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


SESSION ID: VPT-R11

# Wait wait… Don't pwn me!

**MODERATOR:**

**Mark Miller**
Senior Storyteller
TheNEXUS Community Project
@TSWAlliance

**PANELISTS:**

**Jacob West**
Chief Architect, Security Products
NetSuite
@sfjacob

**Joshua Corman**
Chief Community Officer
Sonatype

**Chris Eng**
Vice President of Research
Veracode
@chriseng

# The Panel




#RSAC
@TSWAlliance

# The Rules for Wait Wait…

- Each correct answer to the initial question is worth 3 points
- A wrong answer subtracts 2 points
- A pass on a question loses 1 point
- A correct answer from an audience member gets allocated 2 points to the panelist of their choice

# The Rules for Wait Wait…

**The moderator may arbitrarily give or take away points at any time**

# Online News Resources

- Pandodaily
- Forbes
- Brian Krebs
- Hacker News
- Gizmodo
- Poynter
- Ars Technica
- Wired
- Swift on Security
- FBI/CIA/NSA
- WSJ
- CSO
- TechCo
- The Verge
- Kickstarter

# Swift on Security

TWEETS 13.8K | FOLLOWING 2,986 | FOLLOWERS 70.1K | FAVORITES 17.4K | LISTS 11

# InfoSec Taylor Swift

@SwiftOnSecurity

I make stupid jokes, panic about the machine uprising, talk about consumer technology security, and use Oxford commas. See website link for ethics statement.

WELCOME TO NEW YORK

twitter.com/swiftonsecurit...

Tweet to InfoSec Taylor Swift

Tweets | Tweets & replies | Photos & videos

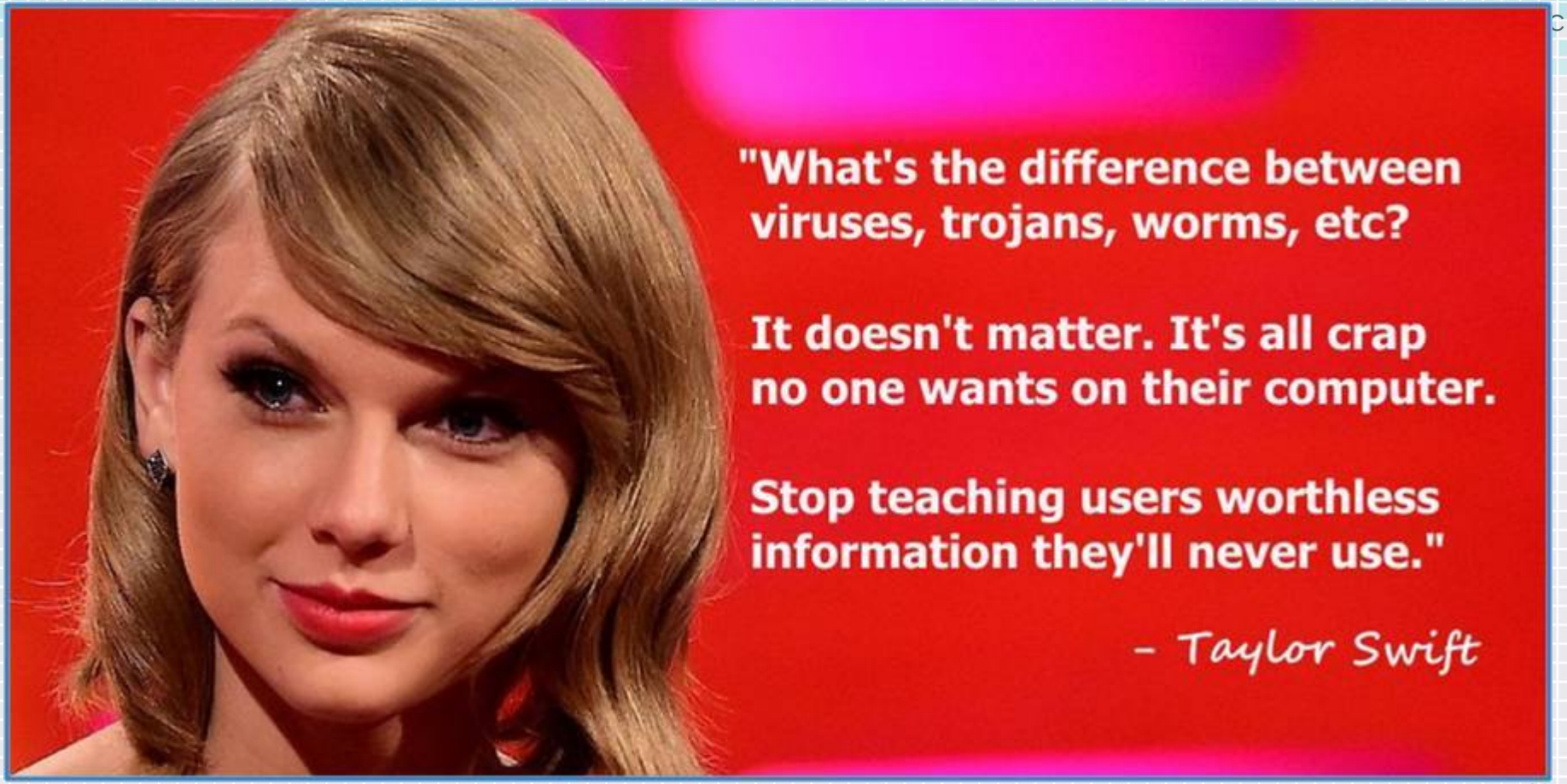
**InfoSec Taylor Swift** @SwiftOnSecurity · 16m

I apologize for the previous tweet and have deleted it. America #1.

5 9

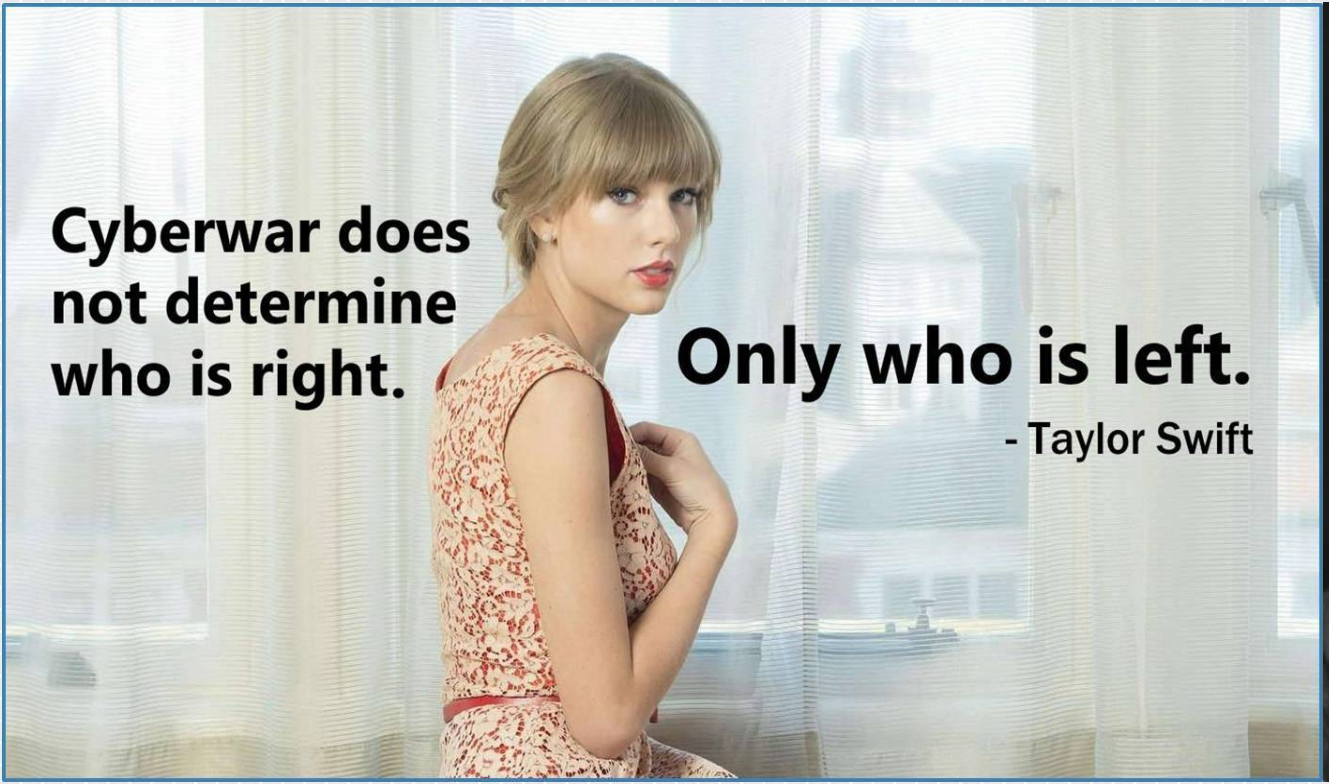
# According to Taylor Swift…

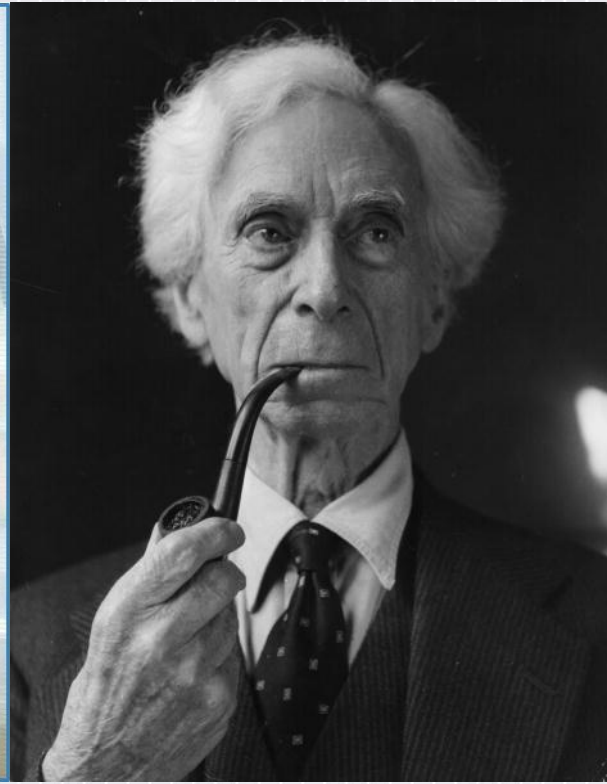
**What's the difference between viruses, trojans, worms, etc?**


"What's the difference between viruses, trojans, worms, etc?
It doesn't matter. It's all crap no one wants on their computer.
Stop teaching users worthless information they'll never use."
- Taylor Swift

# According to Taylor Swift…

**Cyber war doesn't determine who is right…**


Cyberwar does not determine who is right.
Only who is left.
- Taylor Swift



# According to Taylor Swift…

**“Maybe we should send people who don’t celebrate earth day to… <where>”**


InfoSec Taylor Swift @SwiftOnSecurity · 2h
Maybe we should send people who don't celebrate Earth Day to Mars'
12
42

# Three Letter Agencies

# Three Letter Agencies

**What 3 letter agency has placed $3M bounty for the ZeuS Trojan author?**

- FBI
- CIA
- NSA
- All of the Above


## 25 FBI: $3M Bounty for ZeuS Trojan Author

FEB 15

The FBI this week announced it is offering a USD $3 million bounty for information leading to the arrest and/or conviction of one **Evgeniy Mikhailovich Bogachev**, a Russian man the government believes is responsible for building and distributing the **ZeuS banking Trojan**.

Bogachev is thought to be a core architect of ZeuS, a malware strain that has been used to steal hundreds of millions of dollars from bank accounts — mainly from small- to mid-sized businesses based in the United States and Europe. Bogachev also is accused of being part of a crime gang that infected tens of millions of computers, harvested huge volumes of sensitive financial data, and rented the compromised systems to other hackers, spammers and online extortionists.

So much of the intelligence gathered about Bogachev and his alleged accomplices has been scattered across various court documents and published reports over the years, but probably just as much on this criminal mastermind and his associates has never seen the light of day.

# Three Letter Agencies

**What 3 letter agency planned to hijack Apple's developer tools?**

- FBI
- CIA
- NSA
- All of the Above

# How the CIA planned to hijack Apple's developer tools

by James Trew | @itstrew | March 10th 2015 at 8:27 am

# Three Letter Agencies

**What 3 letter agency developed planes that scrape cellphone data?**

- FBI
- CIA
- NSA
- All of the Above

US & WORLD

4 COMMENTS

# The CIA helped develop planes that scrape cell phone data

By Russell Brandom on March 10, 2015 03:35 pm Email @russellbrandom



ssellbrandom

# Strange But True

# Strange But True

**Rightcorps bills pirates for $20 a song. To the nearest $1M, how much money has the company made so far?**

ars technica

MAIN MENU · MY STORIES: 22 · FORUMS · SUBSCRIBE · JOBS · ARS CONSORTIUM

LAW & DISORDER / CIVILIZATION & DISCONTENTS

# Rightscorp bills pirates for $20 a song, burns more money than ever

Company says it's a "pioneer in the fight against piracy," loses $3.4 million.

by **Joe Mullin** - Mar 10, 2015 6:45pm EDT

Share Tweet 101


A visualization of peer-to-peer piracy, from a Rightscorp promotional video

# Strange But True

**Within 10,000, how many emails does Senator Lindsey Graham say he has sent from his personal account?**

pandodaily EVENTS VIDEO AUDIO PANDOLAND

# This US Senator has never sent an email. So why is he on a subcommittee focused on tech?

BY NATHANIEL MOTT
ON MARCH 9, 2015

# Strange But True

**What is the 2nd most funded product on Kickstarter?**

KICKSTARTER Discover Start Search Projects

# COOLEST COOLER: 21st Century Cooler that's Actually Cooler

by **Ryan Grepper**


**62,642**
backers

**$13,285,226**
pledged of $50,000 goal

**0**
seconds to go

**Funded!**

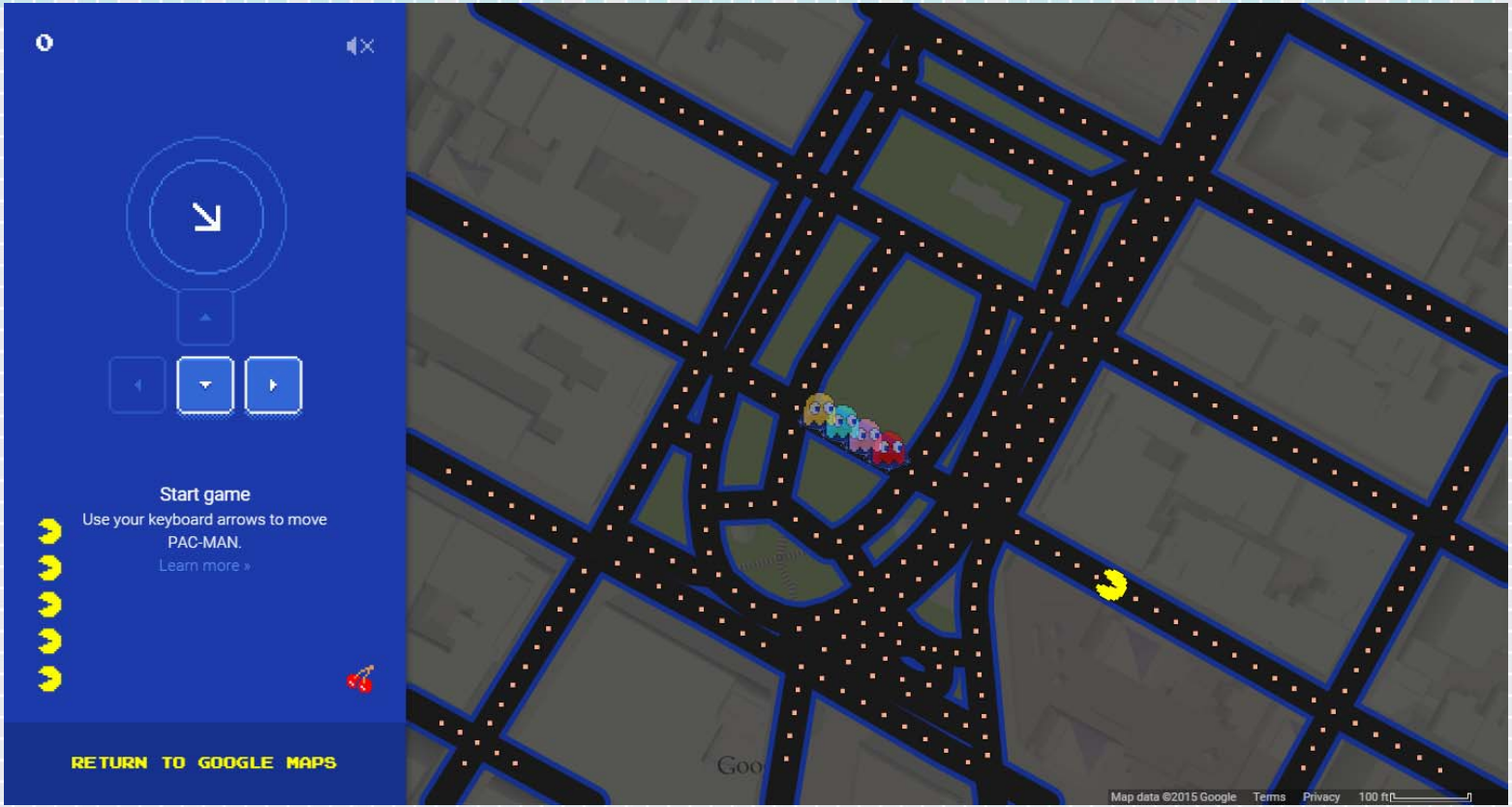
This project was successfully funded on August 29, 2014.

# Bluff the Panel

# Bluff the Panel

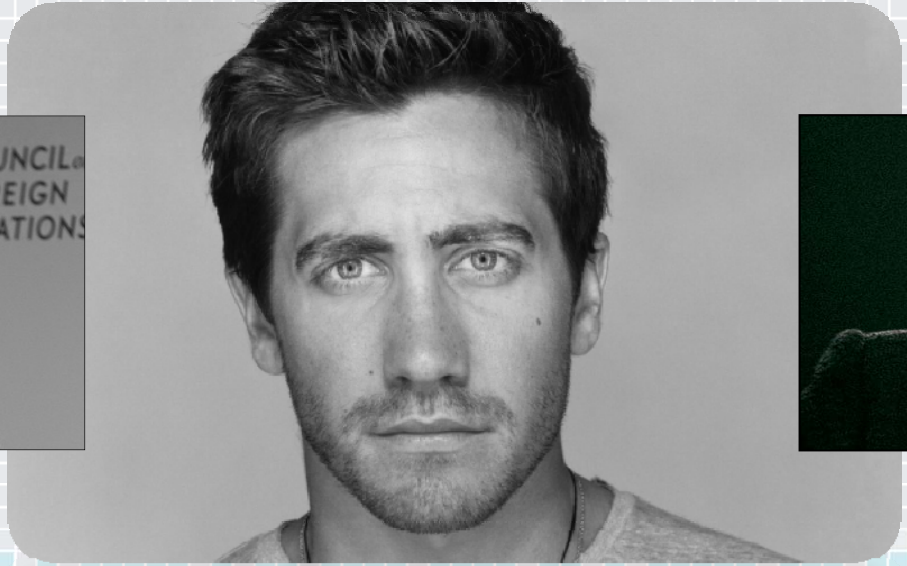
## For three days in early April, Google maps did what?

- Put treasure chest markers in 100 street locations in New York City that could be redeemed for $100 each
- Let you play Pac Man on the streets of New York using Google View
- Mis-directed people who were going from 14th Street Union Square to 16 Street Barnes & Noble, and had them go 24 miles by way of Brooklyn and Queens, over two bridges and through one tunnel


0
Start game
Use your keyboard arrows to move PAC-MAN.
Learn more »
RETURN TO GOOGLE MAPS
Map data ©2015 Google
Terms
Privacy
100 ft

# Bluff the Panel

**According to Edward Snowden, who is 110% sexy?**

WIRED Snowden's 'Sexy Margaret Thatcher' Password Isn't So Secure

BUSINESS DESIGN ENTERTAINMENT GEAR

# SNOWDEN'S 'SEXY MARGARET THATCHER' PASSWORD ISN'T SO SECURE


JOHN DOWNING/GETTY IMAGES

# Bluff the Panel

## Why did prosecutors drop all charges in a pistol whipping robbery in St. Louis

- The perp was part of a witness protection program for informers from the group Anonymous
- To protect a cell-site simulator called stingray
- Detectives discovered the event occurred inside Grand Theft Auto, but was reported as real

ars technica

MAIN MENU | MY STORIES: 25 | FORUMS | SUBSCRIBE | JOBS | ARS CONSORTIUM

LAW & DISORDER / CIVILIZATION & DISCONTENTS

# Prosecutors drop robbery case to preserve stingray secrecy in St. Louis

A pistol-whipped victim, who required 18 stitches, is "shocked" at the outcome.

by Cyrus Farivar - Apr 20, 2015 5:00am PDT

Share Tweet 175


The St. Louis case provides yet another real-world example where prosecutors have preferred to drop charges instead of fully disclose how the devices, also known as cell-site simulators, work in the real world. Last year, prosecutors in Baltimore did the same thing during a robbery trial.

# At the Conference

# At the Conference

**What is the financial value of your personal information at RSAC this year?**

Name
Email Address
Phone Number
Street Address

=

# At the Conference

**In 95% of the cases, how did attackers breach a system?**


USA 2015
April 20–24
Moscone Center, San Francisco
95%
of the time, attackers used stolen credentials
and simply walked right in
3
Source: 2015 Verizon Data Breach Investigation Report

# At the Conference

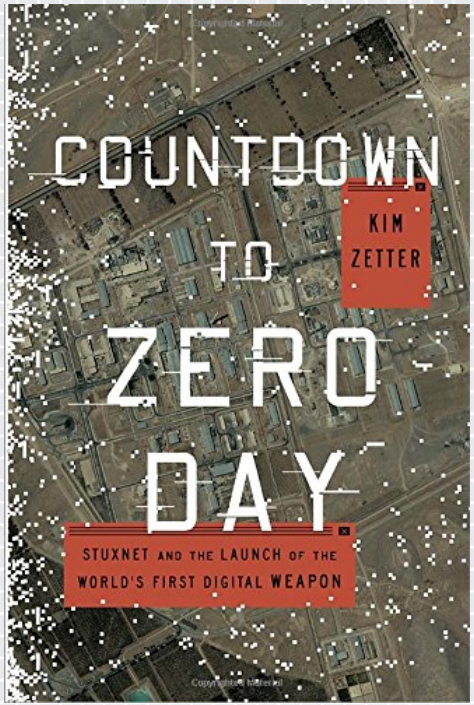
**“Who needs zero-day when you’ve got <what>?” – Amit Yoran**


Stupid!

# At the Conference

**According to research by Kim Zetter, how many Windows machines are currently infected with Stuxnet?**

# At the Conference

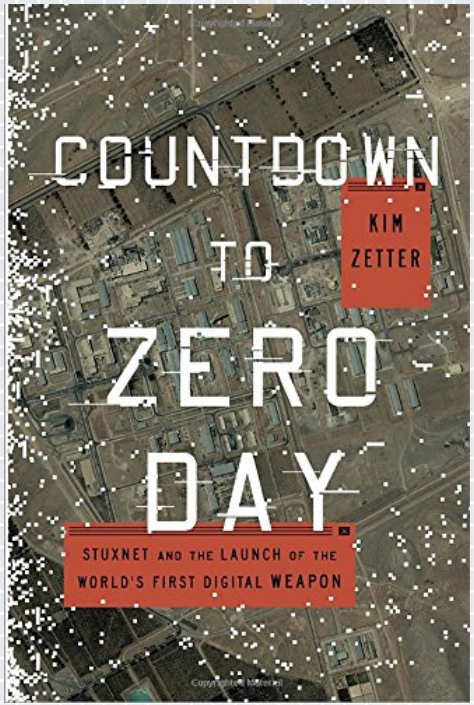



**3 Million +**

# At the Conference

**In the same research on Stuxnet, Zetter declared that 30 days worth of normal activity was recorded by the virus. How was the “normal” activity used?**

# At the Conference

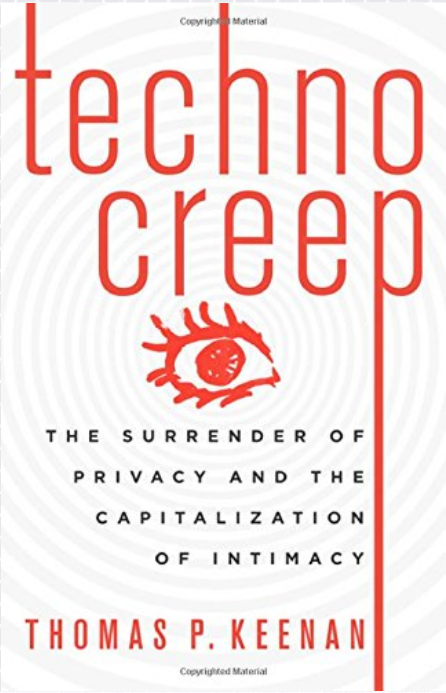



**Fed back normal data to the centrifuge dashboard to hide the current activity**

# At the Conference

**Techno Creep author, Dr. Tom Keenan, insists that this is the “creepiest place in America”.**

# At the Conference




**Any Disney theme park**

# Audience Limerick Challenge

# Audience Limerick Challenge

**“When I think of something so thrilling**
**As a concept that’s well worth it's drilling,**
**I talk to my minions, who have strong opinions**
**On info sec, so un****…”**

***Taylor Swift***

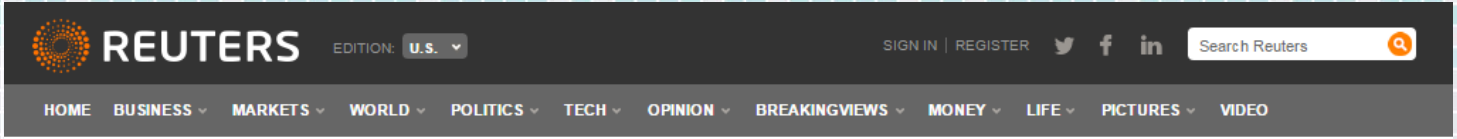
**InfoSec Taylor Swift** @SwiftOnSecurity · 13h

I don't know what info sex is, but it sounds terribly unfulfilling.

26 86

# Audience Limerick Challenge

**“There once was a general who scared us**
**Giving his mistress info she shared up.**
**The case is now done, and he's basically won.**
**With a 40,000 dollar fine for …”**




**Landing** | Thu Apr 23, 2015 7:16am EDT

# Former U.S. General David Petraeus to be sentenced in leak case

**WASHINGTON** | BY MARK HOSENBALL

(Reuters) - Former U.S. military commander and CIA director David Petraeus will appear in federal court in North Carolina on Thursday to face sentencing for allegedly leaking secrets to a mistress who was writing his biography.

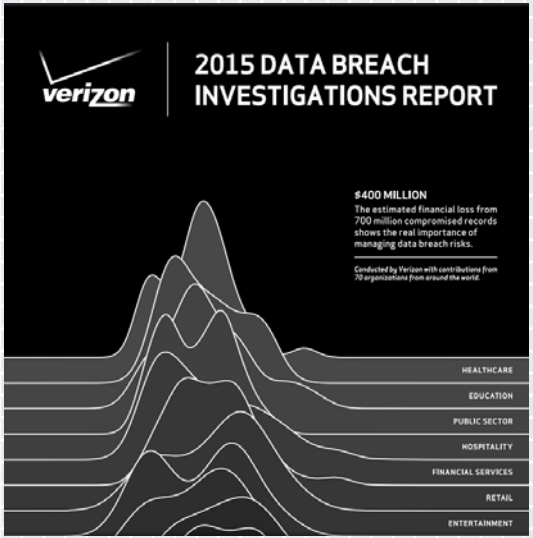
Petraeus, a now-retired U.S. Army General, has already agreed to plead guilty to a criminal misdemeanor charge of unauthorized removal and retention of classified material.

As part of the agreement with prosecutors filed in March, the government will not seek any prison time. Instead, Petraeus will agree to pay a $40,000 fine and receive two years of probation, according to court documents.

The recommendations are not binding on the federal judge who will preside at the hearing Thursday afternoon in Charlotte.

# Verizon Data Breach Report

# Verizon Data Breach Report




**Within 5%, how many recipients still open phishing emails?**

# PHISHING

*Attn: Sir/Madam*

Social engineering has a long and rich tradition outside of computer/network security, and the act of tricking an end user via e-mail has been around since AOL installation CDs were in vogue. Do you remember the "free cup holder" prank? Someone sending you an attachment that opened your CD-ROM drive was cute at the time, but a premonition of more malicious acts to come.

The first "phishing" campaigns typically involved an e-mail that appeared to be coming from a bank convincing users they needed to change their passwords or provide some piece of information, like, NOW. A fake web page and users' willingness to fix the nonexistent problem led to account takeovers and fraudulent transactions.

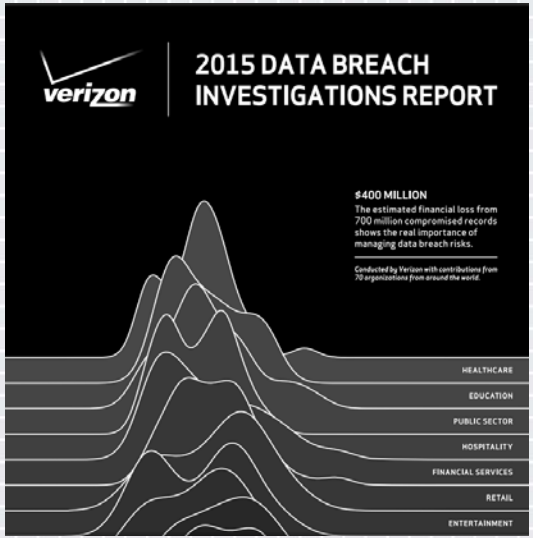
Phishing campaigns have evolved in recent years to incorporate installation of malware as the second stage of the attack. Lessons not learned from the silly pranks of yesteryear and the all-but-mandatory requirement to have e-mail services open for all users has made phishing a favorite tactic of state-sponsored threat actors and criminal organizations, all with the intent to gain an initial foothold into a network.

**23%**

OF RECIPIENTS NOW OPEN PHISHING MESSAGES AND 11% CLICK ON ATTACHMENTS.

For two years, more than two-thirds of incidents that comprise the Cyber-Espionage pattern have featured phishing.

# Verizon Data Breach Report




**Within 5%, what percentage of vulnerabilities were compromised more than one year after the CVE was published?**

# VULNERABILITIES

## *Do We Need Those Stinking Patches?*

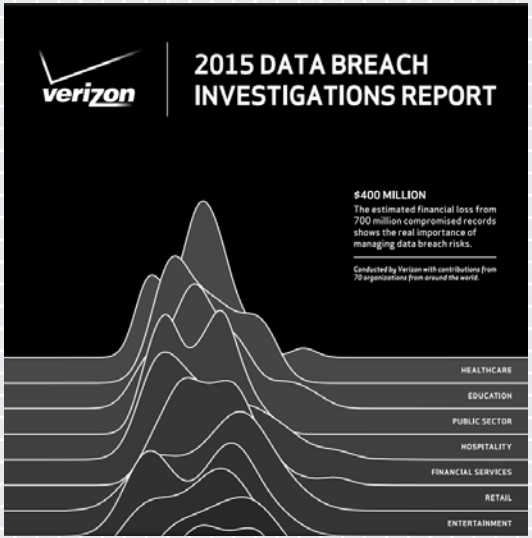
**Of all the risk factors in the InfoSec domain, vulnerabilities are probably the most discussed, tracked, and assessed over the last 20 years. But how well do we really understand them? Their link to security incidents is clear enough after the fact, but what can we do before the breach to improve vulnerability management programs? These are the questions on our minds as we enter this section, and Risk I/O was kind enough to join us in the search for answers.**

Risk I/O started aggregating vulnerability exploit data from its threat feed partners in late 2013. The data set spans 200 million+ successful exploitations across 500+ common vulnerabilities and exposures (CVEs)[11] from over 20,000 enterprises in more than 150 countries. Risk I/O does this by correlating SIEM logs, analyzing them for exploit signatures, and pairing those with vulnerability scans of the same environments to create an aggregated picture of exploited vulnerabilities over time. We focused on mining the patterns in the successful exploits to see if we could figure out ways to prioritize remediation and patching efforts for known vulnerabilities.

**99.9%**

**OF THE EXPLOITED VULNERABILITIES WERE COMPROMISED MORE THAN A YEAR AFTER THE CVE WAS PUBLISHED.**

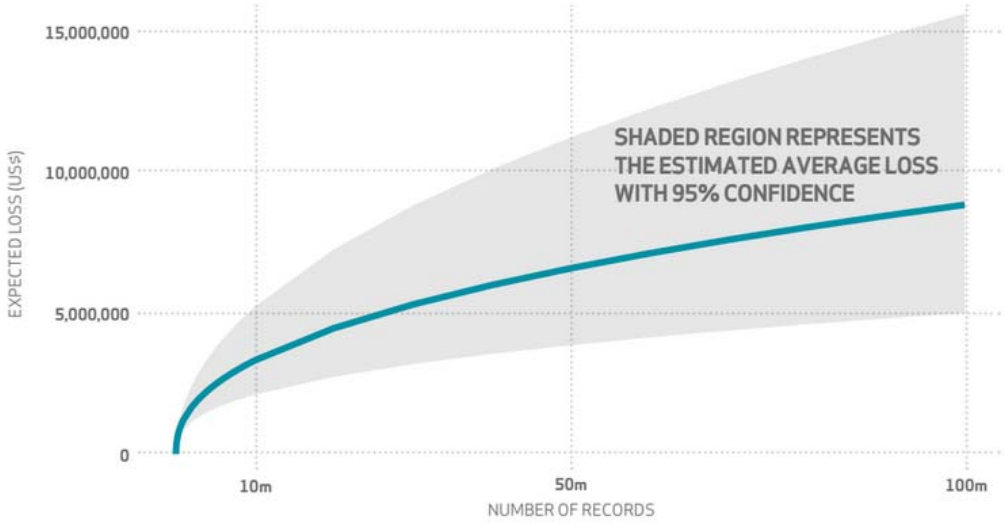
# Verizon Data Breach Report




**Within $1000, how much was the average loss for a breach of 1000 records?**

## The forecasted average loss for a breach of 1,000 records is between $52,000 and $87,000.

Since our glass of model strength is only half full, the precision of the model will suffer a bit. This means we need broad ranges to express our confidence in the output. On top of that, our uncertainty increases exponentially as the breach gets larger. For example, with the new model, the average loss for a breach of 1,000 records is forecast to be between $52,000 and $87,000, with 95% confidence. Compare that to a breach affecting 10 million records where the average loss is forecasted to be between $2.1 million and $5.2 million (note that these are average losses,



# Scary but True

# Scary but True

**A security flaw in a well known drug pump allows hackers to do what?**

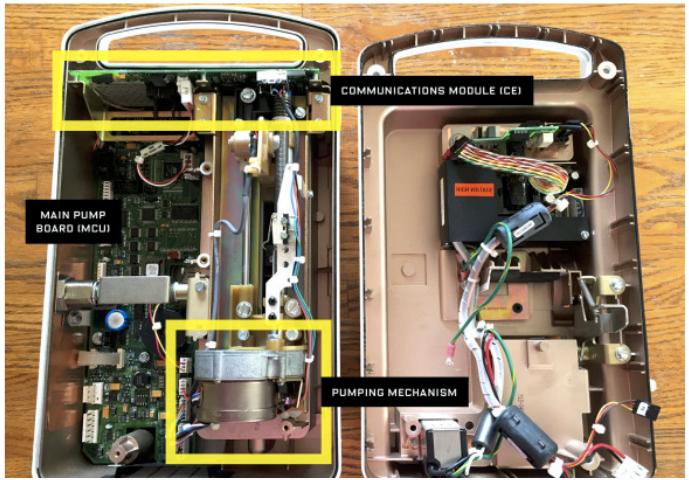
***Wired Magazine***

WIRED Drug Pump's Security Flaw Lets Hackers Raise Dose Limits

BUSINESS | DESIGN | ENTERTAINMENT | GEAR | SCIENC

KIM ZETTER SECURITY 04.09.15 7:00 AM

# DRUG PUMP'S SECURITY FLAW LETS HACKERS RAISE DOSE LIMITS



# Scary but True

**What was Mark Hamill's greatest fear if he turned down the role of Luke Skywalker in the upcoming Star Wars Movie?**

***Entertain This***

ENTERTAiNTHiS!

Movies

# Mark Hamill feared angry geek mobs if he rejected 'Star Wars' return

By Bryan Alexander April 19, 2015 1:33 pm Follow @BryAlexand

3.3k shares SHARE TWEET EMAIL

Mark Hamill has a pretty good idea who would not have been happy if he said no to "Star Wars" (Getty)

MOST POPULAR

10k shares
Watch: The first 'Batman v Superman' trailer is here, officially

1.6k shares
Brooklyn Beckham proves that his dad is just like ours -- embarrassing

6.2k shares
Nope, Target isn't getting more of the (sold-out) Lilly Pulitze

Follow

# Scary but True

**Why was Chris Roberts, a prominent computer security expert, not allowed to board a United Flight last week?**

***International Business Times***

INTERNATIONAL BUSINESS TIMES
SUNDAY, APRIL 19, 2015 AS OF 9:33 PM CDT



# United Airlines Kicks Computer Expert Off Flight For Tweets

By Eric Markowitz @EricMarkowitz e.markowitz@ibtimes.com on April 19 2015 9:09 PM EDT

# Scary but True

**What is the weakest security link that is impossible to lock down in most homes?**

***Wall Street Journal***

THE WALL STREET JOURNAL. ≡ | BUSINESS

JOURNAL REPORTS: LEADERSHIP

# Your Weakest Security Link? Your Children

They are always making mischief online. Here's how to rein them in.

# Scary but True

**According to researcher Scott Bryner, users of Match.com are practicing unsafe <what>?**

***Wall Street Journal***

# eSecurity Planet

Internet security for IT pros

Networks | Windows | Wireless | Mobile | Browsers | Open Source | Patches | Malware | H

News | Trends | Columnists | How-Tos | Buying Guides | Research Center | About

## Researcher Uncovers Match.com Security Flaw

A server configuration error appears to be redirecting all HTTPS traffic to HTTP.

By **Jeff Goldman** | Posted April 21, 2015

Share

Software developer Scott Bryner recently found that the login page for dating site Match.com doesn't use HTTPS encryption, potentially exposing millions of users' passwords every time they log in.

As Ars Technica's Dan Goodin reports, the site uses an unprotected HTTP connection to transmit login credentials, allowing anyone on the same network to capture user names and passwords.

Bryner first noticed the flaw in early March 2015, though it's not clear how long the vulnerability was in place before then.

# Scary but True

**Bonus Question: What was Scott Bryner doing on Match.com?**

***Practicing safe protocols, of course.***

# Scary but True

**To the nearest penny, how much money are half the app markers spending on security?**

***Venture Beat***

VB | NEWS

Channels Newsletters Jobs Got news? Tell us!

# Study: Half of app makers spend $0 on security

# Scary but True

**An 18 year old unpatched vulnerability affects all versions of what?**

***Venture Beat***

The Hacker News™
Security in a serious way

# 18-year-old Unpatched Vulnerability Affects All Versions of Microsoft Windows

Monday, April 13, 2015 Swati Khandelwal



# Final Round

# Final Round

**A man in Colorado was charged last week for doing something to his computer. He was cited and released. What did he do?**


## Colorado man cited for shooting computer to death

We've all been frustrated with our computers at one time or another. A Colorado man did something about it. (AP File Graphic)

# Final Round

**According to a recent report by Stuart McClure, CEO of computer security firm Cylance, what is the final conclusion on how hackers were able to access the Sony network?**

THE STATE OF SECURITY

News. Trends. Insights.

FEATURED ARTICLES | LATEST SECURITY NEWS | TOPICS | RESOURCES | ABOUT

HOME » LATEST SECURITY NEWS » Sony Hackers Used Phishing Emails to Breach Company...

# Sony Hackers Used Phishing Emails to Breach Company Networks

DAVID BISSON

APR 22, 2015 | LATEST SECURITY NEWS

# Bluff the Panel

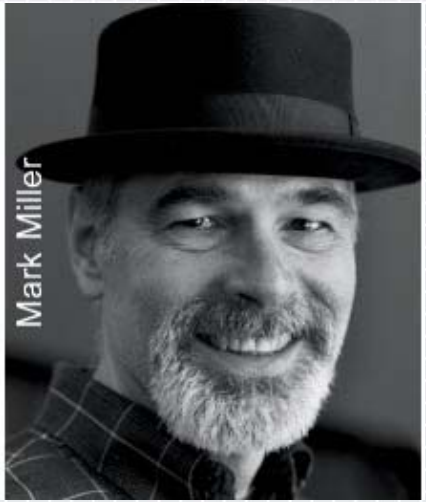
**On April 17, 2015 what band did Alex W. Gibbons declare the “Worst. Boyband. Everrr”?**

- Wham!
- One Direction
- This Panel

**Alex W Gibbons** @BillyGee73 · 2h

@TSWAlliance @joshcorman @chriseng @JacobWest Worst. Boyband. Everrr.



# What's the final score?

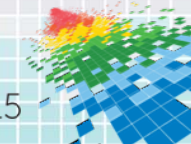
# Thank You to the The Panel

# Get a copy of the slides for this show immediately…

# community@sonatype.com





# Thank you to the team at RSAC for making all this possible

RSAConference2015
San Francisco | April 20-24 | Moscone Center


SESSION ID: VPT-R11

# Wait wait… Don't pwn me!

**MODERATOR:**

**Mark Miller**
Senior Storyteller
TheNEXUS Community Project
@TSWAlliance

**PANELISTS:**

**Jacob West**
Chief Architect, Security Products
NetSuite
@sfjacob

**Joshua Corman**
Chief Community Officer
Sonatype

**Chris Eng**
Vice President of Research
Veracode
@chriseng