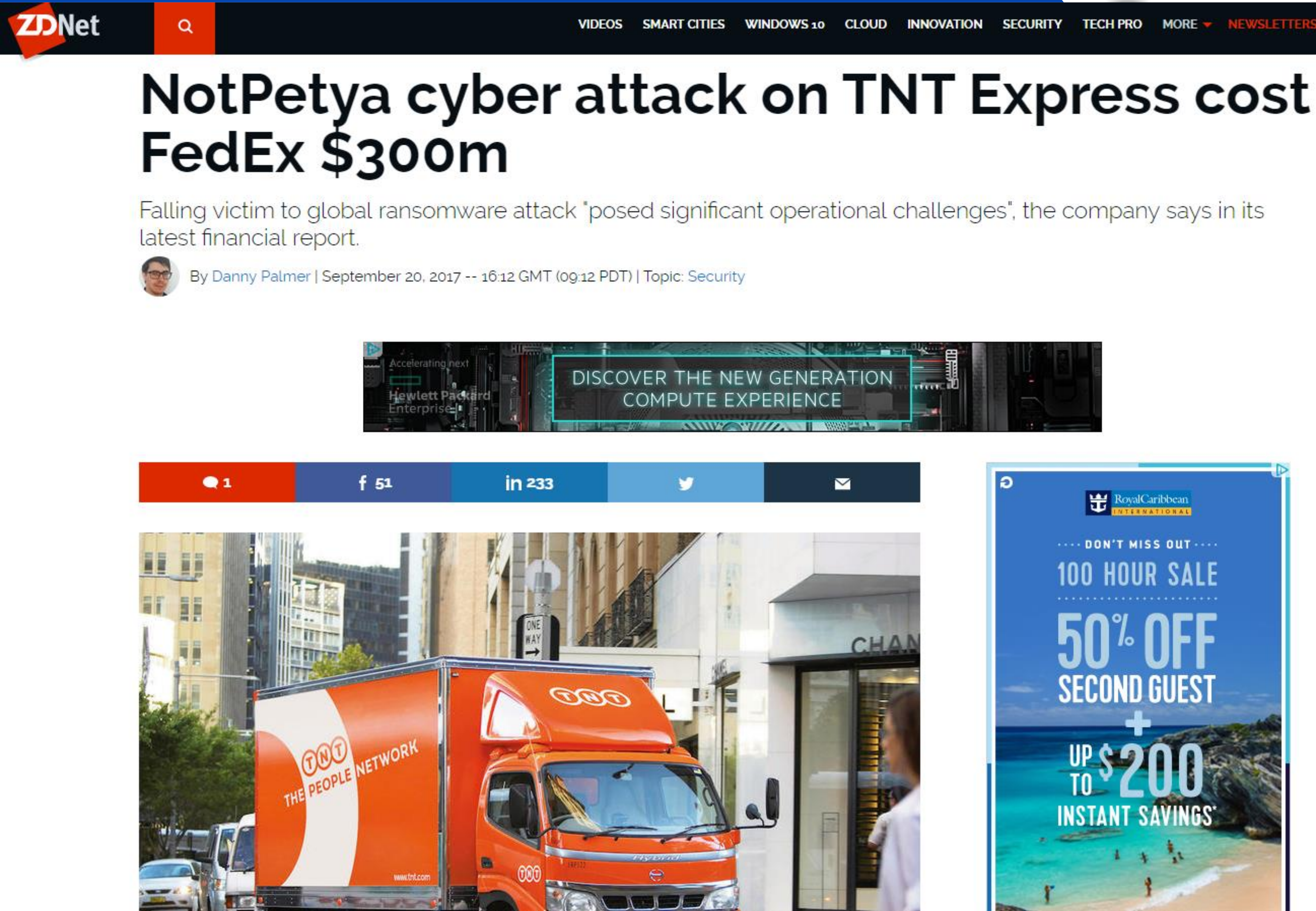
Ransomware



Petya / NotPetya

```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted. Perhaps you are busy looking for a way to recover your
files, but don't wa[illegible] time. Nobody can recover [illegible] files without our
decryption service.

We guarantee that y[illegible] nd easily. All you
need to do is submit [illegible] tion key.

Please follow the instructions:

1. Send $300 [illegible]

   1Mz7153HMu[illegible]

2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   74f296-2Nx1Gm-yHQRWr-S8gaN6-8Bs1td-U2DKui-ZZpKJE-kE6sSN-o8tizV-gUeUMa

If you already purchased your key, please enter it below.
Key: _
```

Petya Estimated Costs

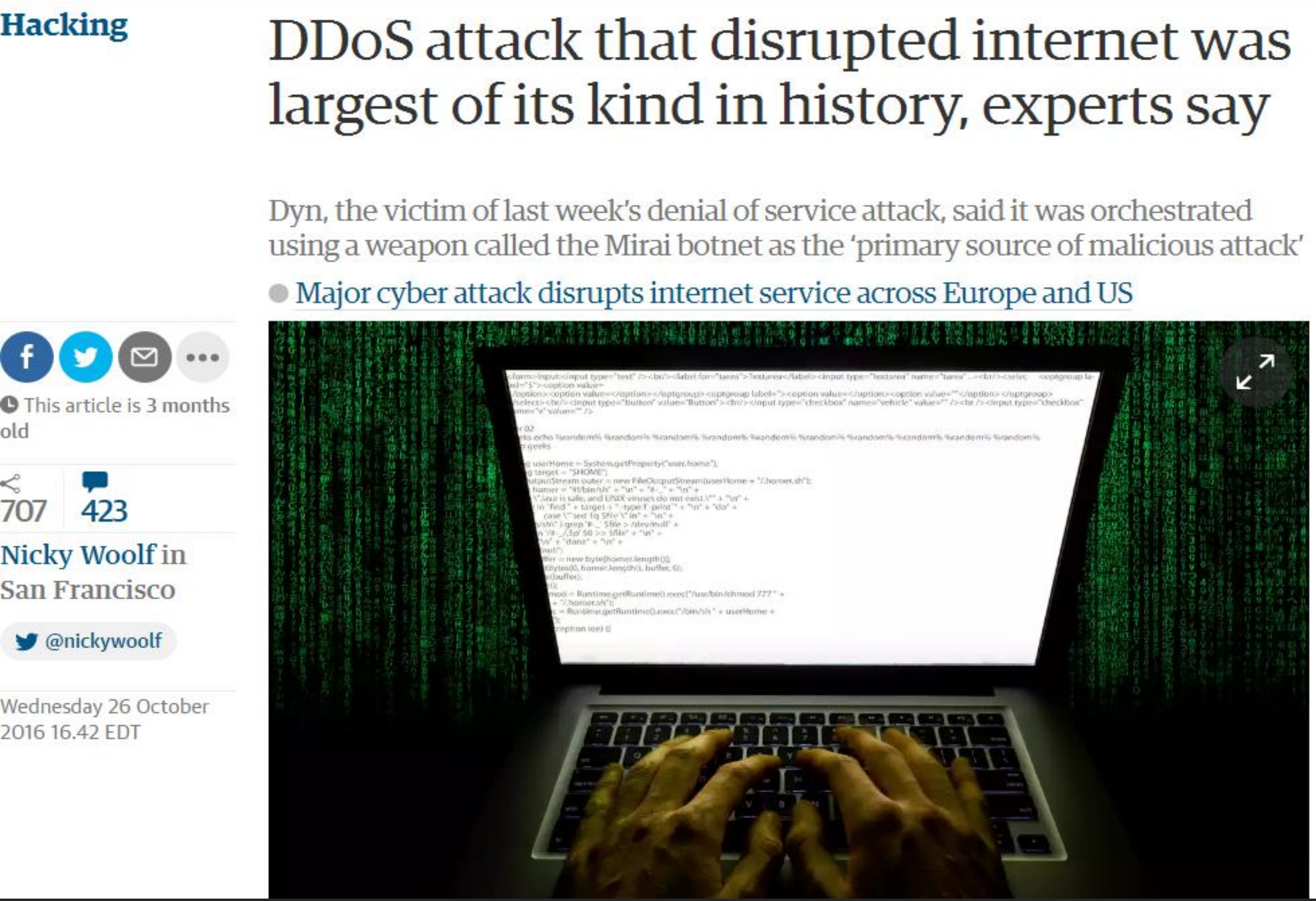


NotPetya cyber attack on TNT Express cost FedEx $300m

Falling victim to global ransomware attack "posed significant operational challenges", the company says in its latest financial report.

By Danny Palmer | September 20, 2017 -- 16:12 GMT (09:12 PDT) | Topic: Security

Large Scale Outages



Hacking

DDoS attack that disrupted internet was largest of its kind in history, experts say

Dyn, the victim of last week's denial of service attack, said it was orchestrated using a weapon called the Mirai botnet as the 'primary source of malicious attack'

- Major cyber attack disrupts internet service across Europe and US

This article is 3 months old

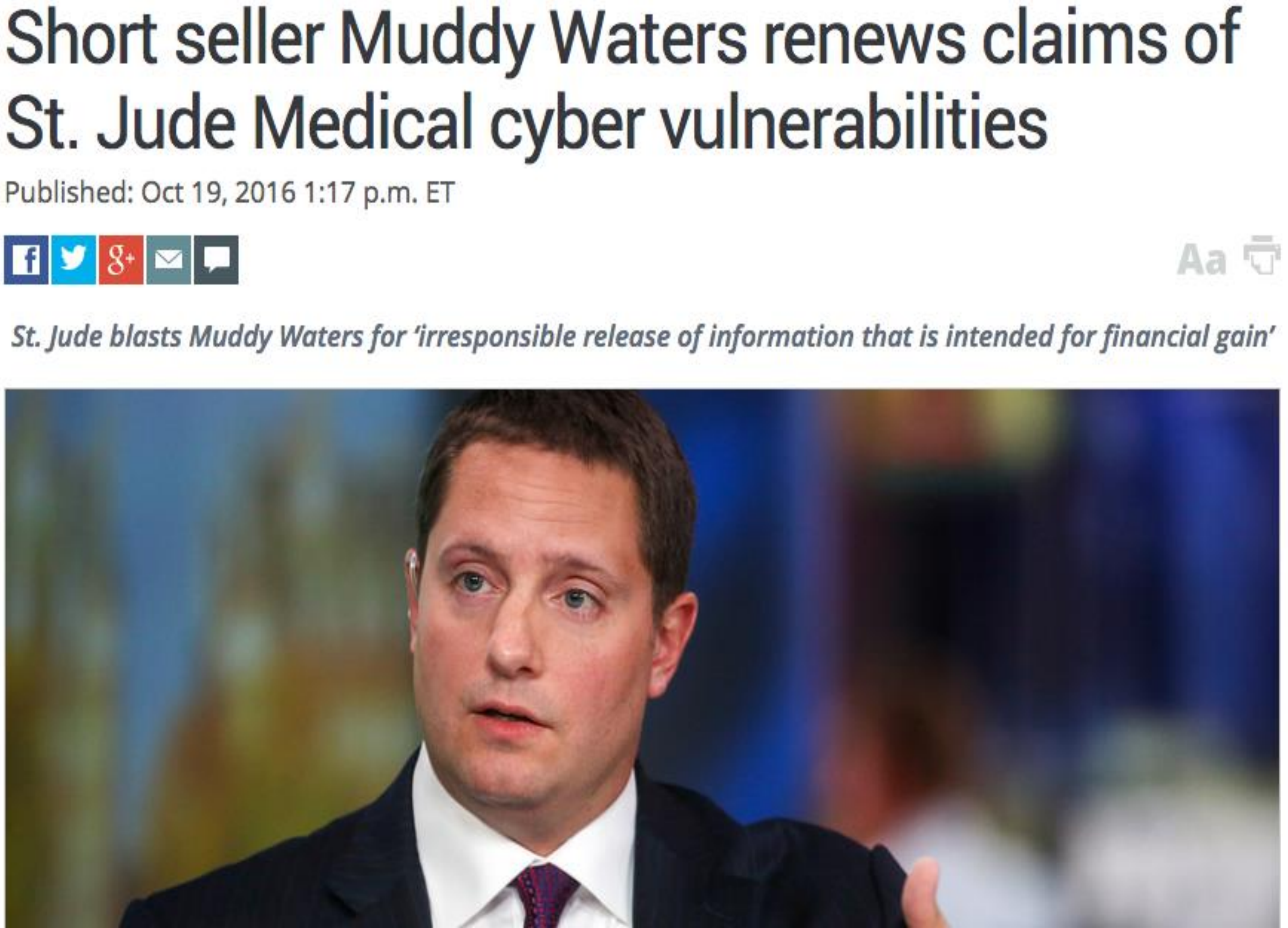
707 423

Nicky Woolf in San Francisco

@nickywoolf

Wednesday 26 October 2016 16.42 EDT

Cyber Impacting Financials?

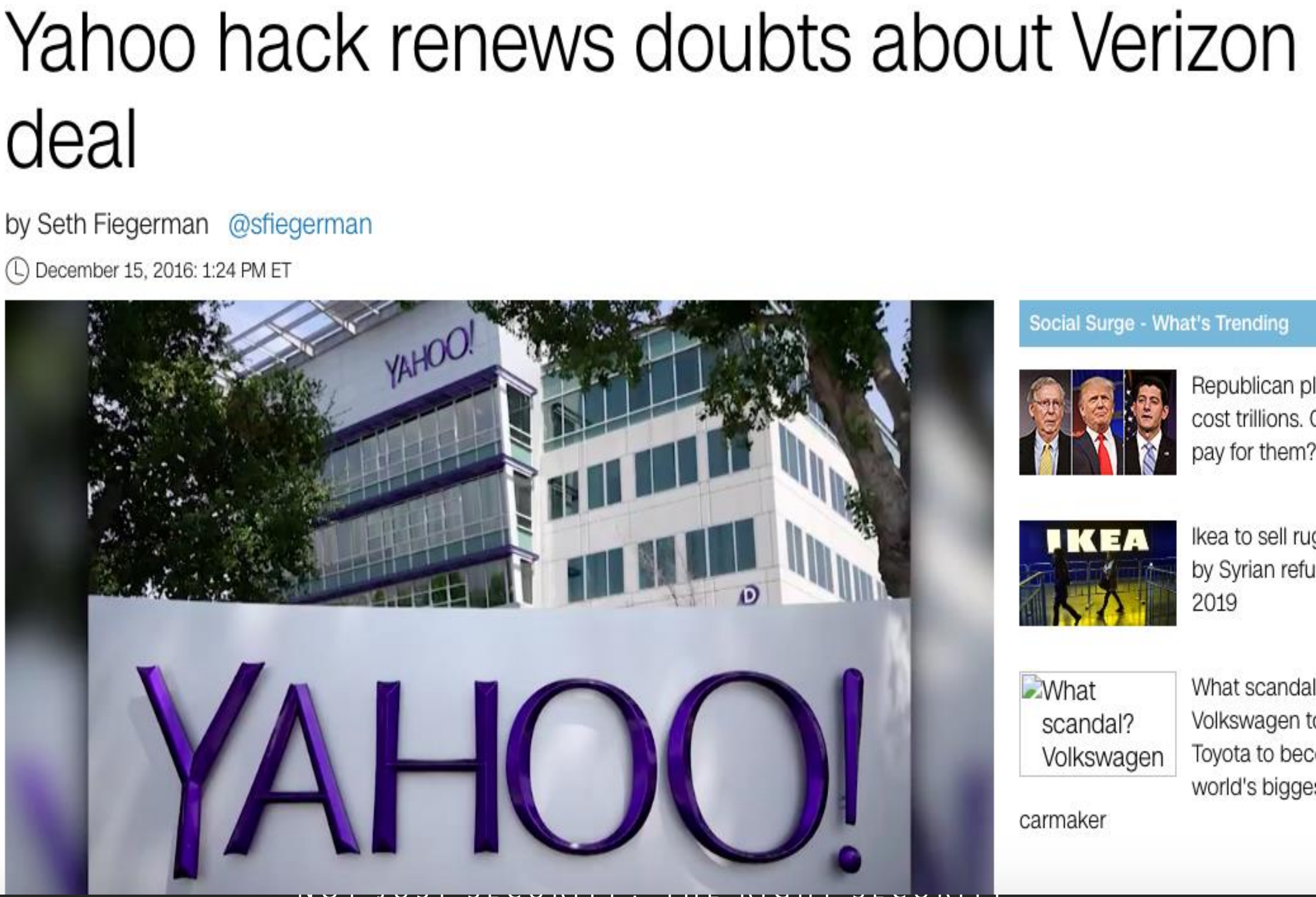


Short seller Muddy Waters renews claims of St. Jude Medical cyber vulnerabilities

Published: Oct 19, 2016 1:17 p.m. ET

St. Jude blasts Muddy Waters for 'irresponsible release of information that is intended for financial gain'

Cyber Impacting Financials?



Yahoo hack renews doubts about Verizon deal

by Seth Fiegerman @sfiegerman

December 15, 2016: 1:24 PM ET

Social Surge - What's Trending

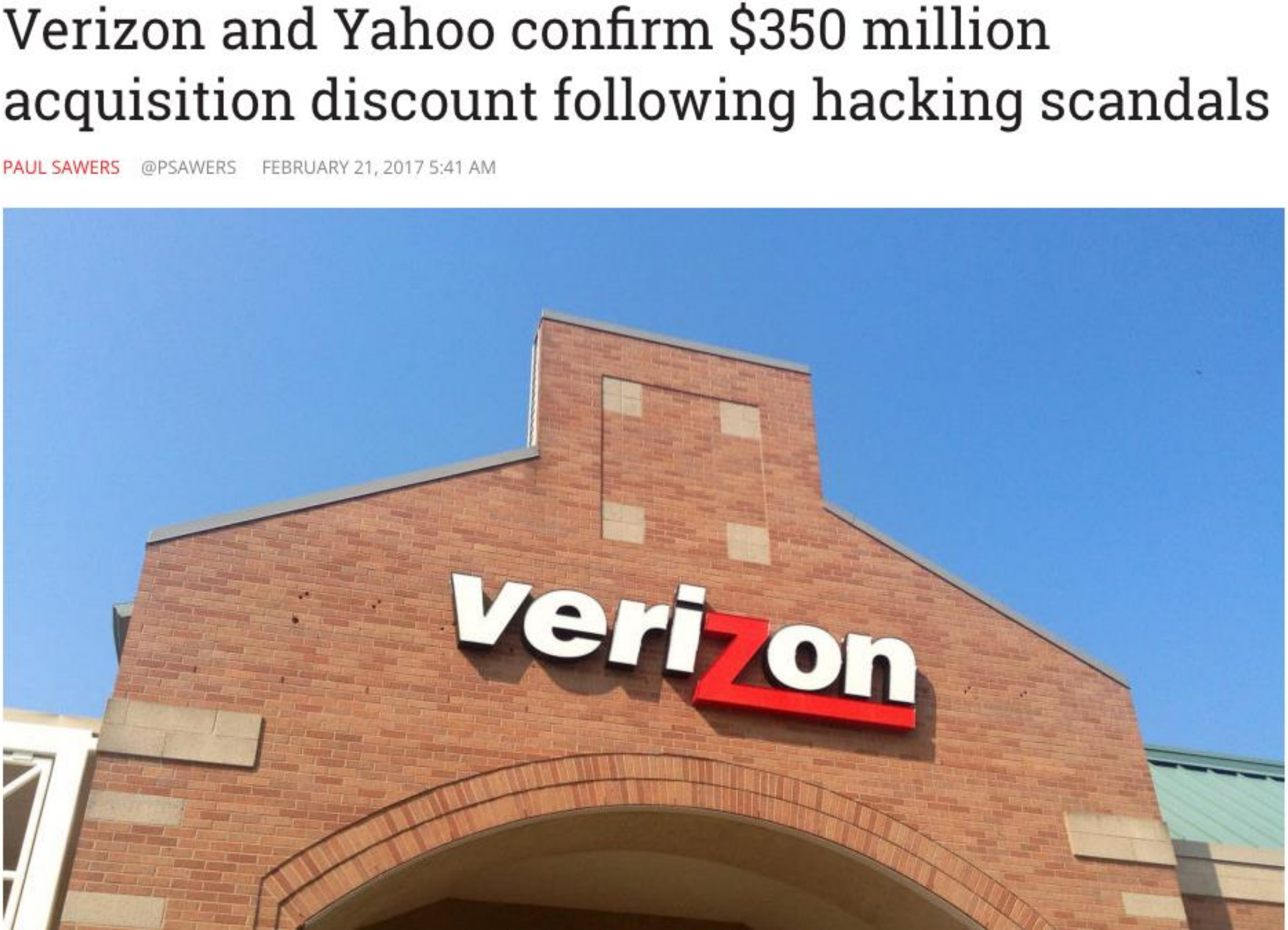
Republican pl
cost trillions. C
pay for them?

Ikea to sell rug
by Syrian refu
2019

What
scandal?
Volkswagen

What scandal
Volkswagen to
Toyota to bec
world's bigges
carmaker

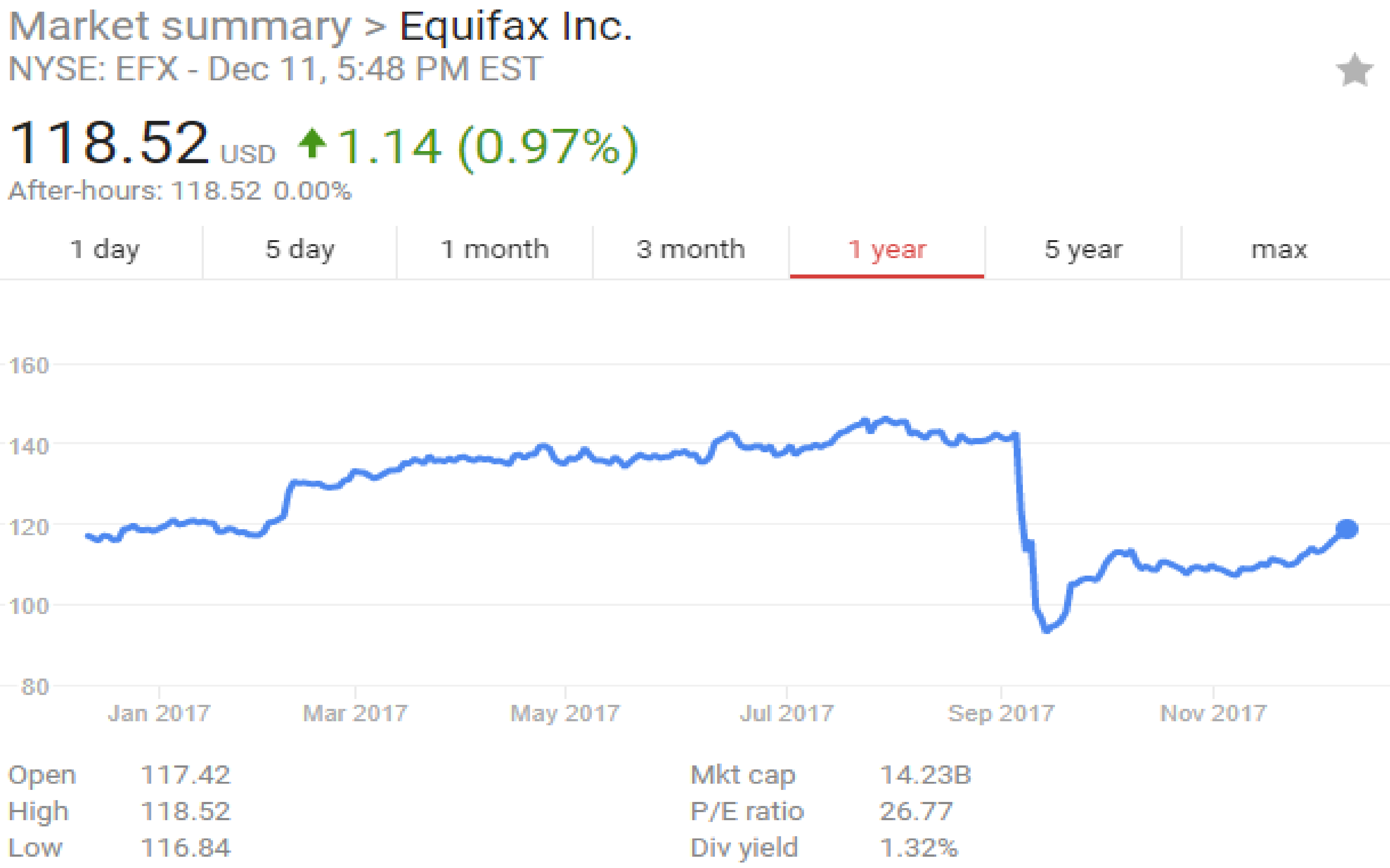
Cyber Impacting Financials – Only $350M



Verizon and Yahoo confirm $350 million acquisition discount following hacking scandals

PAUL SAWERS @PSAWERS FEBRUARY 21, 2017 5:41 AM

Cyber Impacting Financials – Equifax



Market summary > Equifax Inc.

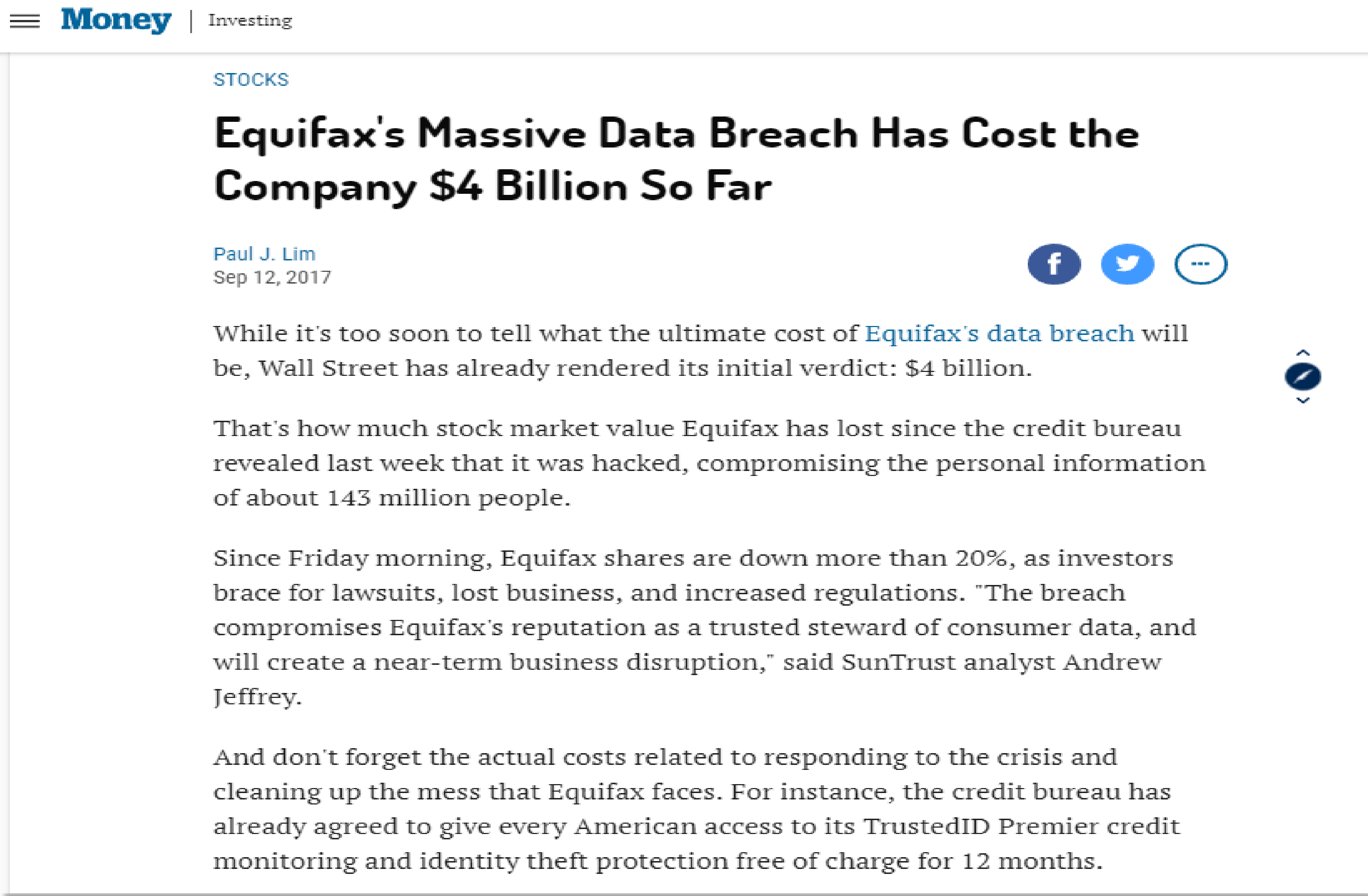
NYSE: EFX - Dec 11, 5:48 PM EST

118.52 USD ↑ 1.14 (0.97%)

After-hours: 118.52 0.00%

Open	117.42	Mkt cap	14.23B
High	118.52	P/E ratio	26.77
Low	116.84	Div yield	1.32%

Cyber Impacting Financials – Equifax



STOCKS

Equifax's Massive Data Breach Has Cost the Company $4 Billion So Far

Paul J. Lim
Sep 12, 2017

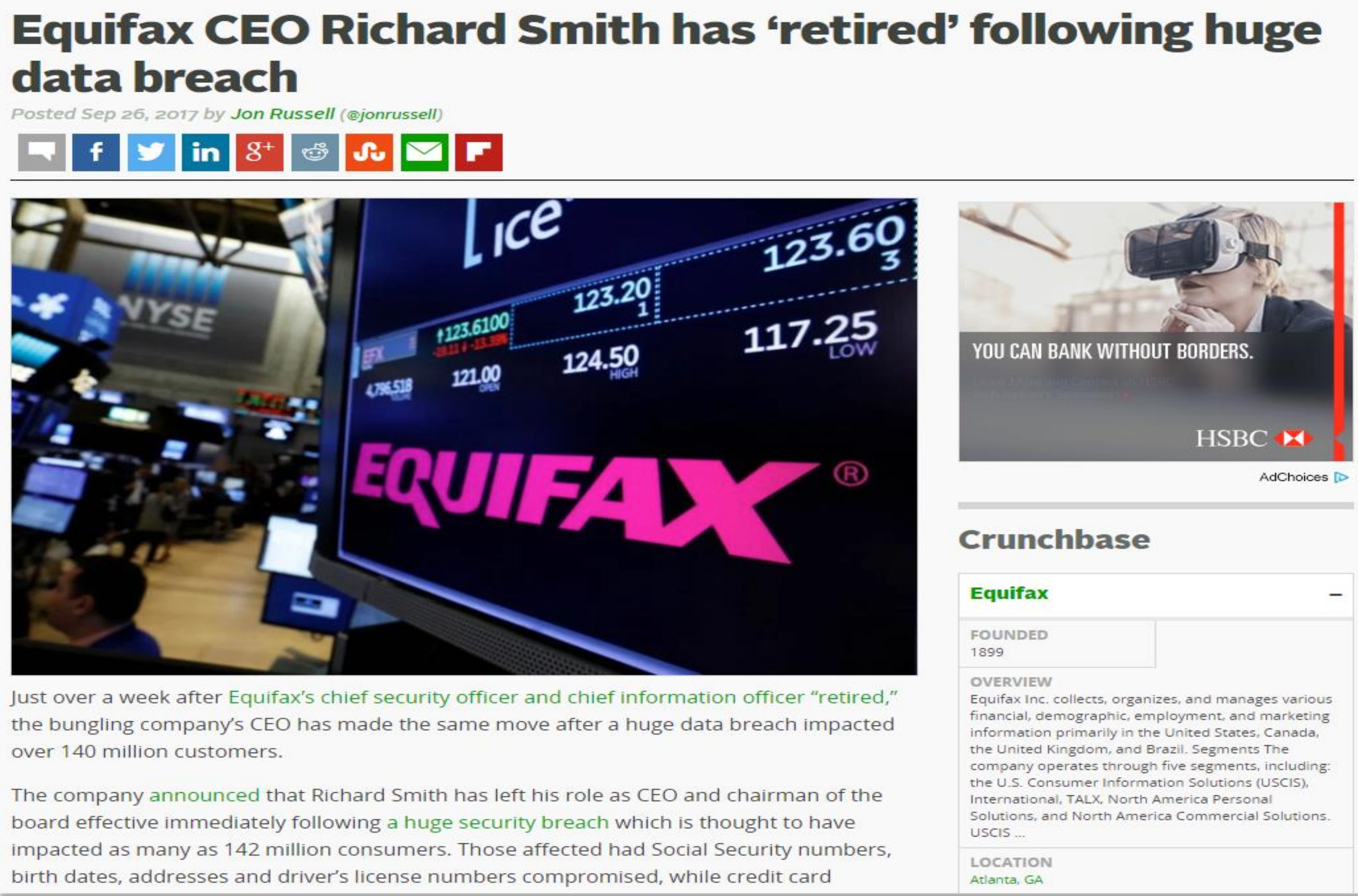
While it's too soon to tell what the ultimate cost of Equifax's data breach will be, Wall Street has already rendered its initial verdict: $4 billion.

That's how much stock market value Equifax has lost since the credit bureau revealed last week that it was hacked, compromising the personal information of about 143 million people.

Since Friday morning, Equifax shares are down more than 20%, as investors brace for lawsuits, lost business, and increased regulations. "The breach compromises Equifax's reputation as a trusted steward of consumer data, and will create a near-term business disruption," said SunTrust analyst Andrew Jeffrey.

And don't forget the actual costs related to responding to the crisis and cleaning up the mess that Equifax faces. For instance, the credit bureau has already agreed to give every American access to its TrustedID Premier credit monitoring and identity theft protection free of charge for 12 months.

Cyber Impacting Financials – Equifax



Equifax CEO Richard Smith has ‘retired’ following huge data breach

Posted Sep 26, 2017 by Jon Russell (@jonrussell)

Just over a week after Equifax’s chief security officer and chief information officer “retired,” the bungling company’s CEO has made the same move after a huge data breach impacted over 140 million customers.

The company announced that Richard Smith has left his role as CEO and chairman of the board effective immediately following a huge security breach which is thought to have impacted as many as 142 million consumers. Those affected had Social Security numbers, birth dates, addresses and driver’s license numbers compromised, while credit card

Crunchbase

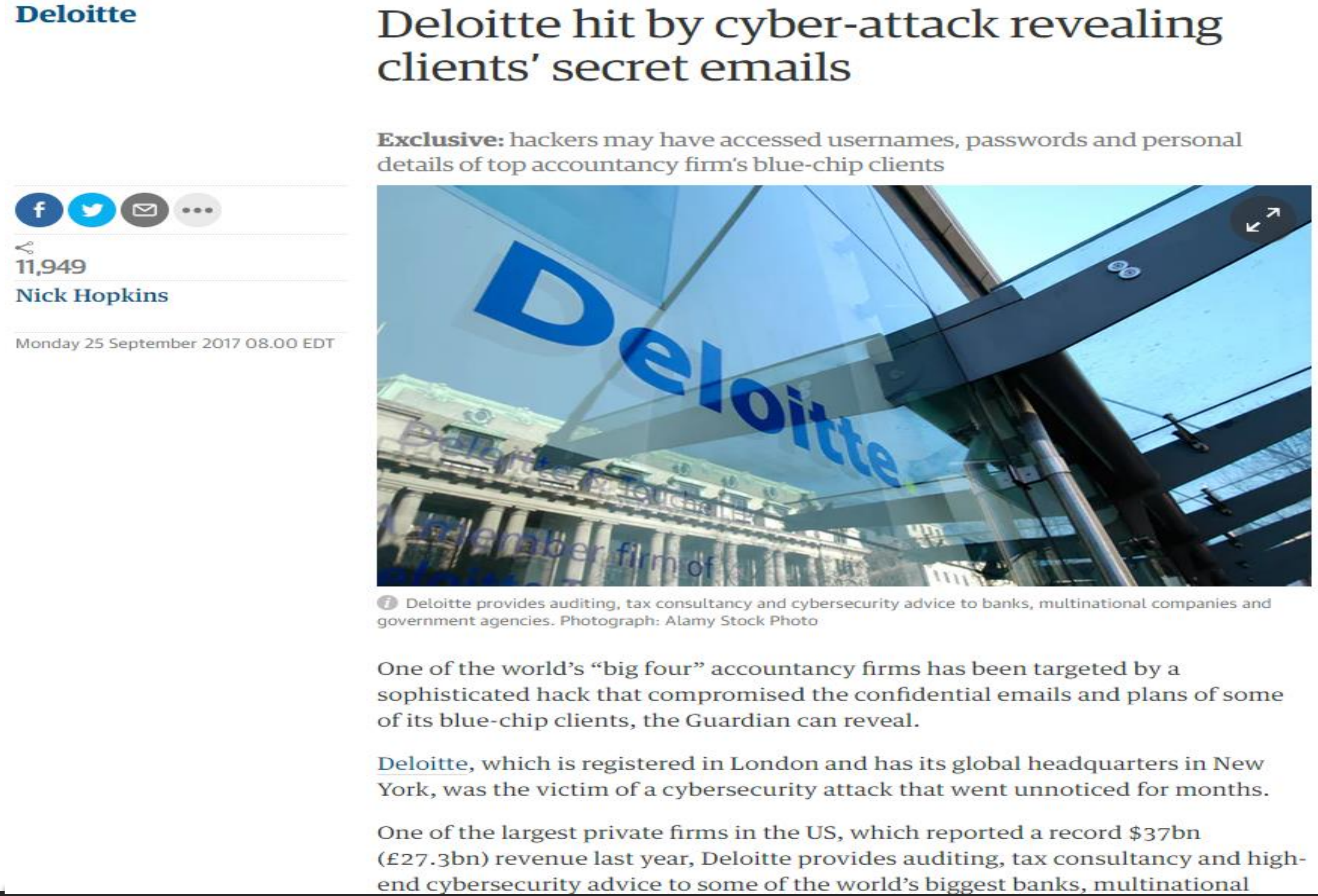
Equifax –

FOUNDED
1899

OVERVIEW
Equifax Inc. collects, organizes, and manages various financial, demographic, employment, and marketing information primarily in the United States, Canada, the United Kingdom, and Brazil. Segments The company operates through five segments, including: the U.S. Consumer Information Solutions (USCIS), International, TALX, North America Personal Solutions, and North America Commercial Solutions. USCIS ...

LOCATION
Atlanta, GA

Cyber Impacting Financials – Deloitte



Deloitte

Deloitte hit by cyber-attack revealing clients' secret emails

Exclusive: hackers may have accessed usernames, passwords and personal details of top accountancy firm's blue-chip clients

11,949

Nick Hopkins

Monday 25 September 2017 08.00 EDT

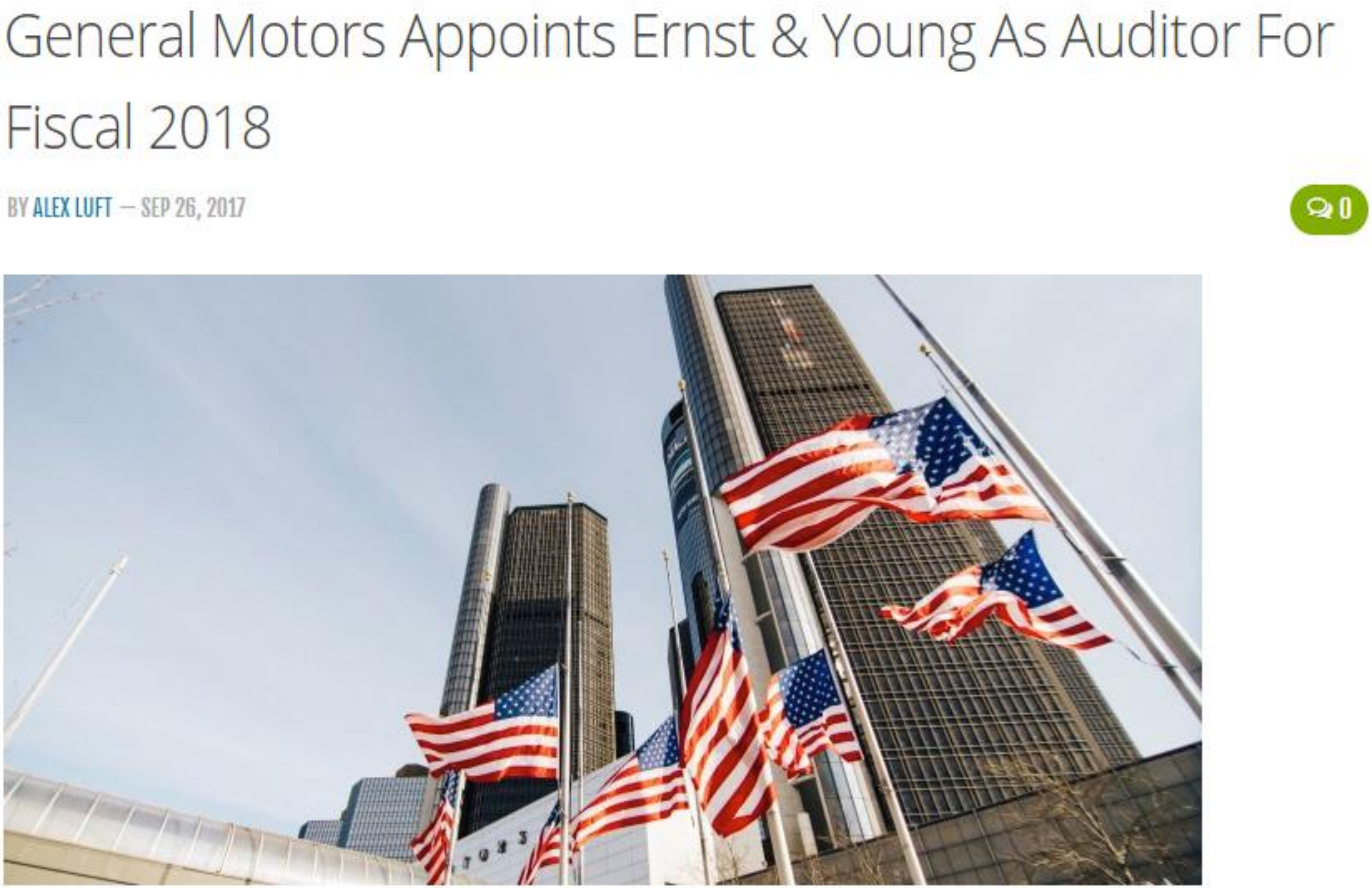
Deloitte provides auditing, tax consultancy and cybersecurity advice to banks, multinational companies and government agencies. Photograph: Alamy Stock Photo

One of the world's "big four" accountancy firms has been targeted by a sophisticated hack that compromised the confidential emails and plans of some of its blue-chip clients, the Guardian can reveal.

Deloitte, which is registered in London and has its global headquarters in New York, was the victim of a cybersecurity attack that went unnoticed for months.

One of the largest private firms in the US, which reported a record $37bn (£27.3bn) revenue last year, Deloitte provides auditing, tax consultancy and high-end cybersecurity advice to some of the world's biggest banks, multinational

Cyber Impacting Financials – Deloitte



General Motors Appoints Ernst & Young As Auditor For Fiscal 2018

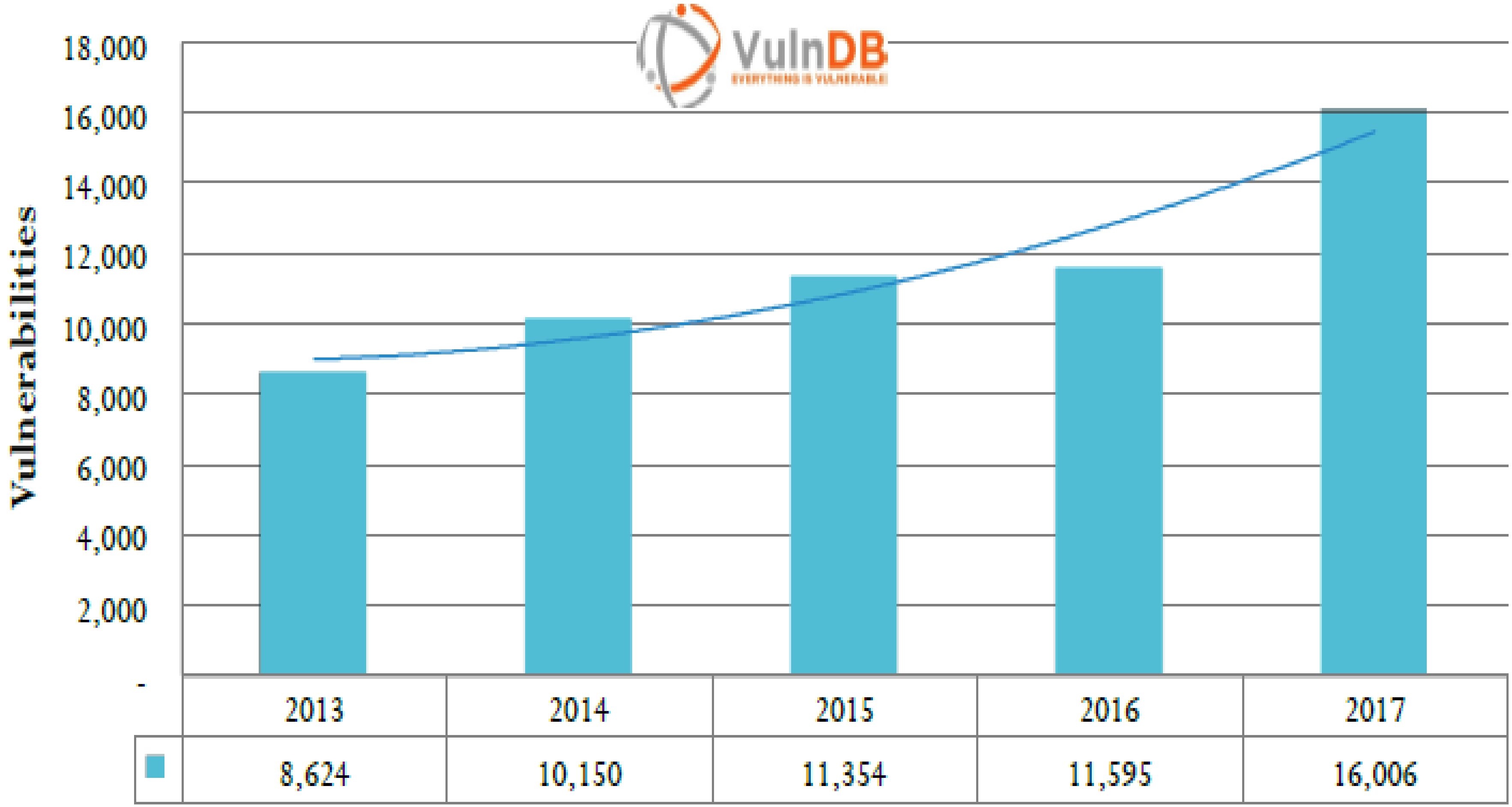
BY ALEX LUFT — SEP 26, 2017

2017 YTD Vulnerabilities

Statistics

2017 YTD - Vulnerabilities

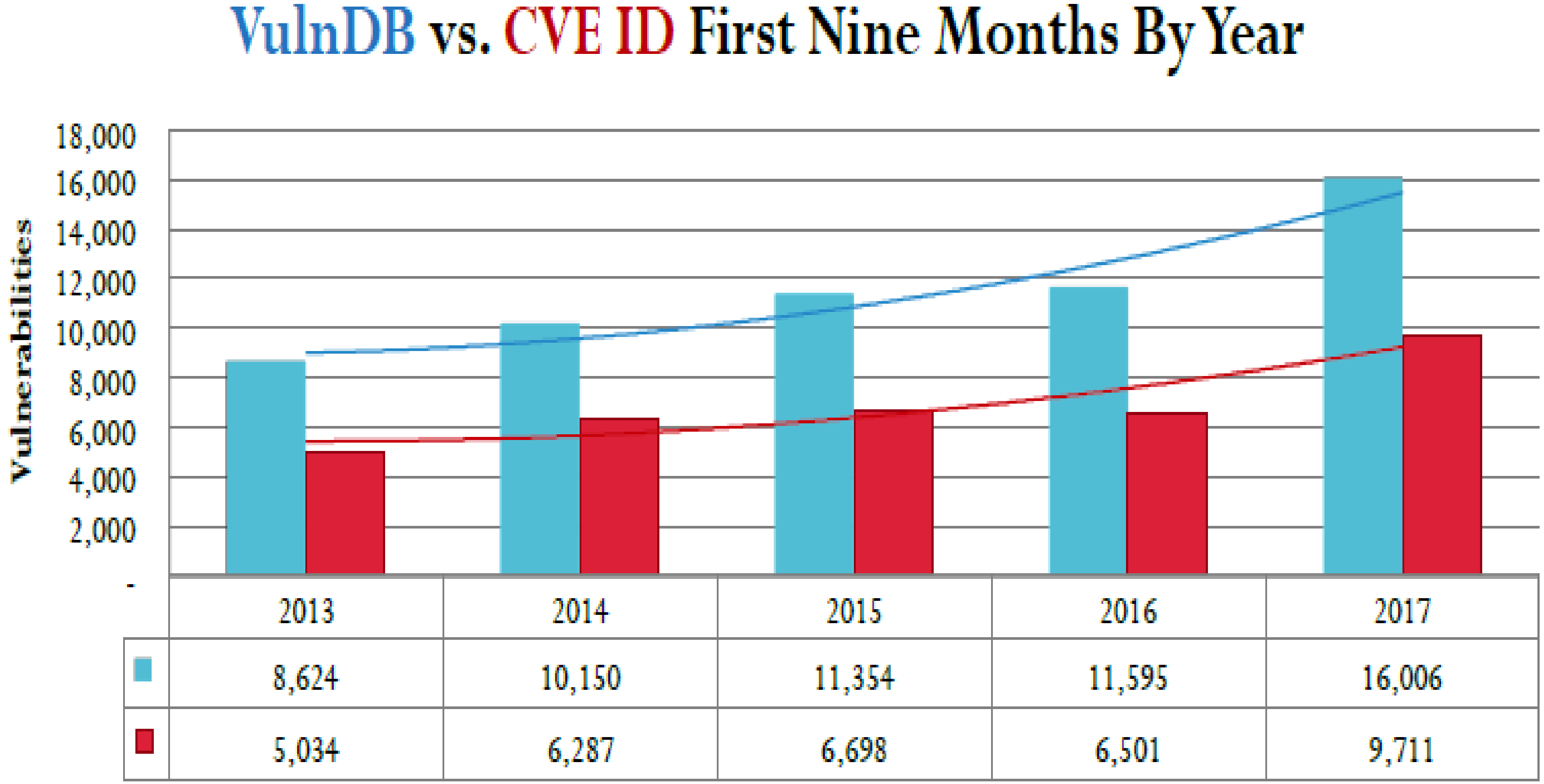
First Nine Months of 2017 Compared to the Same Period for the Past Four Years



	2013	2014	2015	2016	2017
🟦	8,624	10,150	11,354	11,595	16,006

2017 YTD - Vulnerabilities

First Nine Months of Comparisons

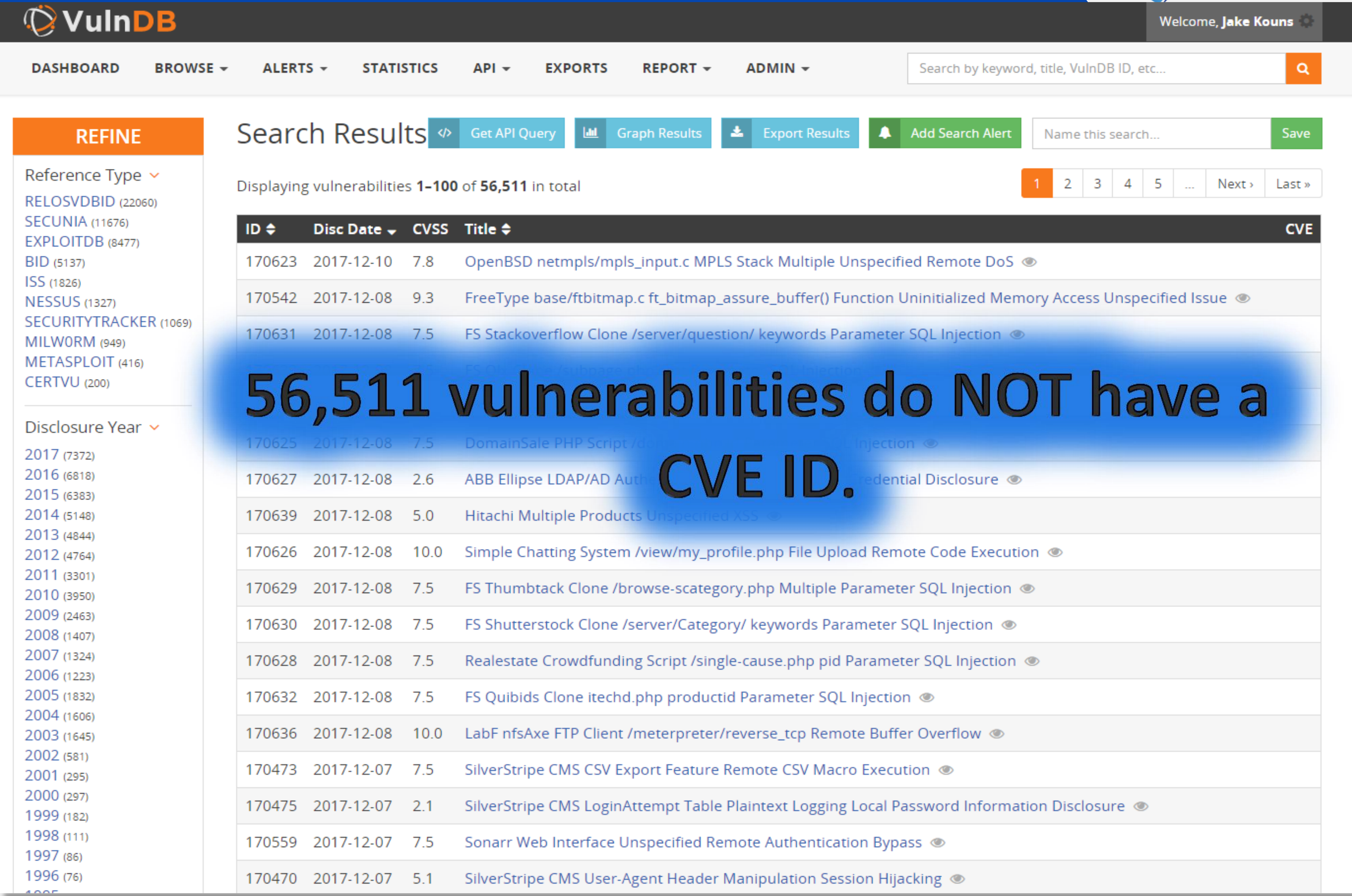


VulnDB vs. CVE ID First Nine Months By Year

	2013	2014	2015	2016	2017
🟦	8,624	10,150	11,354	11,595	16,006
🟥	5,034	6,287	6,698	6,501	9,711

2017 YTD - Vulnerabilities

RiskBased SECURITY



Search Results

Displaying vulnerabilities **1-100** of **56,511** in total

Reference Type

RELOSVDBID	(22060)
SECUNIA	(11676)
EXPLOITDB	(8477)
BID	(5137)
ISS	(1826)
NESSUS	(1327)
SECURITYTRACKER	(1069)
MILW0RM	(949)
METASPLOIT	(416)
CERTVU	(200)

Disclosure Year

2017	(7372)
2016	(6818)
2015	(6383)
2014	(5148)
2013	(4844)
2012	(4764)
2011	(3301)
2010	(3950)
2009	(2463)
2008	(1407)
2007	(1324)
2006	(1223)
2005	(1832)
2004	(1606)
2003	(1645)
2002	(581)
2001	(295)
2000	(297)
1999	(182)
1998	(111)
1997	(86)
1996	(76)

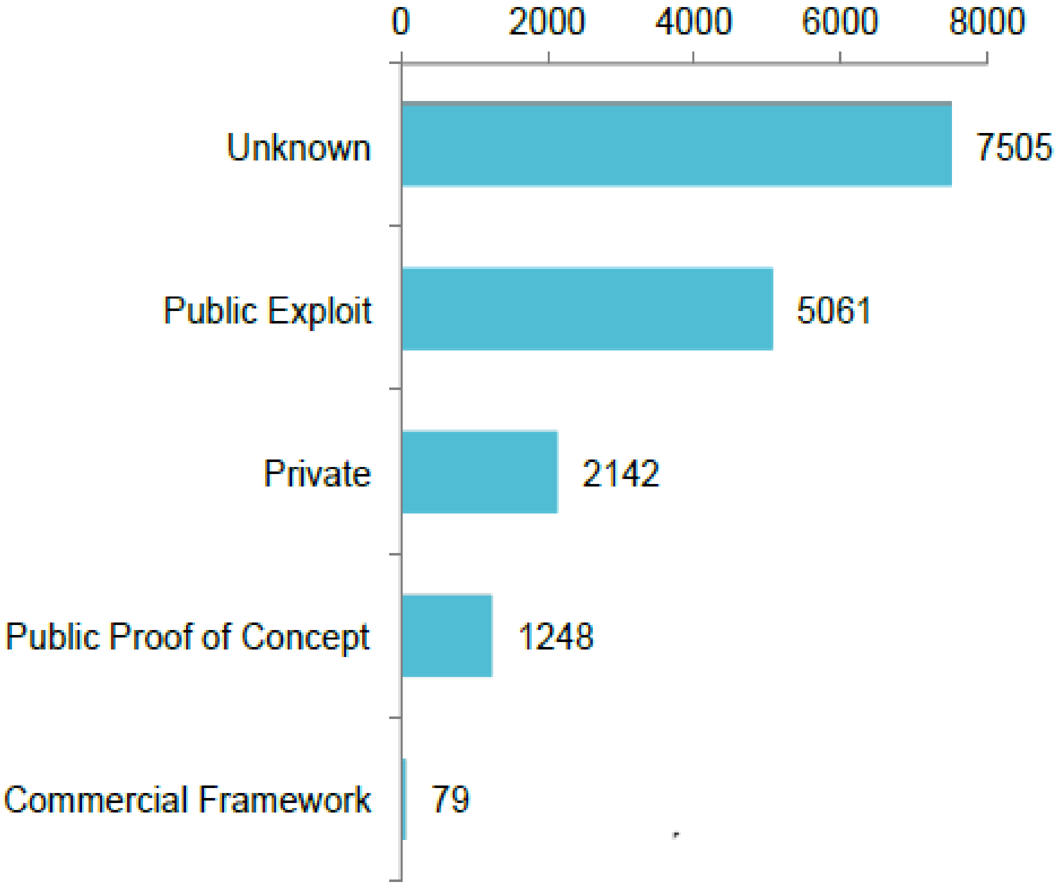
ID	Disc Date	CVSS	Title	CVE
170623	2017-12-10	7.8	OpenBSD netmpls/mpls_input.c MPLS Stack Multiple Unspecified Remote DoS	
170542	2017-12-08	9.3	FreeType base/ftbitmap.c ft_bitmap_assure_buffer() Function Uninitialized Memory Access Unspecified Issue	
170631	2017-12-08	7.5	FS Stackoverflow Clone /server/question/ keywords Parameter SQL Injection	
[illegible]	[illegible]	[illegible]	FS Olx Clone /subpage.php [illegible] SQL Injection	
[illegible]	[illegible]	[illegible]	[illegible]	
170625	2017-12-08	7.5	DomainSale PHP Script /do[illegible]L Injection	
170627	2017-12-08	2.6	ABB Ellipse LDAP/AD Auth[illegible]redential Disclosure	
170639	2017-12-08	5.0	Hitachi Multiple Products Unspecified XSS	
170626	2017-12-08	10.0	Simple Chatting System /view/my_profile.php File Upload Remote Code Execution	
170629	2017-12-08	7.5	FS Thumbtack Clone /browse-scategory.php Multiple Parameter SQL Injection	
170630	2017-12-08	7.5	FS Shutterstock Clone /server/Category/ keywords Parameter SQL Injection	
170628	2017-12-08	7.5	Realestate Crowdfunding Script /single-cause.php pid Parameter SQL Injection	
170632	2017-12-08	7.5	FS Quibids Clone itechd.php productid Parameter SQL Injection	
170636	2017-12-08	10.0	LabF nfsAxe FTP Client /meterpreter/reverse_tcp Remote Buffer Overflow	
170473	2017-12-07	7.5	SilverStripe CMS CSV Export Feature Remote CSV Macro Execution	
170475	2017-12-07	2.1	SilverStripe CMS LoginAttempt Table Plaintext Logging Local Password Information Disclosure	
170559	2017-12-07	7.5	Sonarr Web Interface Unspecified Remote Authentication Bypass	
170470	2017-12-07	5.1	SilverStripe CMS User-Agent Header Manipulation Session Hijacking	

56,511 vulnerabilities do NOT have a CVE ID.

2017 YTD - Vulnerabilities

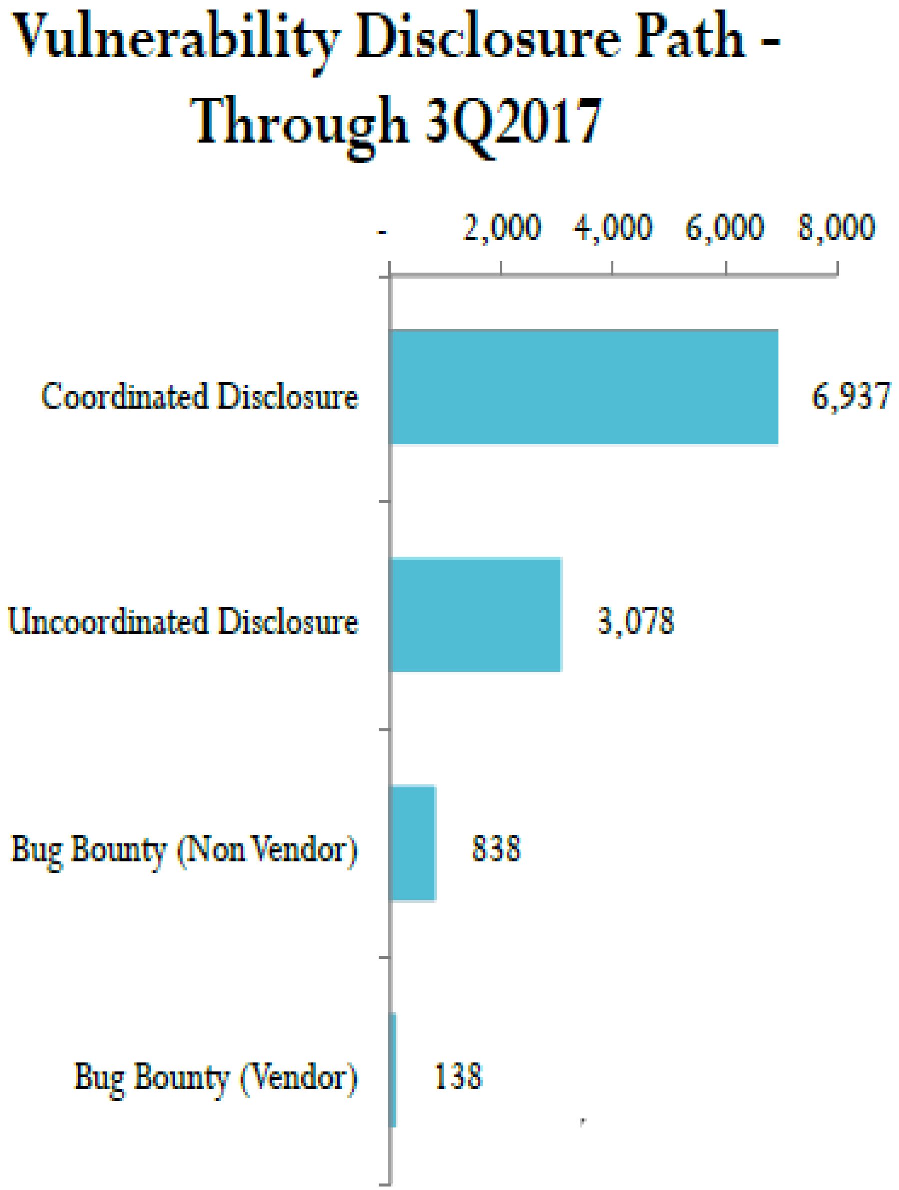
RiskBased SECURITY

Exploit Classification - First Nine Months of 2017



53.1% of all vulnerabilities either had exploits available or sufficient details published to generate a functioning exploit.

2017 YTD - Vulnerabilities



43.3% of 2017 vulnerabilities were coordinated with the Vendor; Just 6.1% were the result of vendor or third-party bug bounties.

Vulnerability and Timeline Exposure Metrics (VTEM)

Vulnerability Timeline and Exposure Metrics (VTEM)

A framework that defines and provides guidance for vulnerability timeline tracking and metric calculations to assist in the evaluation of Vendors and Products as well as understand an organization's exposure.

Why should you care?

1) The metrics will help you evaluate and select **vendors** to work with that care about security!
   - In turn, forcing vendors to focus on actually producing secure products!

2) It will help you truly understand your organization’s exposure and which products are the biggest offenders.

What Do We Want To Accomplish With VTEM?

- Define timeline and exposure terminology that allows consistent usage for:
  - For Organizations
  - For Researcher
  - For Software Vendors
- Define expectations from CERTs, Software Vendors and Researchers on what must be included in vulnerability disclosure

What Do We Want To Accomplish With VTEM?

- Provide a framework to assist organizations with:
  - Understanding their own time of exposure
  - Identify vendors and products that are contributing to an organization's time of exposure
  - Create a scorecard to allow the monitoring of how vendors are performing
  - Assist organizations with understanding exposure metrics that will enable better decision making to choose secure products

VTEM - Dates

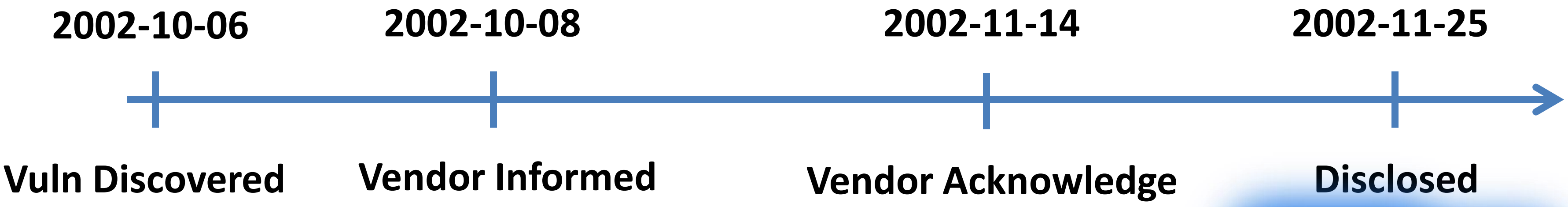
Date	Description
Introduced Date	The date the vulnerability was introduced into a product, or website.
Discovery Date	The date the vulnerability was actually discovered, if available.
Vendor Informed Date	The date the vendor was notified of vulnerability, if available.
Vendor Acknowledge Date	The date the vendor acknowledged the report or vulnerability, if available.
Vendor Solution Date	The date the vendor provided an actionable solution to resolve the vulnerability, if available.
Disclosure Date	The date the vulnerability was publicly disclosed.
Third-Party Solution Date	The date a third-party, not the vendor, provided an actionable solution to resolve the issue, if available.
Exploit Publish Date	The date a functional exploit was publicly disclosed, if available.
Solution Implemented Date	The date the vulnerability has been resolved at an organization, either with a workaround or a patch.

Vendor Response Time

- To demonstrate the vendors response time from being informed to responding to a researcher. This is only the initial response, but not an automated response.
- <Vendor Acknowledge Date> – <Vendor Informed Date>

EXAMPLE

- Netscreen ScreenOS Malicioius-URL Bypass (CVE-2002-2234)



2002-10-06

Vuln Discovered

2002-10-08

Vendor Informed

2002-11-14

Vendor Acknowledge

2002-11-25

Disclosed

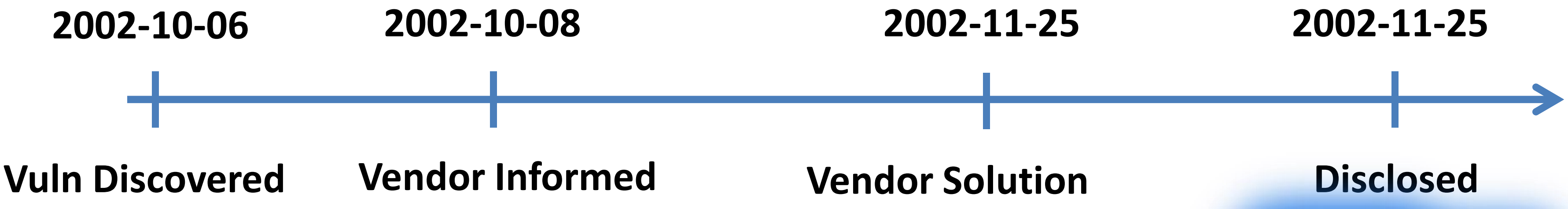
37 Days

Time To Patch

- To demonstrate the vendors response time from being informed of a vulnerability until to having a working fix published for customers.
- <Vendor Solution Date> – <Vendor Informed Date>

EXAMPLE

- Netscreen ScreenOS Malicioius-URL Bypass (CVE-2002-2234)



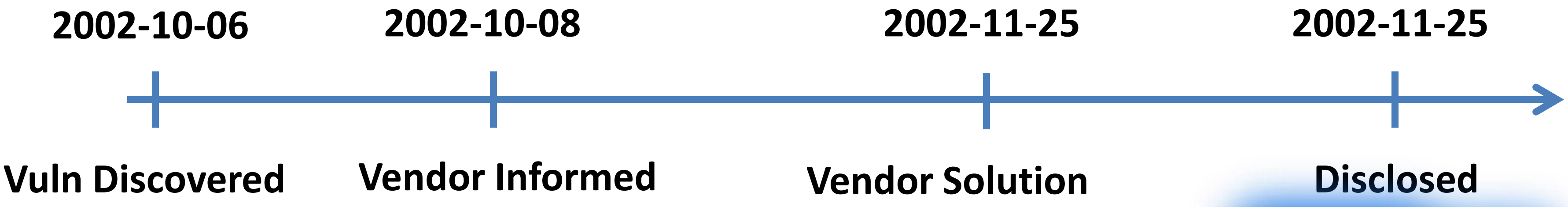
48 Days

Total Time To Patch

- To demonstrate the total time from a vulnerability is discovered until a working fix is published for customers.
- <Vendor Solution Date> – <Vulnerability Discovery Date>

EXAMPLE

- Netscreen ScreenOS Malicioius-URL Bypass (CVE-2002-2234)



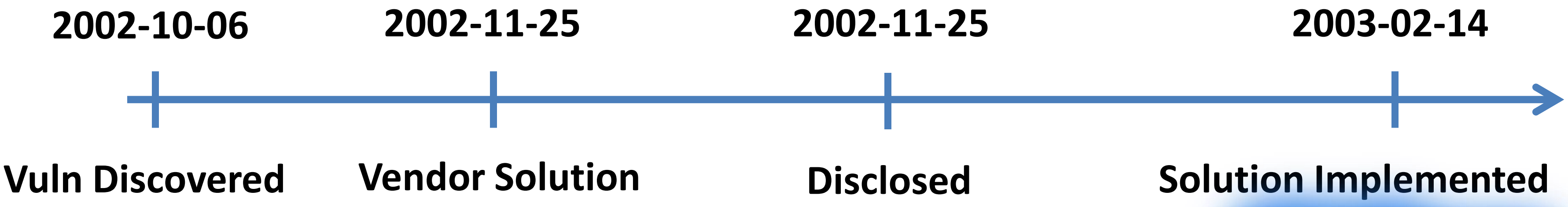
50 Days

Time of Exposure

- To demonstrate the time of exposure an organization is vulnerable from when a working fix is published for customers until the solution is implemented.
- <Solution Implemented Date> - <Vendor Solution Date>

EXAMPLE

- Netscreen ScreenOS Malicioius-URL Bypass (CVE-2002-2234)
- Assume Evil Corp patches next quarterly maintenance window



2002-10-06 — Vuln Discovered

2002-11-25 — Vendor Solution

2002-11-25 — Disclosed

2003-02-14 — Solution Implemented

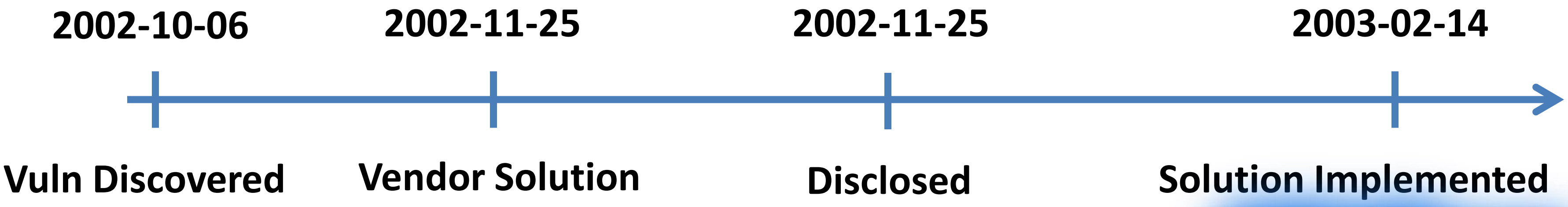
81 Days

Total Time of Exposure

- To demonstrate the total time of exposure an organization is vulnerable from when the issues is discovered until the solution is implemented.
- <Solution Implemented Date> - <Vulnerability Discovery Date>

EXAMPLE

- Netscreen ScreenOS Malicioius-URL Bypass (CVE-2002-2234)
- Assume Evil Corp patches next quarterly maintenance window



131 Days

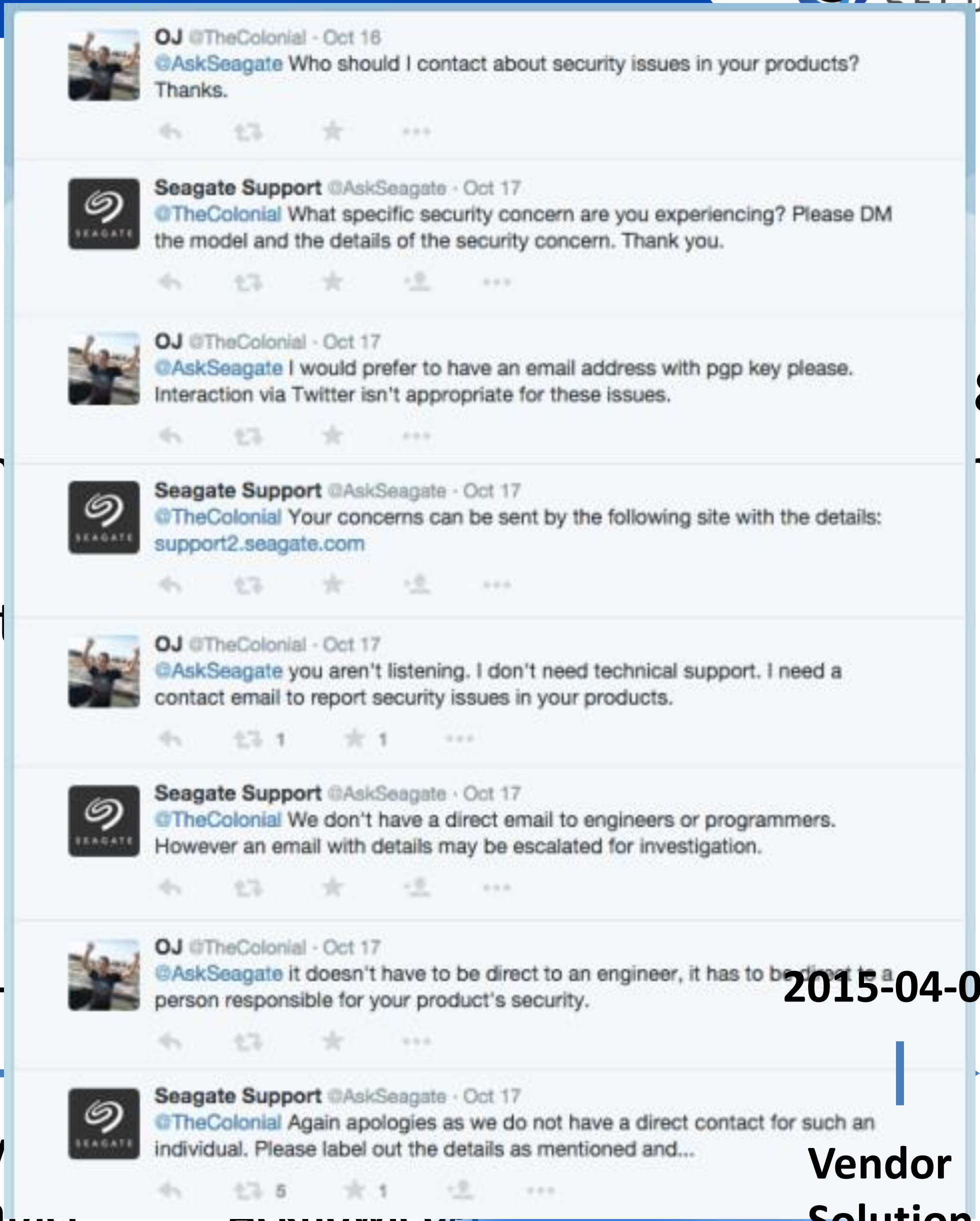
Netscreen ScreenOS Malicioius-URL Bypass (CVE-2002-2234)

VTEM Metric	Number Of Days
Vendor Response Time	37 Days
Time To Patch	48 Days
Total Time To Patch	50 Days
Time Of Exposure	81 Days
Total Time Of Exposure	131 Days

Vendor

EXAMPLE

- Seagate NAS Remote Code … 87)
- Vendor responses were tim… n delay
- Researcher ultimately ident… LinkedIn to report issue



OJ @TheColonial · Oct 16
@AskSeagate Who should I contact about security issues in your products? Thanks.

Seagate Support @AskSeagate · Oct 17
@TheColonial What specific security concern are you experiencing? Please DM the model and the details of the security concern. Thank you.

OJ @TheColonial · Oct 17
@AskSeagate I would prefer to have an email address with pgp key please. Interaction via Twitter isn't appropriate for these issues.

Seagate Support @AskSeagate · Oct 17
@TheColonial Your concerns can be sent by the following site with the details: support2.seagate.com

OJ @TheColonial · Oct 17
@AskSeagate you aren't listening. I don't need technical support. I need a contact email to report security issues in your products.

Seagate Support @AskSeagate · Oct 17
@TheColonial We don't have a direct email to engineers or programmers. However an email with details may be escalated for investigation.

OJ @TheColonial · Oct 17
@AskSeagate it doesn't have to be direct to an engineer, it has to be direct to a person responsible for your product's security.

Seagate Support @AskSeagate · Oct 17
@TheColonial Again apologies as we do not have a direct contact for such an individual. Please label out the details as mentioned and...

2014-10-07 **2014-10-18** **2015-** **2015-04-01**

Vuln Discovered

Vendor Contact

New V… Contact

…Acknowledge

Vendor Solution

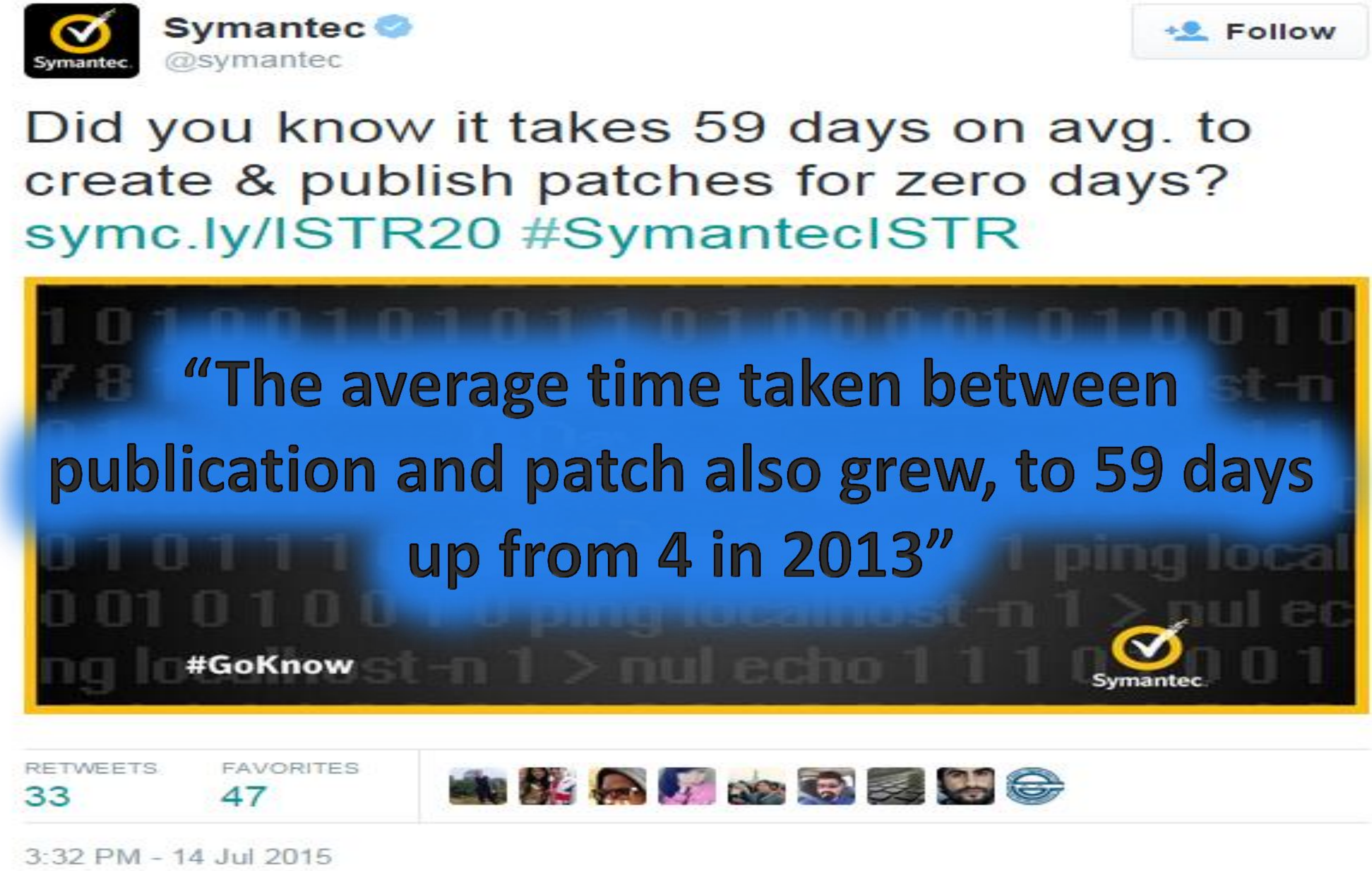
83 Days

Seagate NAS Remote Code Execution Vulnerability (CVE-2014-8687)

VTEM Metric	Number Of Days
Vendor Response Time	83 Days
Time To Patch	164 Days
Total Time To Patch	175 Days
Time Of Exposure	90 Days
Total Time Of Exposure	265 Days

But wait!
There's more!
ICANHASCHEEZBURGER.COM

VTEM



Symantec
@symantec

Follow

Did you know it takes 59 days on avg. to create & publish patches for zero days? symc.ly/ISTR20 #SymantecISTR

"The average time taken between publication and patch also grew, to 59 days up from 4 in 2013"

RETWEETS 33
FAVORITES 47

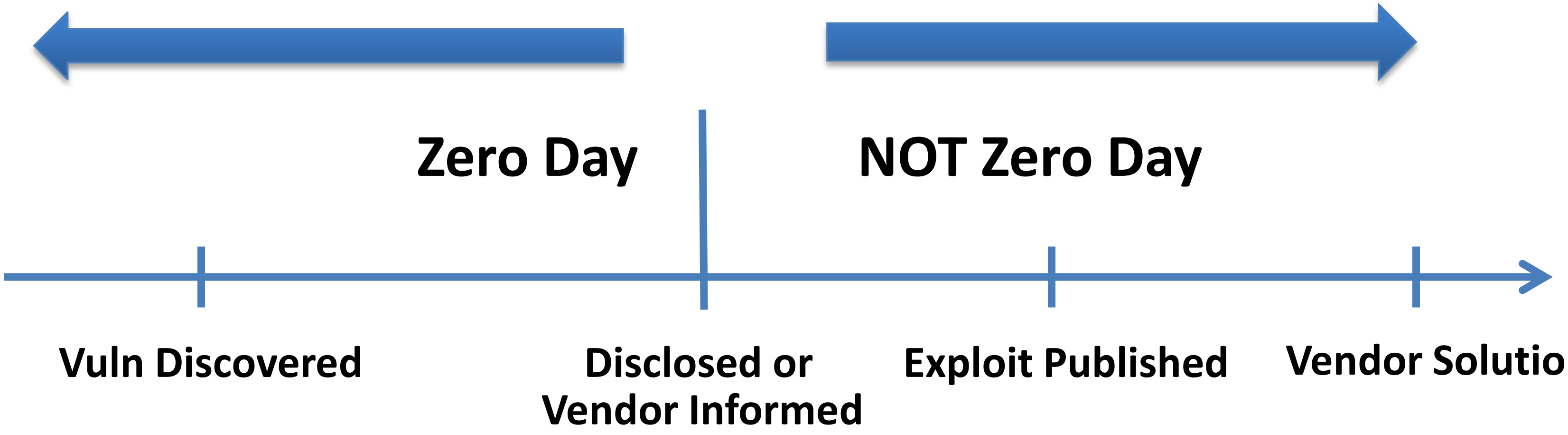
3:32 PM - 14 Jul 2015

What is 0 Day?

- “A zero day vulnerability refers to a hole in software that is unknown to the vendor. “
- “A zero-day (also known as zero-hour or 0-day) vulnerability is an undisclosed and uncorrected computer application vulnerability”
- So many more!

0 DAY

- Can we finally define what 0 day really means based on dates?
- In VTEM framework, we have a few points in time that can assist:
  - Vendor Informed Date
  - Disclosure Date
- 0 Day is when a vendor doesn't know about the Vulnerability and/or it has not been publically disclosed



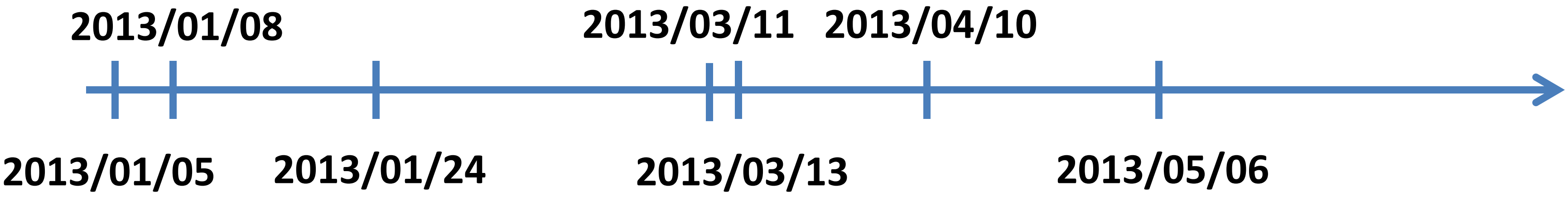
MORE TO VTEM!

- Time to Exploit Availability
- Time of Exploit Exposure
- Research into other variations including:
  - Vulnerability Introduction
  - Third Party Solutions
- Rollup calculations for products and vendors
- Names and calculations argued to death!
- More!

SCADA Time Of Exposure Analysis

VTEM

2013/01/05: RCE vulnerability discovered in ModBus Serial Driver
Used by 11 different products from Schneider Electric
2013/01/08: Vulnerability reported to ICS-CERT
2013/01/24: Schneider Electric confirms vulnerability
2013/03/11: Schneider Electric published security notification with no patch
2013/03/13: ICS-CERT provides status update
2013/04/10: Details published to RBS VulnDB customers
Other vulnerability databases follow suit shortly after
2013/05/06: Publication of detailed vulnerability report by RBS



ICS-CERT provided a warning on April 1, 2014

The vulnerability was discovered by Carsten Eiram on January 5th, 2013

No CVE assigned, anyone relying on NVD was in the dark…

Total Time to Patch

451 Days

Incorre[illegible] advisory
(refers to issue as ‘[illegible]rect CVSSv2 score)

No patch – **or rather one was developed, but the vendor didn’t release it.**

VTEM

- **Time to Patch** and **Total Time To Patch** are metrics defined in **VTEM**.
  - They can be used to evaluate not the security of a piece of software, but the vendors vulnerability response capabilities.
- Unfortunately, not many provide date information required to do these calculations
  - Why not?
  - Why doesn’t ICS-CERT provide the date the vendors were informed of the issue?

VTEM

- As with everything, the amount of time appropriate to spend on addressing an issue depends on:
  - The type of vulnerability (i.e. a simple buffer overflow fix is quicker than something that may require architectural changes)
  - Number of products impacted.
- General consensus is that the vast majority of vulnerabilities should easily be fixed within 180 days (many believe it should be 90 days or less).

VTEM

- We decided to evaluate SCADA vulnerabilities over a two year period, where we would calculate **Total Time to Patch.**
  - 25 Vulnerabilities Analyzed
  - 14 Different Vendors
- **Total Time to Patch** Calculations:
  - Average: 15[illegible]52 Days
  - Mean: 107 Days
  - Max: 451 Days

NERC requires: “Responsible Entity implement a security patch or upgrade within 30 calendar days”

Time of Exposure or Total Time Of Exposure based heavily on vendors and their responsiveness!

Actions

How Do We Solve These ”cyber” Issues?

Vulnerability Intelligence – What Do We Use?

- We need to have proper asset management in place!
- We need to know what software we are running as well as 3rd Party Libraries in order to secure them!
  - You can collect this manually or there are vendor products that can assist!
- Admin or Developer reported documentation is prone to omissions, errors, and lack of updating
- Your legal and ITIL teams are your friends here

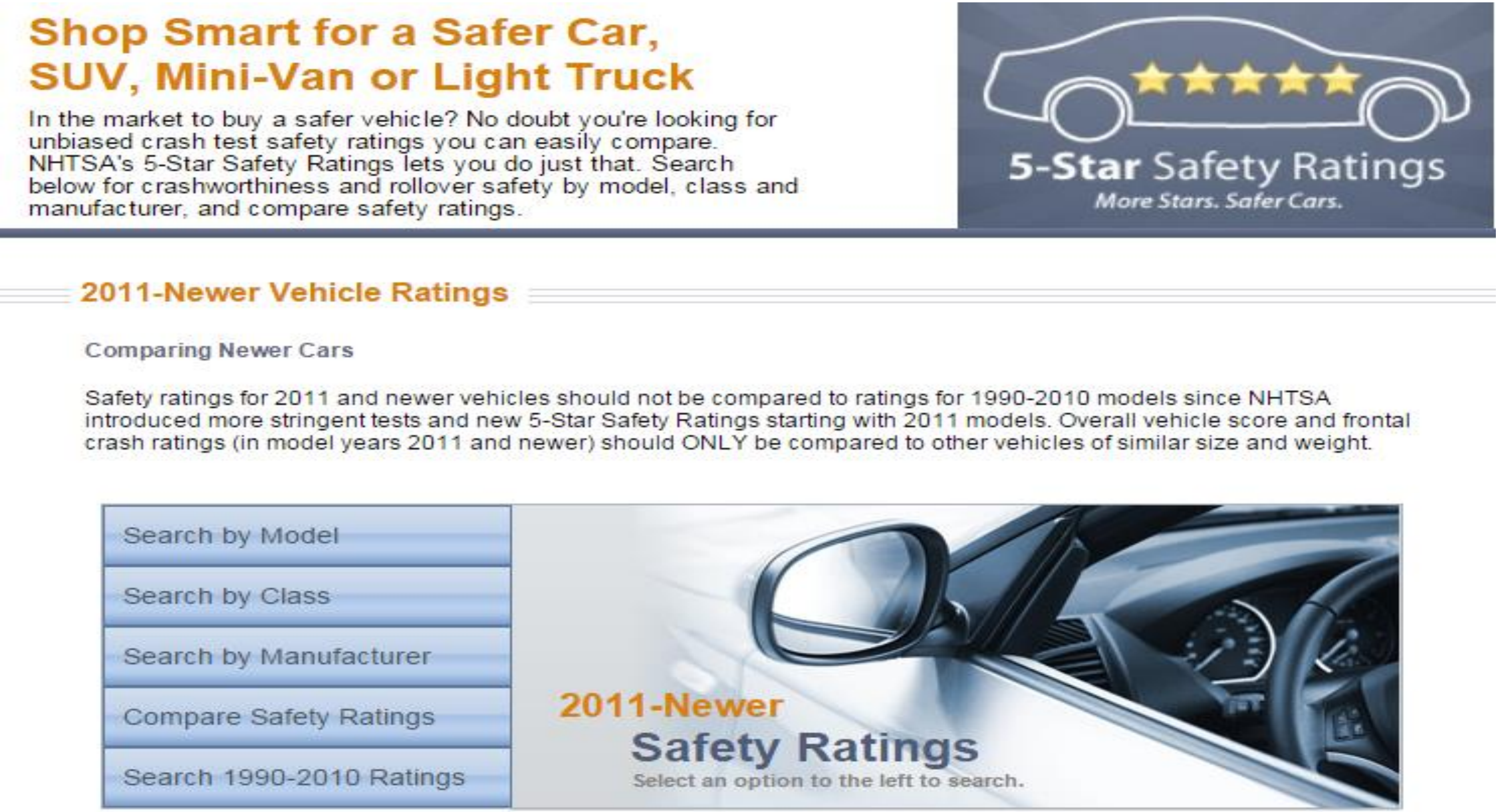
Vulnerability Intelligence – Alerting

- "Whack A Mole" fixing of vulnerabilities is critical, not just in your own code!
- How will you be notified of new issues?
- Why does the cadence of release cycle matter?
  - Too few? Leaves you open to risks, compromise and liability
  - Too many? Huge cost of ownership and potentially not possible
  - Need the porridge to be JUST right and prefer secure coding from the beginning

Vulnerability Intelligence – What Should We Use?

- Based on the issues, companies should evaluate software including OSS prior to usage!
  - Companies need to determine if they think the OSS project is mature enough to rely on
- Is the product/project End of Life? Or still seeing regular updates?
- Determine if there are known vulnerabilities that are not fixed
- Does the company or project work with researchers?
- Determine the true Cost of Ownership
  - Initial free usage looks amazing
  - But are they hidden costs to maintain that are not factored in properly?
- Vulnerability Timeline Metrics can help!
  - How long does it take for researchers to get a response?
  - How long does it take to provide a patch?

5 Star Ratings



Shop Smart for a Safer Car, SUV, Mini-Van or Light Truck

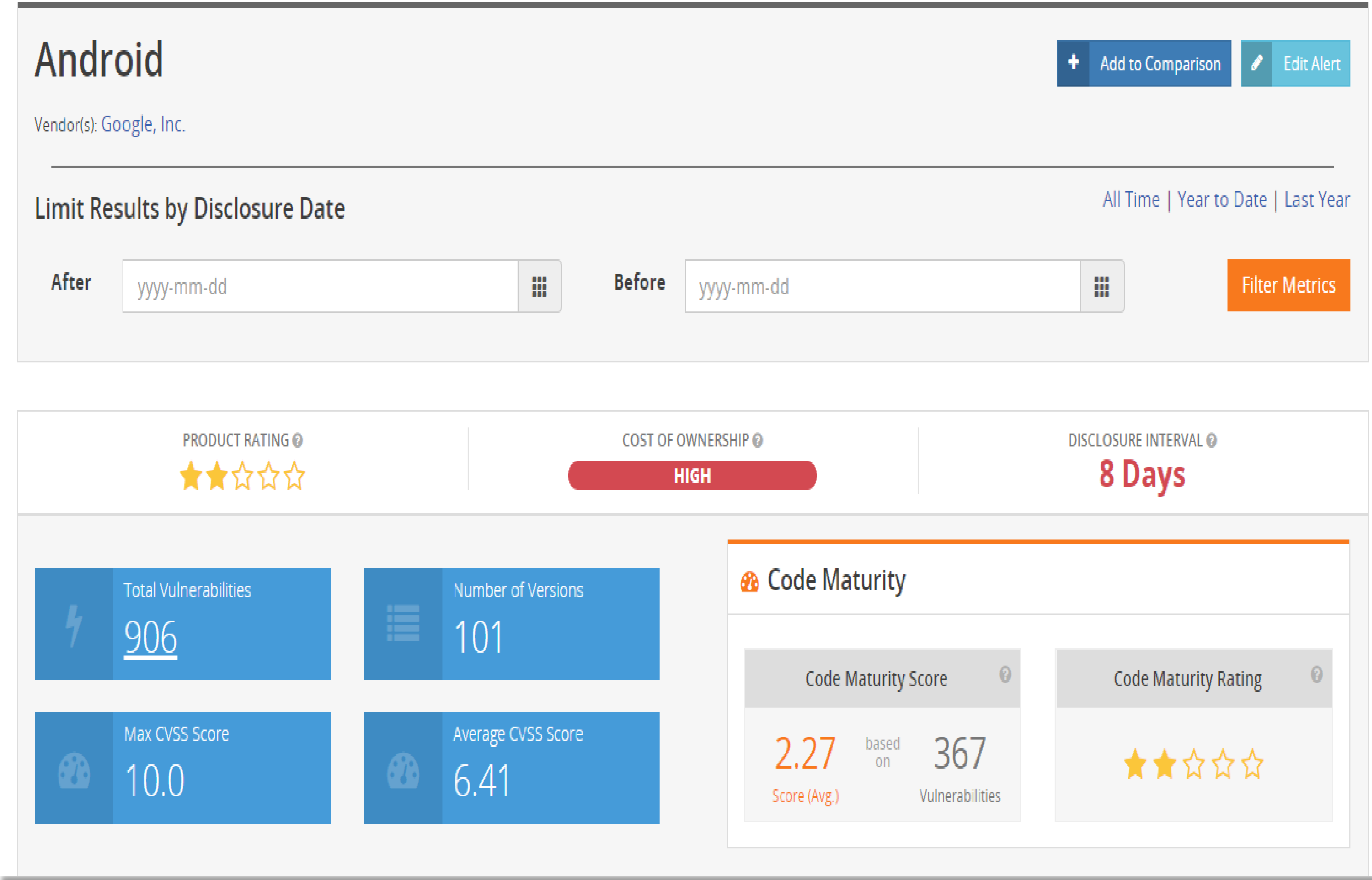
In the market to buy a safer vehicle? No doubt you're looking for unbiased crash test safety ratings you can easily compare. NHTSA's 5-Star Safety Ratings lets you do just that. Search below for crashworthiness and rollover safety by model, class and manufacturer, and compare safety ratings.

2011-Newer Vehicle Ratings

Comparing Newer Cars

Safety ratings for 2011 and newer vehicles should not be compared to ratings for 1990-2010 models since NHTSA introduced more stringent tests and new 5-Star Safety Ratings starting with 2011 models. Overall vehicle score and frontal crash ratings (in model years 2011 and newer) should ONLY be compared to other vehicles of similar size and weight.

VulnDB Ratings



Android

Vendor(s): Google, Inc.

Limit Results by Disclosure Date

After: yyyy-mm-dd

Before: yyyy-mm-dd

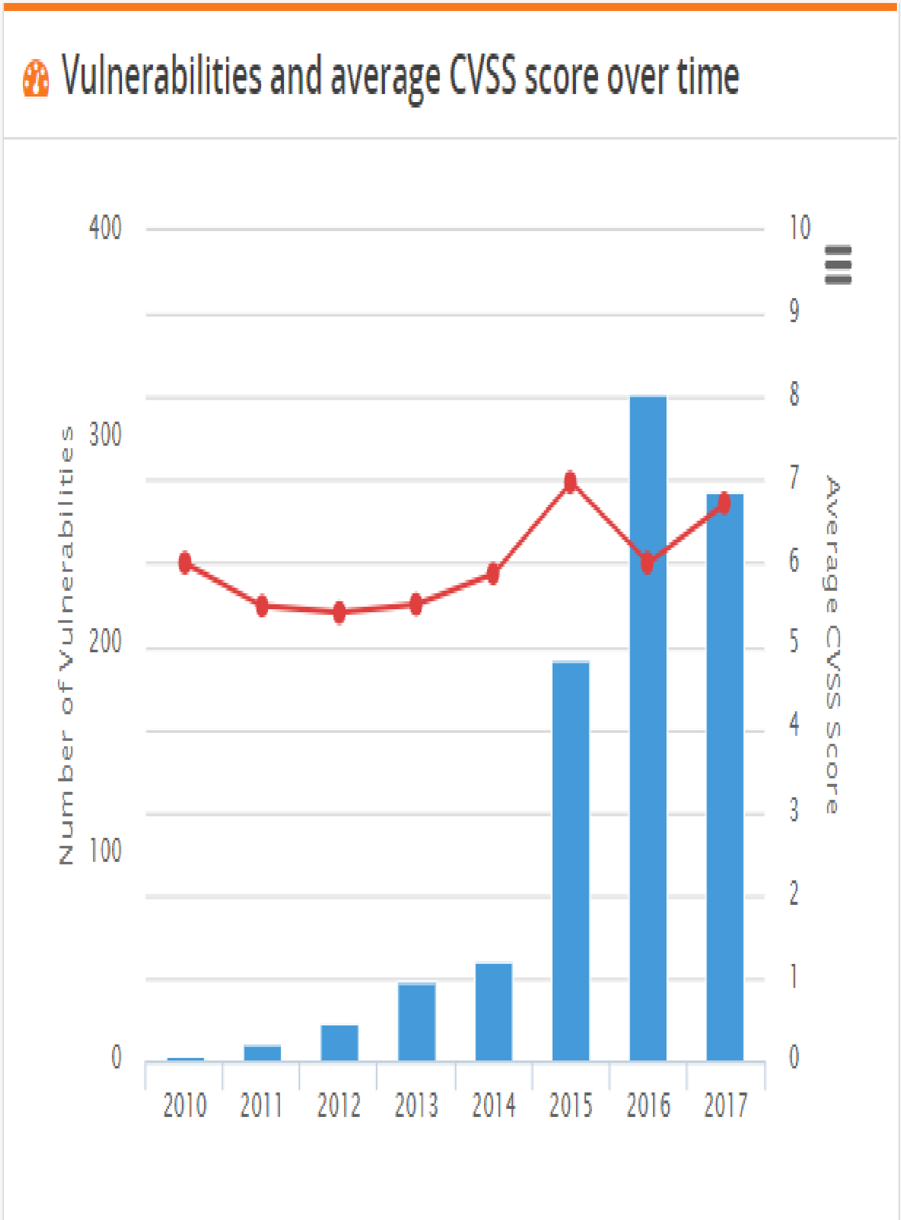
PRODUCT RATING	COST OF OWNERSHIP	DISCLOSURE INTERVAL
★★☆☆☆	HIGH	8 Days

Total Vulnerabilities: 906	Number of Versions: 101
Max CVSS Score: 10.0	Average CVSS Score: 6.41

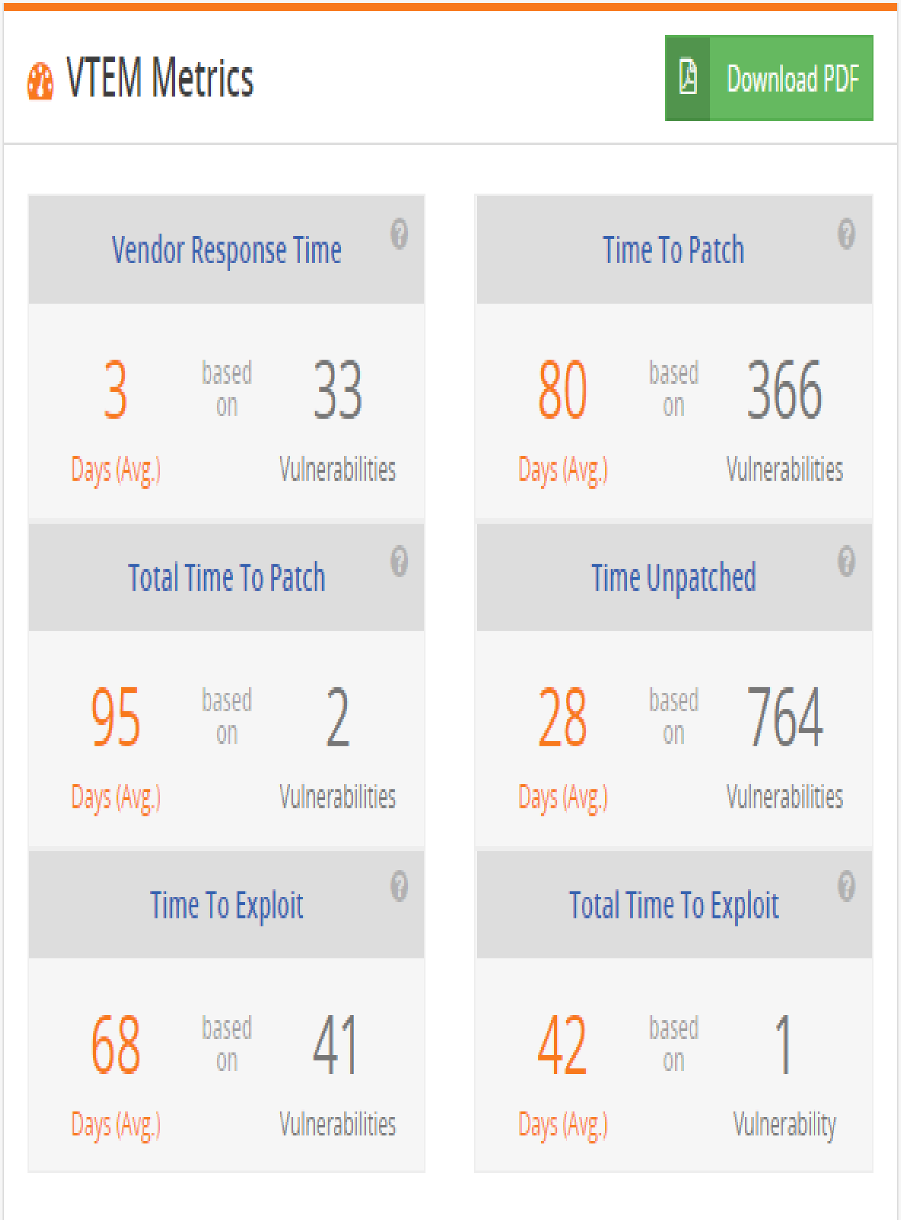
Code Maturity

Code Maturity Score	Code Maturity Rating
2.27 Score (Avg.) based on 367 Vulnerabilities	★★☆☆☆

VulnDB Ratings



Vulnerabilities and average CVSS score over time



VTEM Metrics

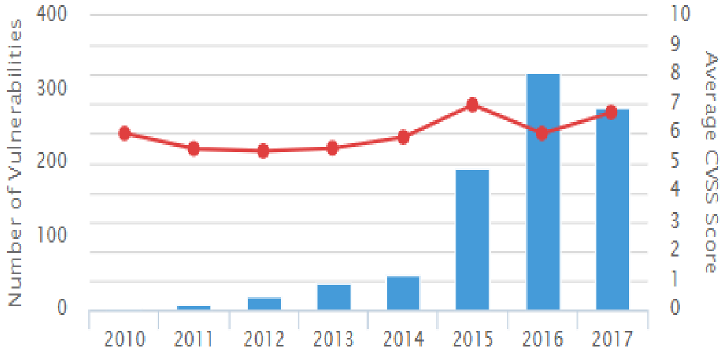
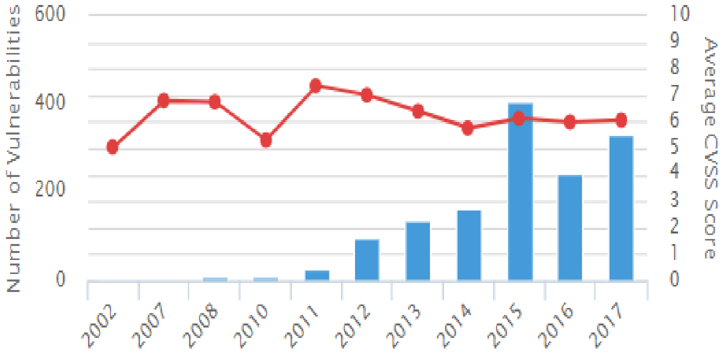
Download PDF

Vendor Response Time		
3 Days (Avg.)	based on	33 Vulnerabilities
Total Time To Patch		
95 Days (Avg.)	based on	2 Vulnerabilities
Time To Exploit		
68 Days (Avg.)	based on	41 Vulnerabilities

Time To Patch		
80 Days (Avg.)	based on	366 Vulnerabilities
Time Unpatched		
28 Days (Avg.)	based on	764 Vulnerabilities
Total Time To Exploit		
42 Days (Avg.)	based on	1 Vulnerability

VulnDB Ratings

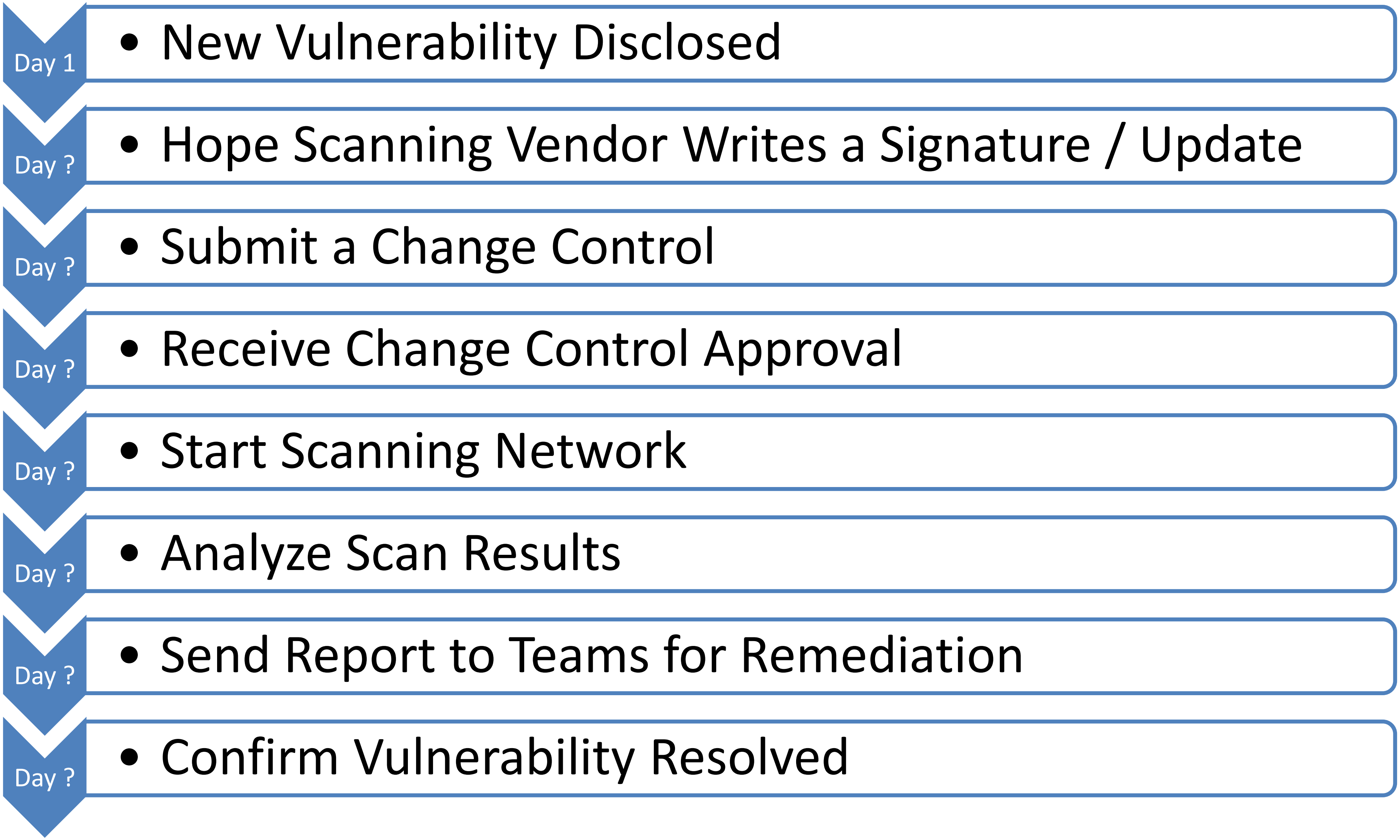
VulnDB Product Comparison

	Android	Apple iOS
Vulnerability & CVSS History		
Total Vulnerabilities	906	1425
Average CVSS Score	6.41	6.13
Cost of Ownership	HIGH	HIGH
Disclosure Interval	**8 Days**	**21 Days**
Vendor Response Time (Number of Vulnerabilities)	3 (33)	52 (29)
Time to Patch (Number of Vulnerabilities)	80 (366)	72 (240)
Code Maturity Score	2.27	2.36

Vulnerability Intelligence – Not Scanners!

- Vulnerability Scanners are what most organizations use for managing vulnerabilities
- Much longer Time of Exposure, than if you truly know your environment (assets) and map to know vulnerabilities as primary
  - Use scanners as a catch all and to help uncover config issues
  - Focus on being adaptive with assets inventory and mapping to vulnerability intelligence

Vulnerability Scanning – Timeline Examples



Day 1
- New Vulnerability Disclosed

Day ?
- Hope Scanning Vendor Writes a Signature / Update

Day ?
- Submit a Change Control

Day ?
- Receive Change Control Approval

Day ?
- Start Scanning Network

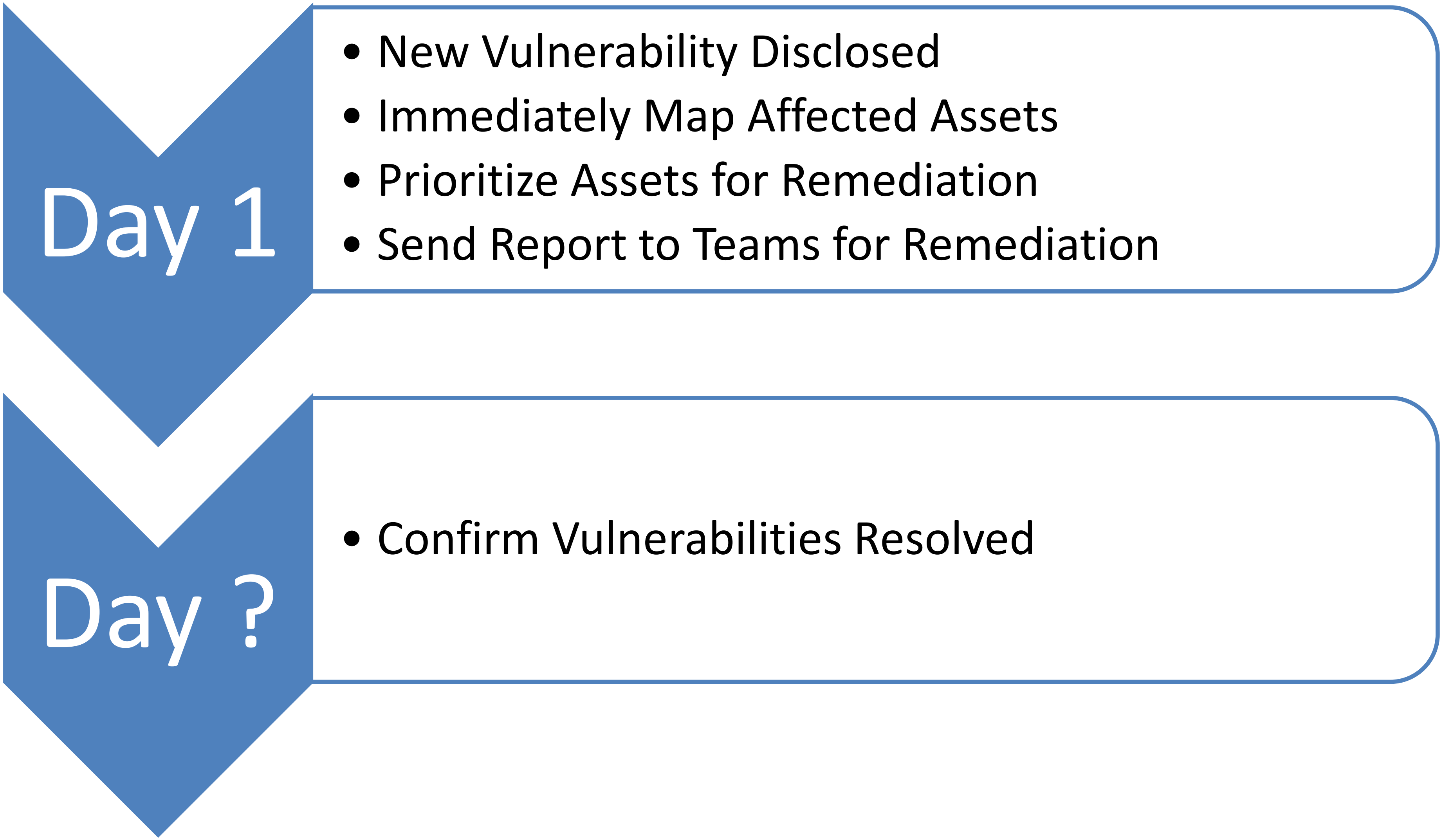
Day ?
- Analyze Scan Results

Day ?
- Send Report to Teams for Remediation

Day ?
- Confirm Vulnerability Resolved

This approach misses critical issues & can take days, weeks or months!

Vulnerability Intelligence – Timeline Examples



Day 1

- New Vulnerability Disclosed
- Immediately Map Affected Assets
- Prioritize Assets for Remediation
- Send Report to Teams for Remediation

Day ?

- Confirm Vulnerabilities Resolved

This approach is non-intrusive and provides instant threat modeling!

Regulation Might Be Required

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?

Microsoft
Windows xp
April 8, 2014

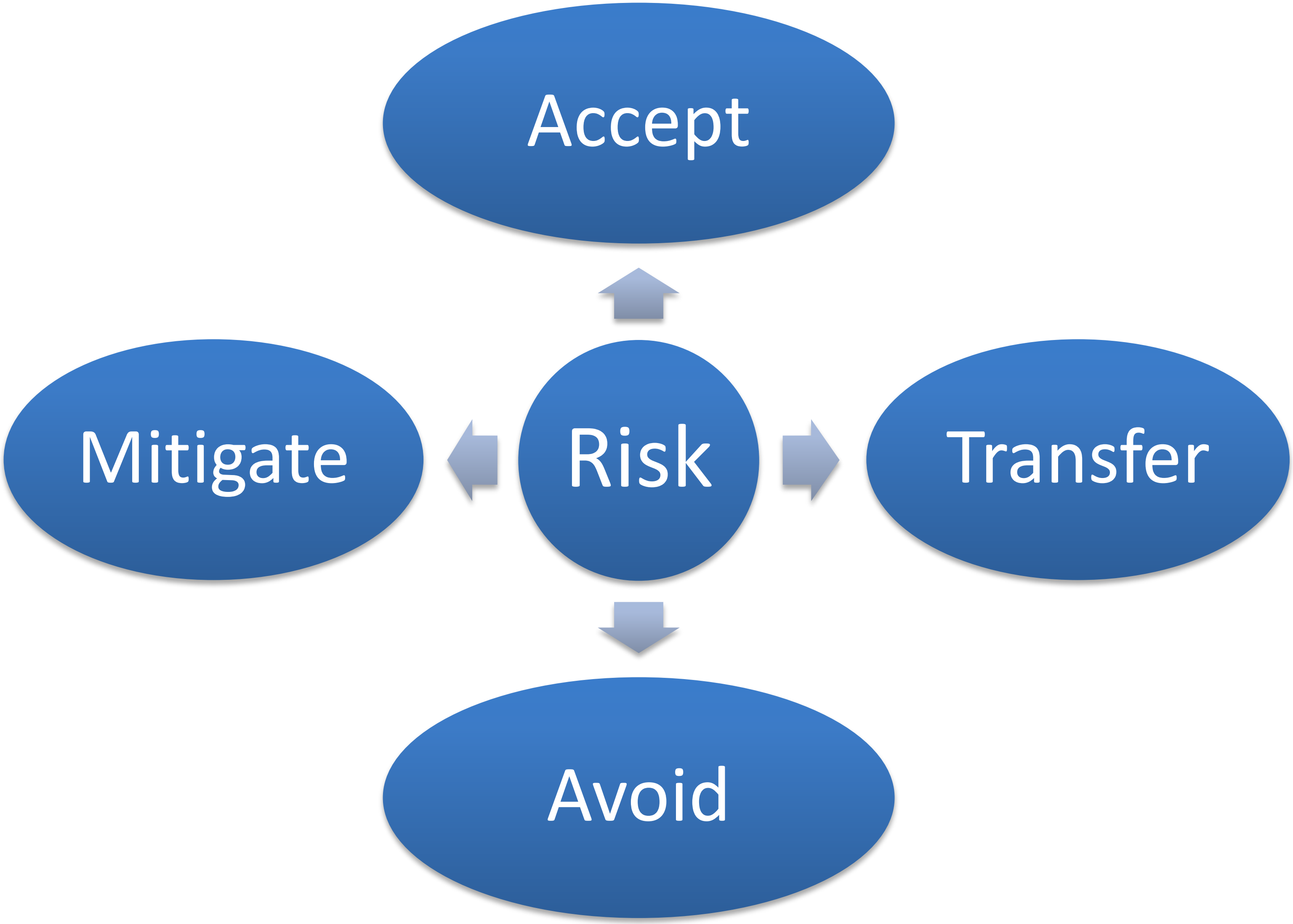
Data Breach – Ticking Time Bomb?

Only a matter of when for most organizations?

Data Breach – Cost Money?

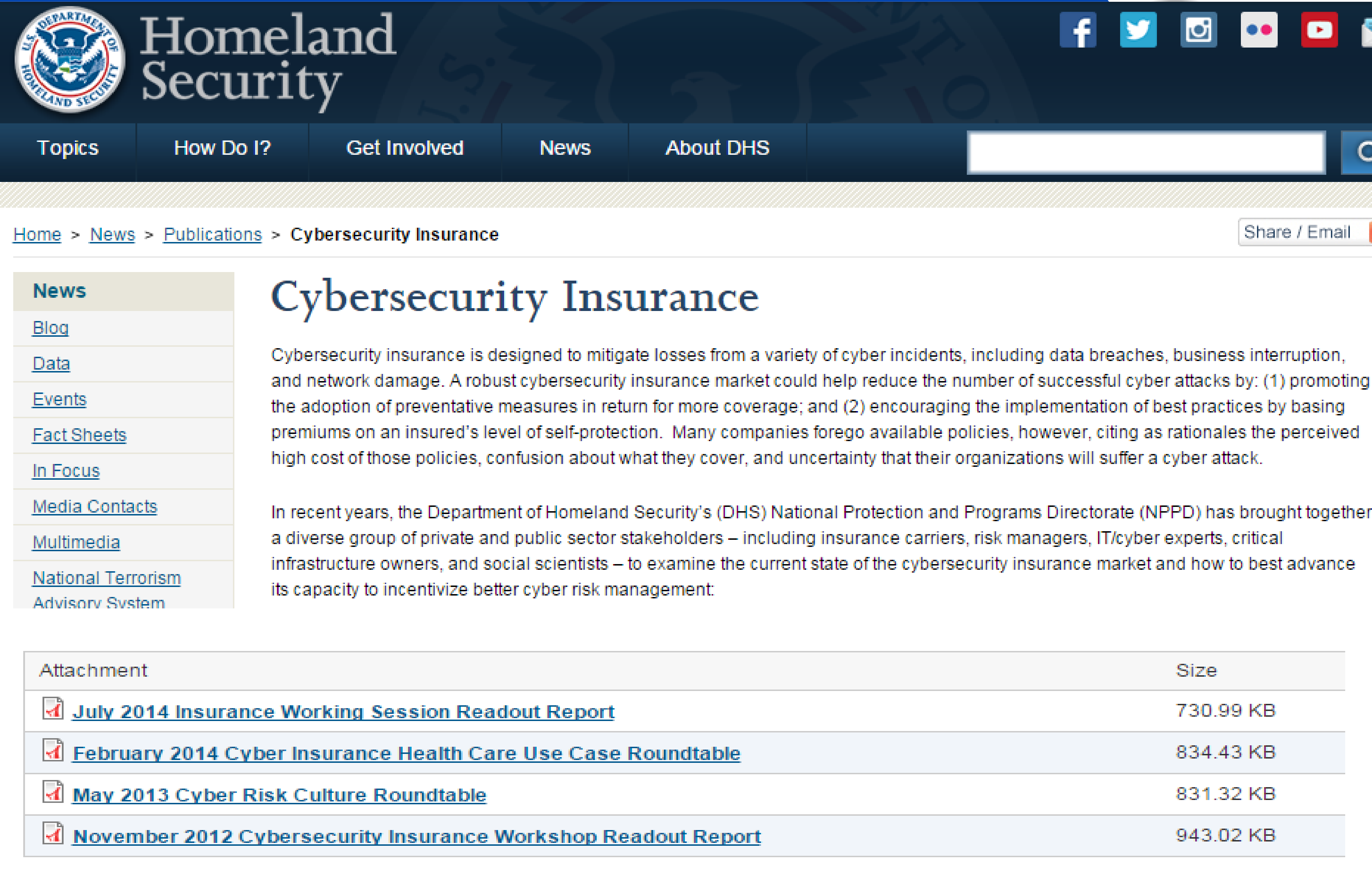
Data Breaches cost organizations money?

Reality of Risk



Cyber Liability – DHS

RiskBased Security



Cybersecurity Insurance

Cybersecurity insurance is designed to mitigate losses from a variety of cyber incidents, including data breaches, business interruption, and network damage. A robust cybersecurity insurance market could help reduce the number of successful cyber attacks by: (1) promoting the adoption of preventative measures in return for more coverage; and (2) encouraging the implementation of best practices by basing premiums on an insured's level of self-protection. Many companies forego available policies, however, citing as rationales the perceived high cost of those policies, confusion about what they cover, and uncertainty that their organizations will suffer a cyber attack.

In recent years, the Department of Homeland Security's (DHS) National Protection and Programs Directorate (NPPD) has brought together a diverse group of private and public sector stakeholders – including insurance carriers, risk managers, IT/cyber experts, critical infrastructure owners, and social scientists – to examine the current state of the cybersecurity insurance market and how to best advance its capacity to incentivize better cyber risk management:

Attachment	Size
July 2014 Insurance Working Session Readout Report	730.99 KB
February 2014 Cyber Insurance Health Care Use Case Roundtable	834.43 KB
May 2013 Cyber Risk Culture Roundtable	831.32 KB
November 2012 Cybersecurity Insurance Workshop Readout Report	943.02 KB

Starts With Us!

- Basic information security program is a must!
- Understand your exposures
- Understand your data and number of records
- Evaluate software prior to usage
  - Make sure you understand 3rd Party Libraries usage
  - Companies make buying decisions based on security and not new features
  - Vendor lose a few deals due to lack of security it will change their focus

Internet of Things – Questions Remain!

Questions?

EVIL CORP