BerkeleyLaw
UNIVERSITY OF CALIFORNIA

BERKELEY CENTER FOR
LAW & TECHNOLOGY

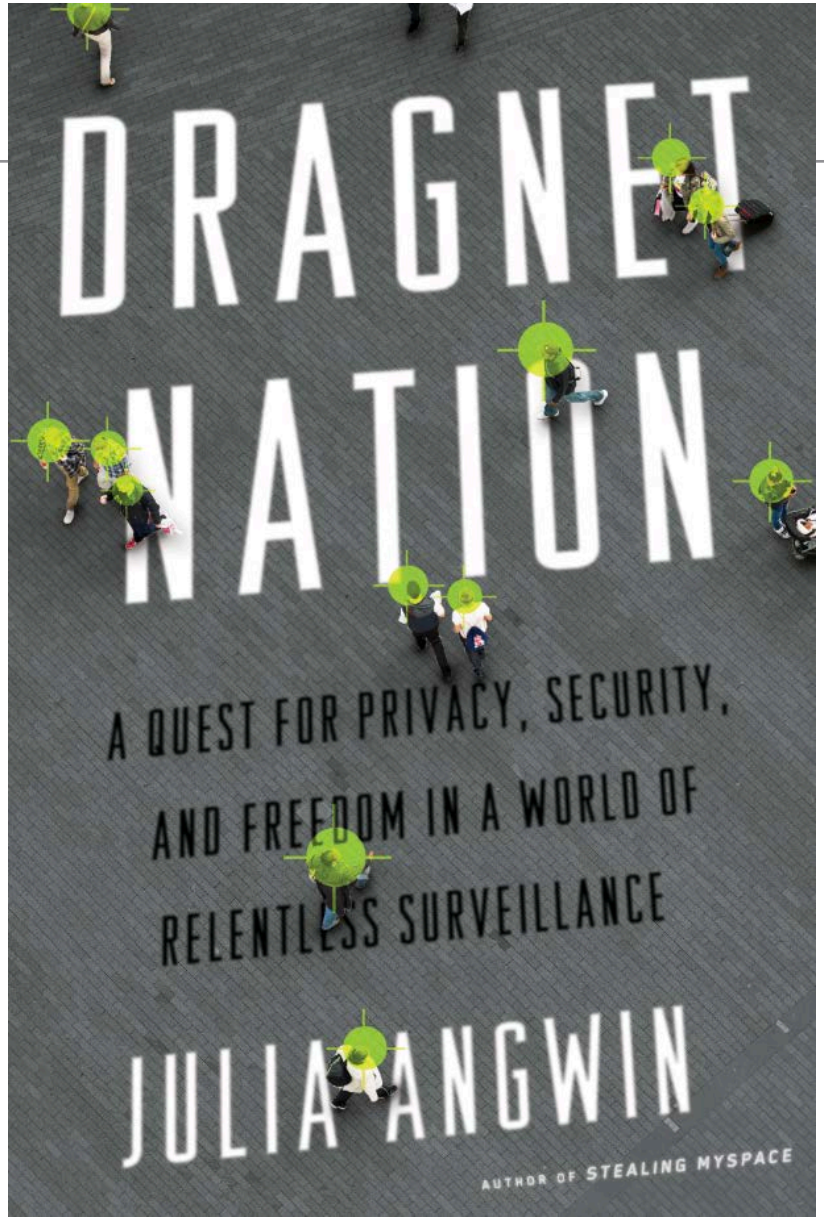
Data Security Issues

Moderated by:
Paul M. Schwartz
Berkeley Law School
Fourth Annual BCLT Privacy Forum
March 13, 2015

Roadmap

I. Introduction: Data Security
II. Top Three Data Security Issues or Trends of the Next 18 Months
III. Pragmatic Data Security Advice
IV. Questions and Answers

"The problem with computer security is that most of the advice we are given is absurd."



The CyberSummit (Feb. 13)

"Mr. Obama...made clear that his six years in the presidency had given him a new appreciation of how the government will be called upon to protect citizens against the most severe [cyber] attacks..."

Source (text and image): N.Y. Times;
http://www.nytimes.com/2015/02/14/business/obama-urges-tech-companies-to-cooperate-on-internet-security.html?_r=0

The White House, CyberSummit (Feb. 13)

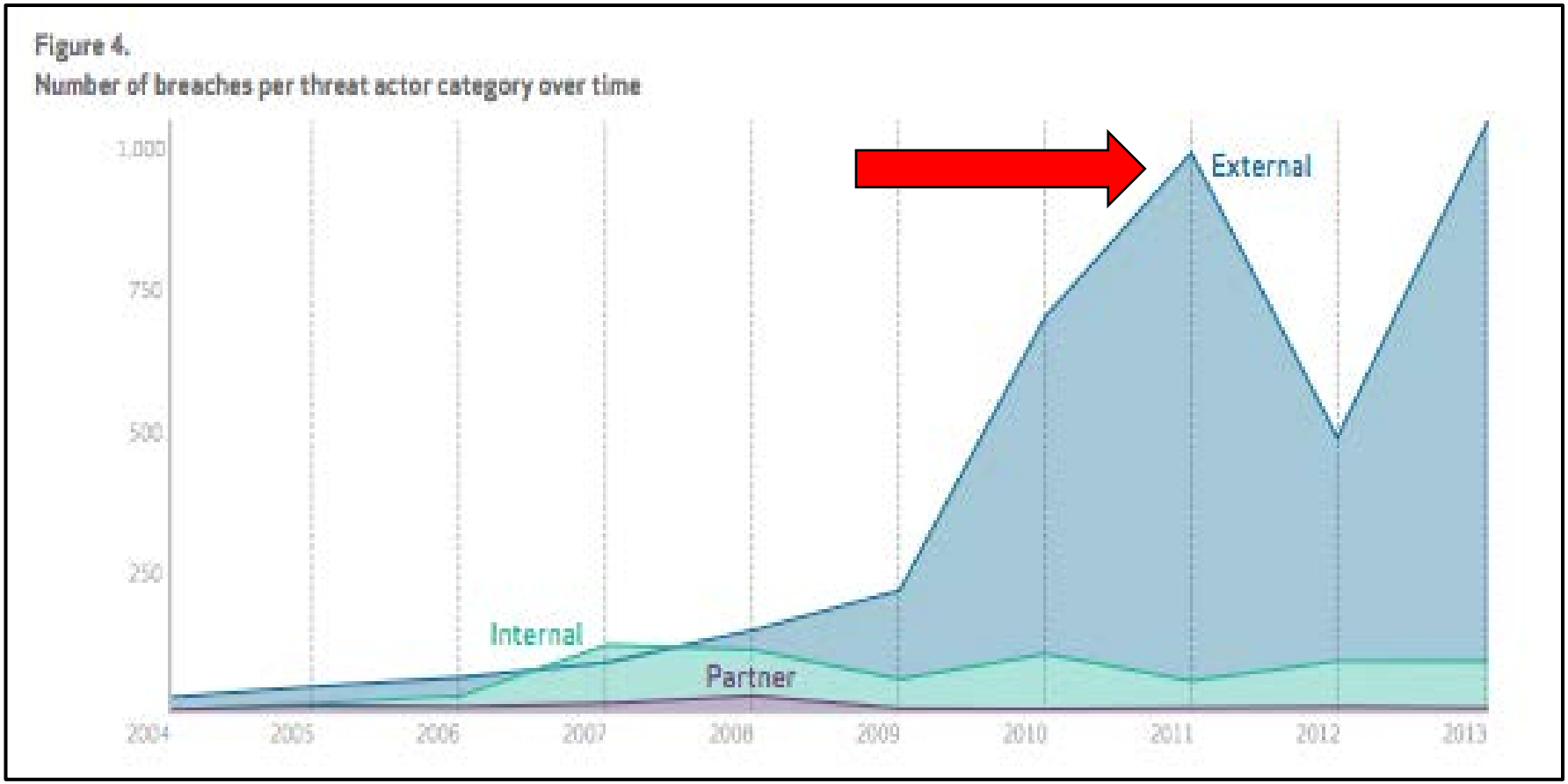
"[O]ur connectivity brings extraordinary benefits to our daily lives, but also brings risks."

The White House CyberSummit (Feb. 13)

"'People have entrusted us with their most personal and precious information . . . We owe them nothing less than the best protections that we can possibly provide."

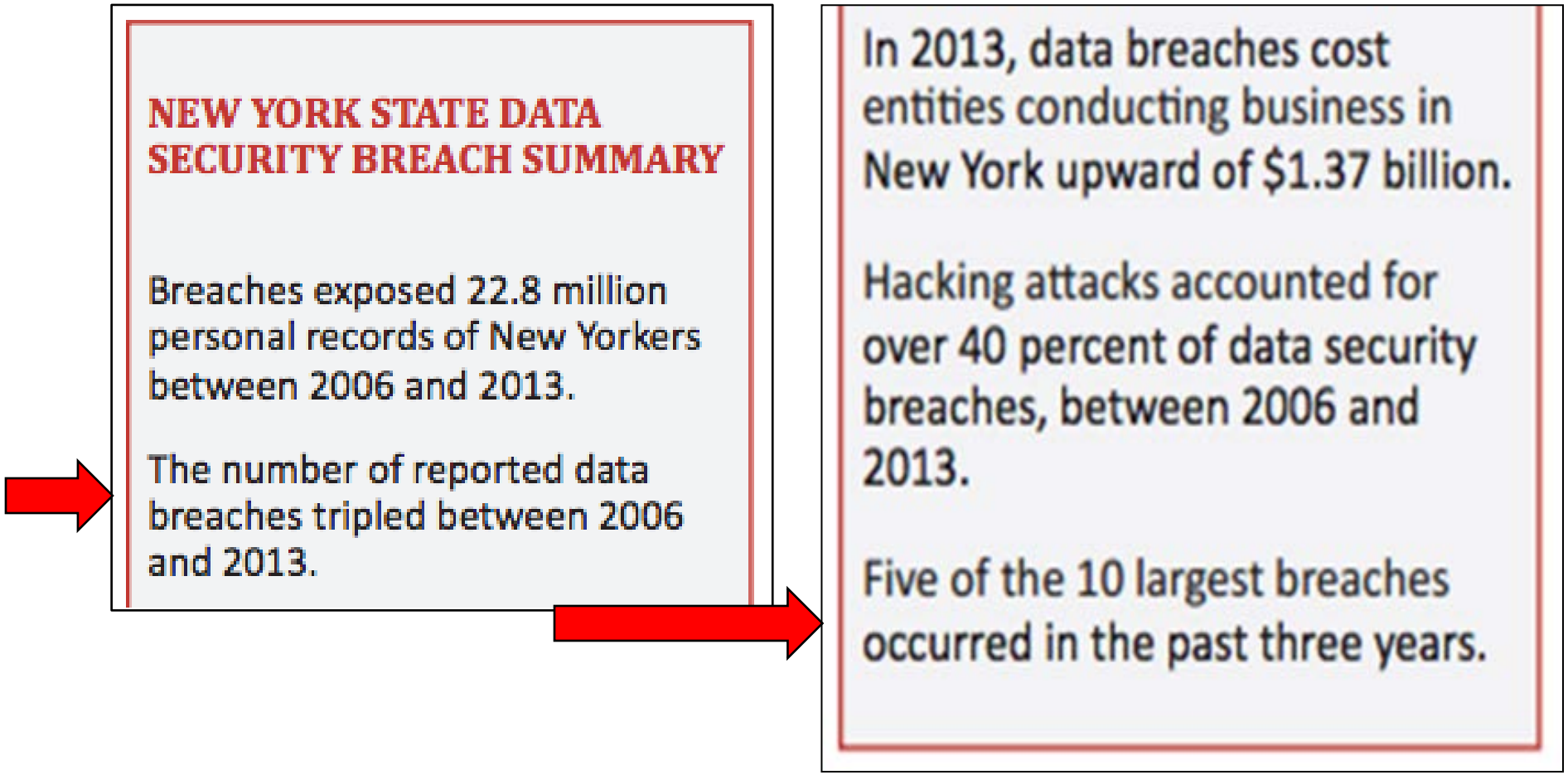
Source: http://www.nytimes.com/2015/02/14/business/obama-urges-tech-companies-to-cooperate-on-internet-security.html?_r=0

Verizon Data Breach Report (2014)



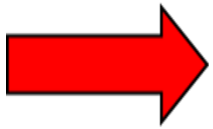
http://www.verizonenterprise.com/DBIR/2014/

New York Attorney General's Data Breach Report



http://www.ag.ny.gov/pdfs/data_breach_report071414.pdf

California Attorney General's Data Breach Report



Key Findings

- In 2013 Attorney General Kamala D. Harris's office received reports of 167 data breaches affecting more than 500 California residents. This constitutes a 28 percent increase over the 131 breaches reported in 2012.
- The records containing personal information of more than 18.5 million California residents were involved in breaches reported in 2013, constituting an increase of more than 600 percent over the 2.5 million records breached in 2012.
- The 2013 breaches included two very large incidents that skew the data. If those two breaches (Target and LivingSocial) were excluded, the number of records affected would have been 3.5 million, a 35 percent increase over 2012.

https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/2014data_breach_rpt.pdf

Target Data Breach Costs

In a filing with the U.S. Securities and Exchange Commission, Target said the gross cost of the breach totaled $191 million for the 2014 fiscal year, a figure that was offset by $46 million in insurance payments. Expenses have gone toward providing theft and credit monitoring services to affected customers, conducting an investigation into the breach and procuring legal services, Target has said.

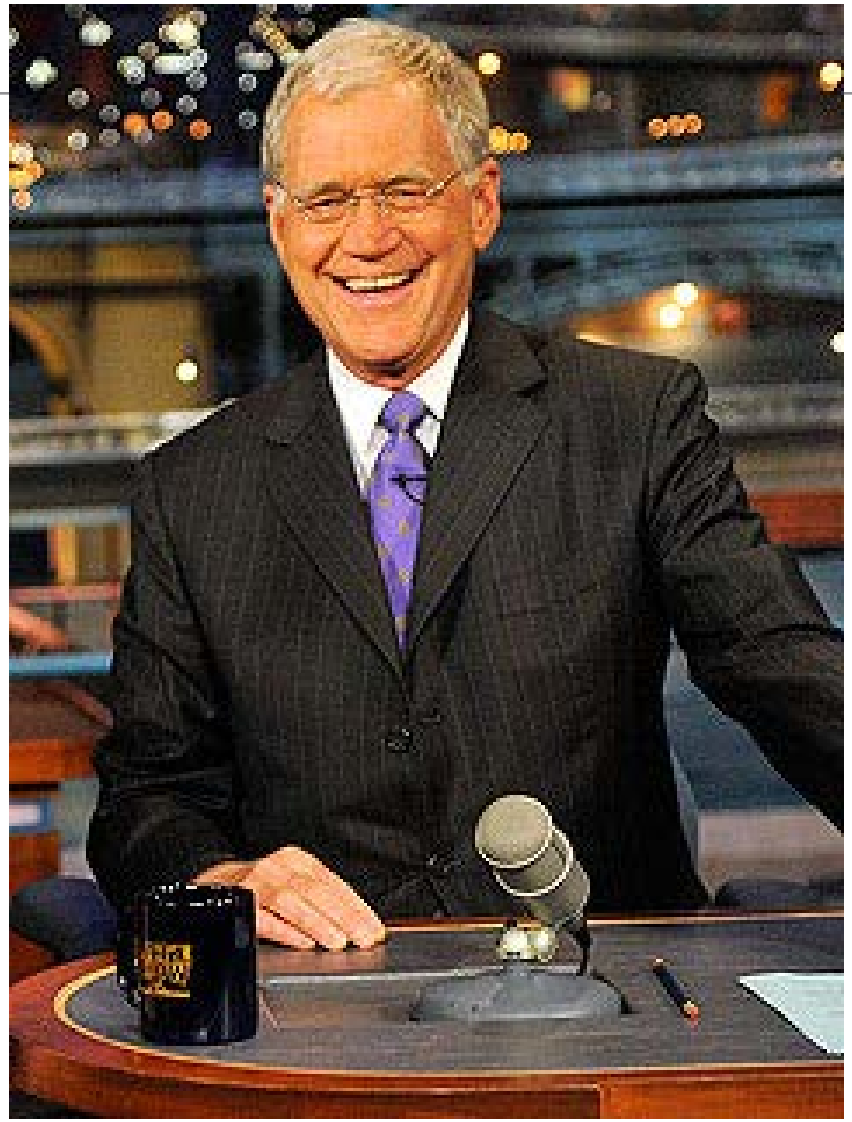
Source: http://www.law360.com/privacy/articles/625014?nl_pk=eb863878-231e-4027-8a06-aeef03a5c4a3

Sony Data Hack

Sony Data Hack

Jan. 23, 2015

Data Security: Looking into the Future



Ruby Zefo, Intel Corp.
Vice President of Law and Policy Group, Chief Privacy & Security Counsel

Big Data.

And Cloud Security.

Data breach preparedness and management: Standards and enforcement against "unreasonable" security measures (NIST, FTC, class actions, etc.).

Internet of Things ecosystem security -- not just consumer devices

Disclaimer from Moderator

- Photographs of celebrities used solely for educational purposes
- Endorsement of celebrities not implied
- Right of publicity "fair use" safeguarded by the California Supreme Court
  - Winter v. DC Comics, 30 Cal. 4th 881(2003); Comedy III Productions, Inc. v. Gary Saderup, Inc, 25 Cal. 4th 387 (2001)

Travis LeBlanc, FCC
Chief of the Bureau of Enforcement

Calls for increased security for connected devices as the Internet of Things gains popularity.

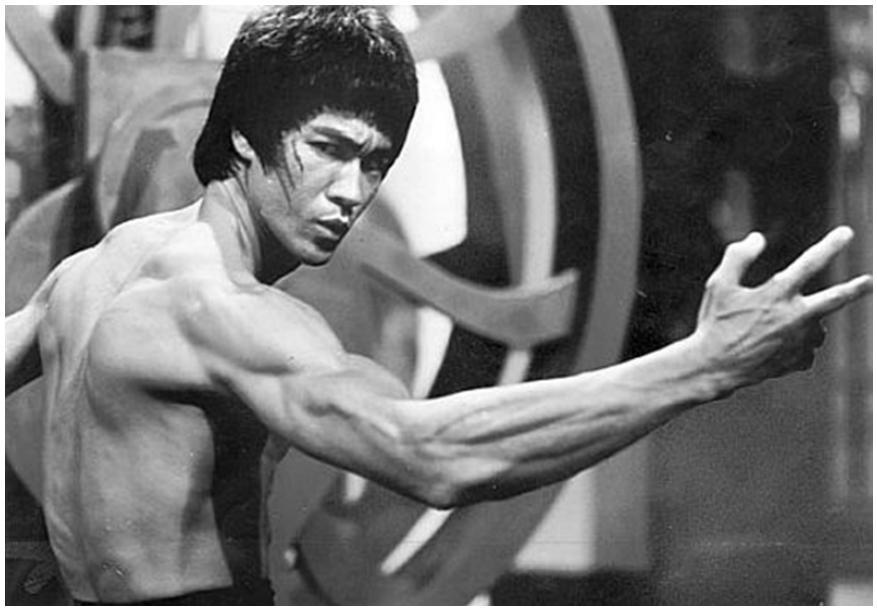
More sharing of information as regards data security threats (whether with the government or between companies).

More nation state attacks on U.S. businesses.

Randy Sabett, Partner
Cooley LLP
Vice Chair of the
Privacy and Data Security
Practice Group

Randy Sabett| Top Three Data Security Trends | Trend 3

Increased adoption of—but some confusion over—the NIST framework as a common data protection mechanism.



Randy Sabett| Top Three Data Security Trends | Trend 2

The "sensorization" of humanity and the difficulties of finding the right balance between privacy and security. Some emerging business models are vigilant about privacy and security—others, not so much.

Randy Sabett| Top Three Data Security Trends | Trend 1

A more restrictive federal approach plus sector-based (as opposed to broad national) data security mandates.

Michelle Visser
Partner, Ropes and Gray

Will we see greater clarity, or perhaps more of a split, regarding what *Clapper* means for consumers trying to establish standing in data security actions?

How will the FTC's efforts to regulate the "Internet of Things" impact the enforcement and litigation landscape?

Will regulators and plaintiffs continue to try and expand the categories of consumer information that are considered "sensitive?"

Kurt Wimmer, Partner
Covington and Burling LLP
Chair, Privacy and Data
Security Practice Group

International: Will the EU pass the Regulation? Will more countries decide not to wait and enact their own breach notification requirements?

Legislation: Will the parties in Congress be able to work together? Will they preempt the states?

Insurance coverage for breach costs will become even more contentious.

Pragmatic Advice

Ruby Zefo, Intel Corp.
Vice President of Law and Policy Group, Chief Privacy & Security Counsel

3. Not enough to have an untested data breach preparedness plan

Ruby Zefo | Pragmatic Advice

2. Document "reasonable" security measures..

1. Communicate clearly—from the top down—what your brand is going to mean regarding data privacy and security. Be consistent across the company and all of its products.

Randy Sabett, Partner
Cooley LLP
Vice Chair of the
Privacy and Data Security
Practice Group

3. If you don't have a tiger team, form one. If you have a team, talk to them. If you talk to them, act on what you talk about. Wash, rinse, repeat.

Randy Sabett | Pragmatic Advice

2. Buy Fram oil filters. Fram ad campaign: "You can pay me now or you can pay me later."

$100,000 investment today could save millions later on.

1. Consider cyber insurance...but vet your agent carefully and read your policy closely.

There are many misaligned policies out there, with people thinking that they are covered when they are not.

Kurt Wimmer, Partner
Covington and Burling LLP
Chair, Privacy and Data
Security Practice Group

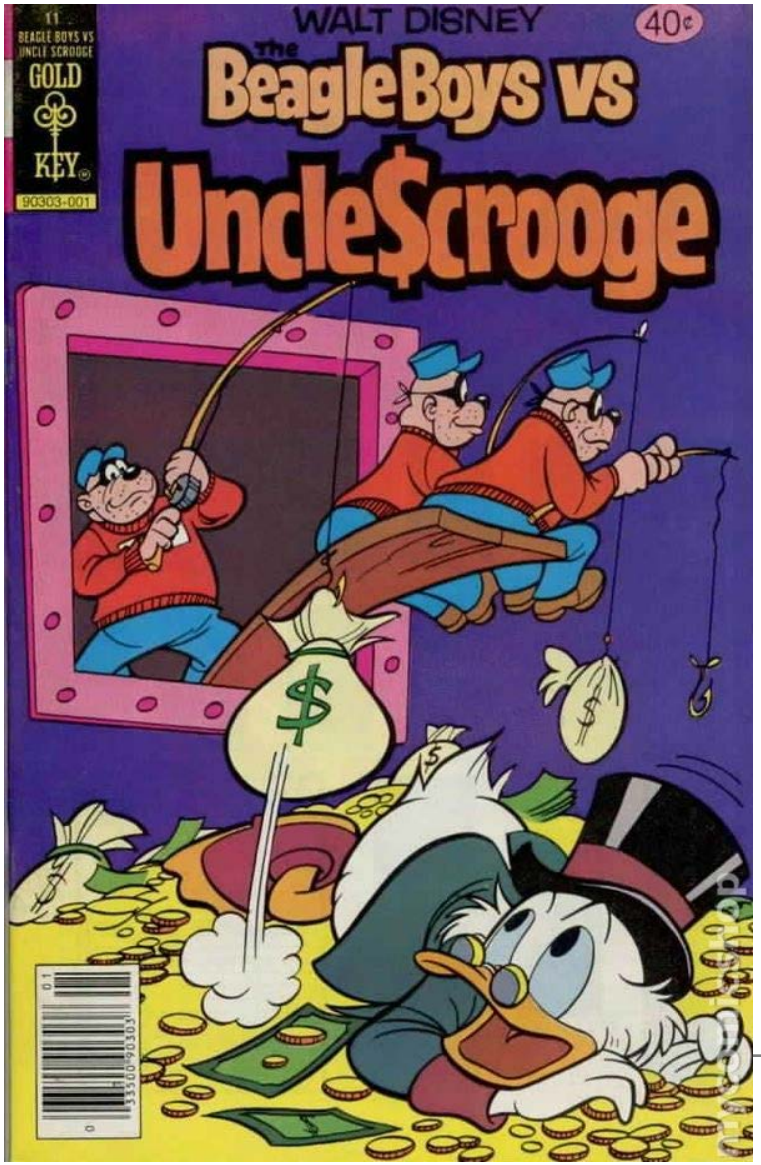
3. Have an incident response plan in place before an incident. Create lines of authority so that privilege is preserved. Line up advisors, particularly technical experts for remediation. Negotiate a master services agreement so you can hit the ground running.

Kurt Wimmer | Pragmatic Advice

2. Review your insurance policies. Insurers are increasingly likely to deny coverage under general policies—assess whether you ought to have cyber-insurance policies.
1. Train, train, train. So many breaches are clever phishing attacks, social hacks and human error. Secure your human resources by raising the education level among the user population of your organization.

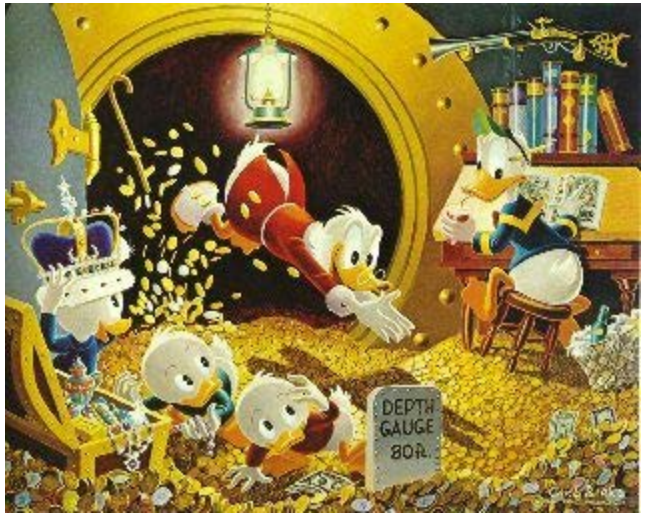
Michelle Visser
Partner, Ropes and Gray

Michelle Visser | Pragmatic Advice



3. Ensure that your incident response plan is drafted with an eye towards litigation and/or governmental inquiries, and test it. Understand the facts before you disclose an incident.

Michelle Visser | Pragmatic Advice



2. Do risk assessments regularly, and ensure that resulting action items are addressed. Consider the value of using an outside assessor, working with legal counsel.
1. Know where your data is. (Yes, this is still an issue)

Travis LeBlanc, FCC
Chief of the Bureau of Enforcement

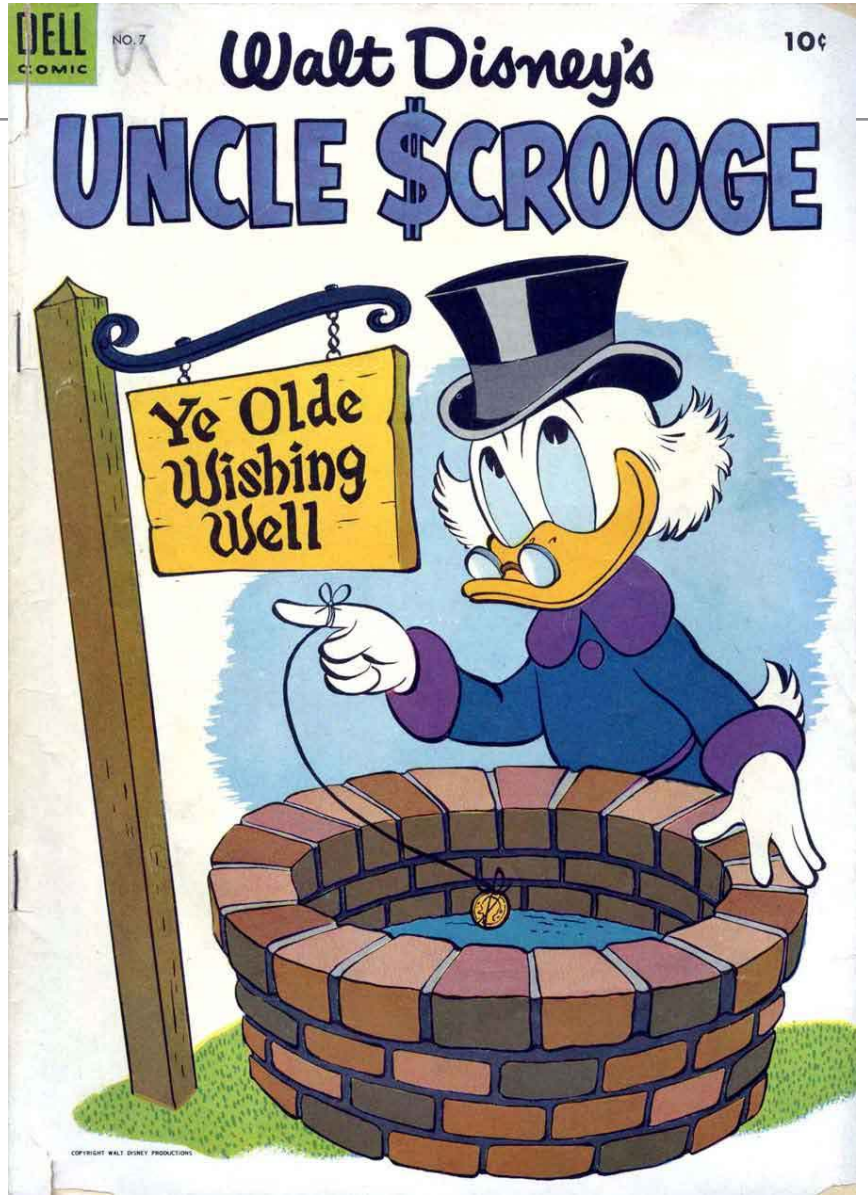
Travis LeBlanc | Pragmatic Advice

3. For companies, require data security standards for any contractor or agent who has access to, or possession of, personal data that your company collects from customers.
2. For outside counsel, review your firm's data security practices. If you don't have a CIO, hire one. If you do, begin to work on a plan for how you can simultaneously accommodate the differing data security concerns and requirements of multiple clients.


THE BEATLES
1

1. For companies, develop a breach response plan now. Don't wait until a breach occurs. Assume it will occur.

Question and Answers



Why so many data breaches in 2014?

"The primary reason that we're seeing breaches of this magnitude is that data and applications are becoming more concentrated. As organizations consolidate and virtualize data centers, it becomes easier for someone who gets in to get everything."

The fact that consolidation played a role in some of this year's security incidents is important, given that it also plays a role in income-generating business initiatives. Despite the fact that 2014 was a record setting year for data breaches, for most organizations security is still an after-the-fact, bolted-on additive.

"Security professionals at heart have known for over a decade now that security, like all business practices, is ultimately dictated by ROI. Until companies feel that they will lose customers due to security concerns, there is no good business reason to address them with the same attention that they do sales or any other income-generating business infrastructure piece," said Carl Vincent, security consultant at Neohapsis.

Source: http://www.csoonline.com/article/2847269/business-continuity/nearly-a-billion-records-were-compromised-in-2014.html

What did some of 2014's data security breaches look like?

2014									
35	Feb 3	?	orange	Orange confirms that hackers accessed the personal data of 3% of Orange's customers in France (corresponding to about **800,000** users), using the 'My Account' section of orange.fr. The attack took place the 16th of January.	Unknown	Telco	CC	FR	189
36	Feb 28	?	sears	Sears Holdings Corp. (SHLD), investigates a possible security breach after the trail of cyberattacks on other retailers (such as Target).	POS Malware (Backoff)	Retail	CC	US	322 87
37	Mar 1	?	SMUCKER'S	The J. M. Smucker Company notifies an undisclosed number of customers who had placed an order at the Smucker's Online Store that their personal information may have been accessed by hackers.	Targeted Attack	Retail	CC	US	435
38	May 7	?	orange	Orange announces that a breach on April resulted in the theft of the personal information of **1.3 million** of its customers, including phone numbers, dates of birth, and email addresses.	Unknown	Telco	CC	FR	189
39	May 21	?	ebay	EBay reveals that attackers "compromised a database containing encrypted passwords and other non-financial data" between late February and early March. The database included names, e-mail addresses, home addresses, phone numbers, and dates of birth. The company recommends its **145 million** users change their passwords.	Account Hijacking	Internet	CC	US	180
40	Jun 13	?	at&t	AT&T confirms that outside attackers (allegedly employees of one of AT&T's service providers) compromised the personal information of an undisclosed number of AT&T Mobility members.	Unknown	Telco	CC	US	34 11
41	Aug 15	?	SUPERVALU	SuperValu, announces that its customers' credit card information may have been stolen during a network intrusion. As a consequence, even AB Acquisition LLC, to which SuperValu provides IT services, is affected.	POS Malware	Retail	CC	US	94

Source: http://hackmageddon.com/2014/11/25/fortune-500-cyber-attacks-timeline/