

Welcome to the 2015 Cyber Risk Insights Conference!



@Advisen #CyberRisk

Opening Remarks



Bill Keogh
CEO
Advisen



@Advisen #CyberRisk

Leading the way to smarter and more efficient risk and insurance communities, Advisen delivers:

- the **right** information into
- the **right** hands at
- the **right** time

to *power* performance.

Thank you to our Sponsors

 **NAS** insurance

 **KIVU**

 **AllClearID**

 **beazley**

 **TRAVELERS**

 **McGladrey**



CYBER RISK **NETWORK**

Insurance Intelligence for the Cyber Community

For more information about subscriptions
contact Jim Delaney at jdelaney@advisen.com

Welcoming Remarks



Garrett Koehn

President Northwestern US, Regional Director
CRC Insurance Group
[2015 Conference Chair]

Cyber Security 2015

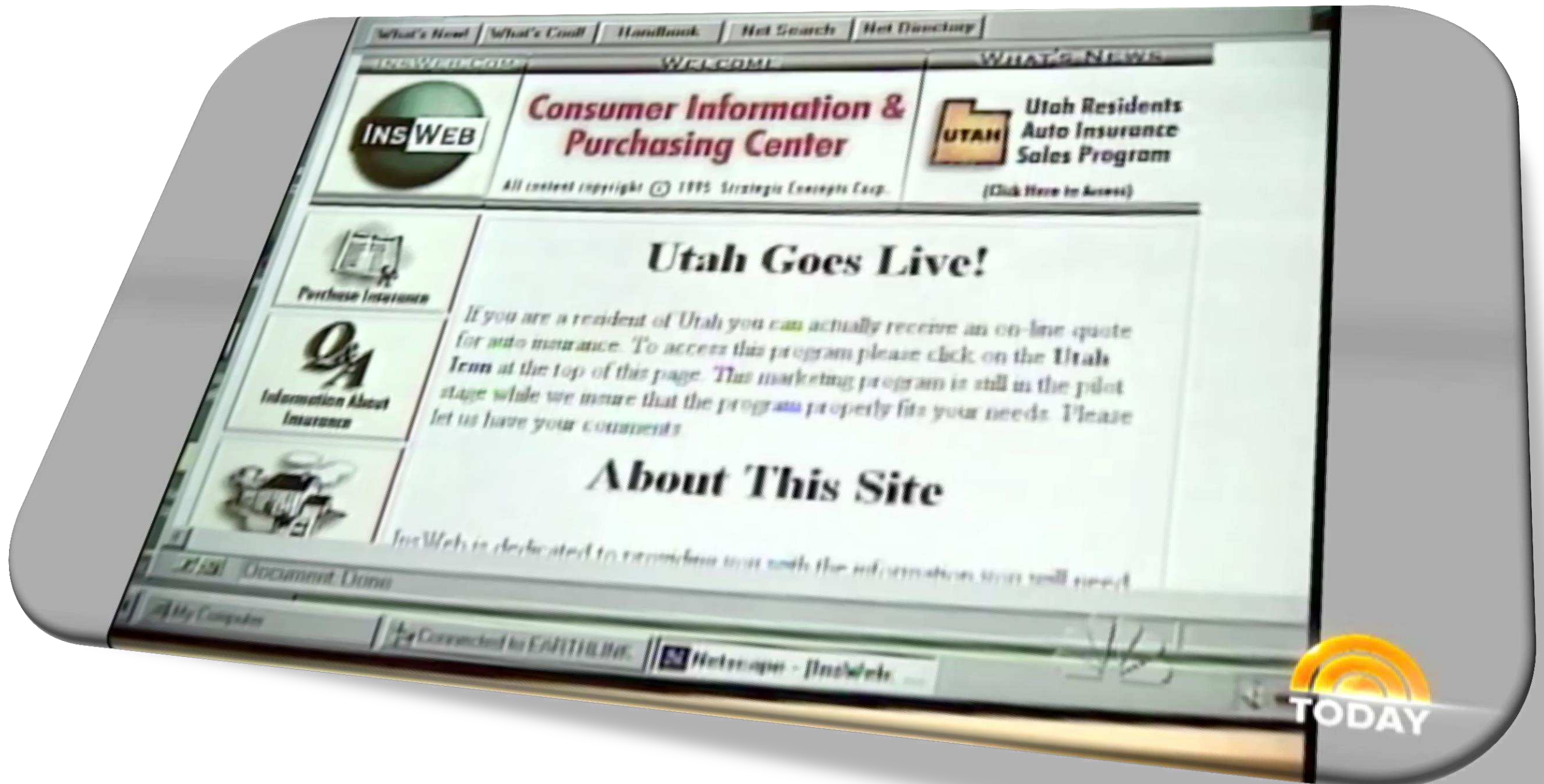
20-years of Insuring the WWW

Garrett Koehn

President NWUS, CRC

[@KoehnGarrett](#)

What is “Internet”? (1994-5)



The Cyber Past

- Guessing at what the exposures might be
- No comprehensive specific insurance coverage available
- Difficult to see what we don't know...



New in 1995

- **THE INTERNET**

- The dot-com boom starts
- Yahoo.com domain registered in January
- Amazon.com opens in July
- Internet Explorer launched in August
- eBay opens in September
- the first **wiki** created (Portland Pattern Repository)
- New lexicon:
 - @
 - “Browser”
 - “Search Engine”
 - “Surfing”

- **THE CONCERNS**

- Only tech companies concerned
- User generated content
 - Bodily injury
- Intellectual Property
- Hackers / Virus
- Commerce
 - Safety of data (credit cards)
 - Quality of purchases
- International / Village laws
- Privacy
- Pornography

The Cyber Insurance Market 1995

- No Specific Comprehensive Products
 - Media
 - E&O
 - Crime
 - Computer (not internet) specific
 - Hacker/Virus specific
 - Property (data)
 - GL (advertising)



The Cyber Insurance Present

- Betterley Report – June 2014 29-Markets offering coverage specifically for “cyber insurance”
- No longer a nascent market, but highly dynamic and growing
- Policies are not fungible – each is highly differentiated and in many ways still reflect the puzzle of the mid-1990’s compilations
- Current Cyber Market estimated at \$2-3 billion; targets of \$80 billion



Today

THE INTERNET

- Tech attacks everyone
 - Retail
 - Taxis
 - Hotels
 - Financial Services
 - things
- Things** (doors, tv, picture frames, piano, security, light bulbs, dish washer)
- BYOD**
- “Cloud”
- Mobile**
- Access to **EVERYTHING** on-line
 - Money
 - IP
 - Personal Information
 - “BitCoin”
- “Crowdfunding”
 - **Tools** – exploit kits
- Military or Nation State attacks
- “SPAM” – “Malware”
- 3D Printing

THE CONCERNS

- “Old” and growing Concerns:
 - HACKERS
 - Blackmail
 - Home Automation Systems
 - BYOD
 - “Hacktivists” and State-Sponsored Attackers
 - Complex Data
 - Privacy
 - Loss of financial information or theft
- “New” concerns
 - It is a concern of every company
 - SPAM (snowshoe), malvertising
 - Employee Data
 - Theft of Trade Secrets
 - PR and Instant Information
 - Huge Vendor threats
 - Banking “trojans”
 - Incident response
 - Board Level Controls
 - First Party Losses

Recent Events of Interest!!!

Cyber bank robbers steal \$1bn

Kaspersky report



- Kaspersky Lab estimates \$1bn has been stolen in the attacks, which it says started in 2013 and are still active
- A cybercriminal gang with members from Russia, Ukraine and China is responsible
- It said the attacks had taken place in 30 countries

Samsung warns that customers should.

Things

- “Be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition.”



14-year Old Hacks Car With \$15 of Parts



- He was able to remotely hack into a car with nothing but a handful of parts from [RadioShack](#) and an iPhone in one day.
- The next day, he was able to operate the vehicle's wipers, lights, door locks, and even the remote start feature.
- He even played a song from his phone through the car's speakers, flashing the headlights to the beat in a clever taunt.

Insecam Displays Unsecured Webcams From Around The World

- 73,000 unsecured webcams from around the world, most of them CCTV and simple IP cameras. All of the cameras have two things in common – they're streaming on publicly accessible network ports and they are still using the default passwords



A new Cyber division in the US Army -- CTIIC

- A new cyber agency is about to be established. This new agency, named CTIIC an acronym for (Cyber Threat Intelligence Integration Center),
- Coordinating various agencies, such as the CIA, NSA, DHS, FBI and the US military Cyber Command.
- Requires the agencies to share information



SPAM /Malware

SPAM!

- SPAM Volume increased 250% from January to November 2014 – Cisco 2015 Report
- In 2014 the pharmaceutical and chemical industry emerged as the number-one, highest risk industry vertical for malware exposure
- Bootkits represent the most advanced technology in this area, allowing malicious code to start before the operating system itself loads.



North Korea v. Sony



The White House believes North Korea to be ultimately responsible for the cyber attack on Sony

Angelina Jolie Blasted as "Minimally Talented Spoiled Brat" by Producer Scott Rudin in Leaked Sony Emails

The past does not = the future

Who Predicted...

- Bitcoin
- Uber
- LMAO
- Llamasontheloose
- Snapchat
- Hot Spots
- IP addresses
- Trolling



The past does not = the future

Who Predicted...

- B itcoin
- U ber
- L MAO
- L lamasontheloose
- \$ napchat
- H ot Spot
- ! P addresses
- T rolling



The Future?

- [Elon Musk](#) has spoken out against **artificial intelligence** (AI), declaring it the most serious threat to the survival of the human race.
- Musk made the comments to students MIT talking about computer science, AI, space exploration and the colonization of Mars.



THANK YOU!!
(TTFN!!)

Garrett Koehn
President NWUS, Regional Director CRC

415-675-2278

gkoehn@crcins.com

[@KoehnGarrett](#)

- <http://www.whitehouse.gov/the-press-office/2015/02/25/presidential-memorandum-establishment-cyber-threat-intelligence-integrat>
- <http://www.eweek.com/security/slideshows/five-things-hackers-are-doing-with-victims-data-in-2015.html>
- http://www.theregister.co.uk/2015/01/31/ye_olde_laptoppe_is_back_after_byod_backlash/
- <http://www.digitaltrends.com/cars/14-year-old-hacker-breaks-into-car/>
- <http://wallstcheatsheet.com/politics/obama-imposes-sanctions-on-north-korea-in-response-to-destructive-sony-hack.html/?a=viewall>
- <http://www.usmagazine.com/celebrity-news/news/angelina-jolie-called-spoiled-brat-by-scott-rudin-in-leaked-emails-20141012>
- <http://securelist.com/analysis/quarterly-malware-reports/65340/it-threat-evolution-q2-2014/>
- <http://techcrunch.com/2014/11/07/insecam-displays-insecure-webcams-from-around-the-world/>
- <http://www.theguardian.com/technology/2014/oct/27/elon-musk-artificial-intelligence-ai-biggest-existential-threat>
- 2015 Cisco Annul security Report
- Digital Life in 2025 – PewResearchCenter
- Managing Cyber Risks with Insurance – PWC June 2014
- Advisen October 2014 Cyber Liability Insurance Trends

Keynote Address



David Johnson

Special Agent in Charge of the San Francisco Division
FBI

Cyber Market Metrics



Jim Blinn
Executive Vice President
Advisen



Insurance Intelligence for the Cyber Community

Cyber Market Metrics are available to
members of the Cyber Risk Network only.

For more information about subscriptions
contact Jim Delaney at jdelaney@advisen.com

Reputational Risk



@Advisen #CyberRisk

Reputational Risk

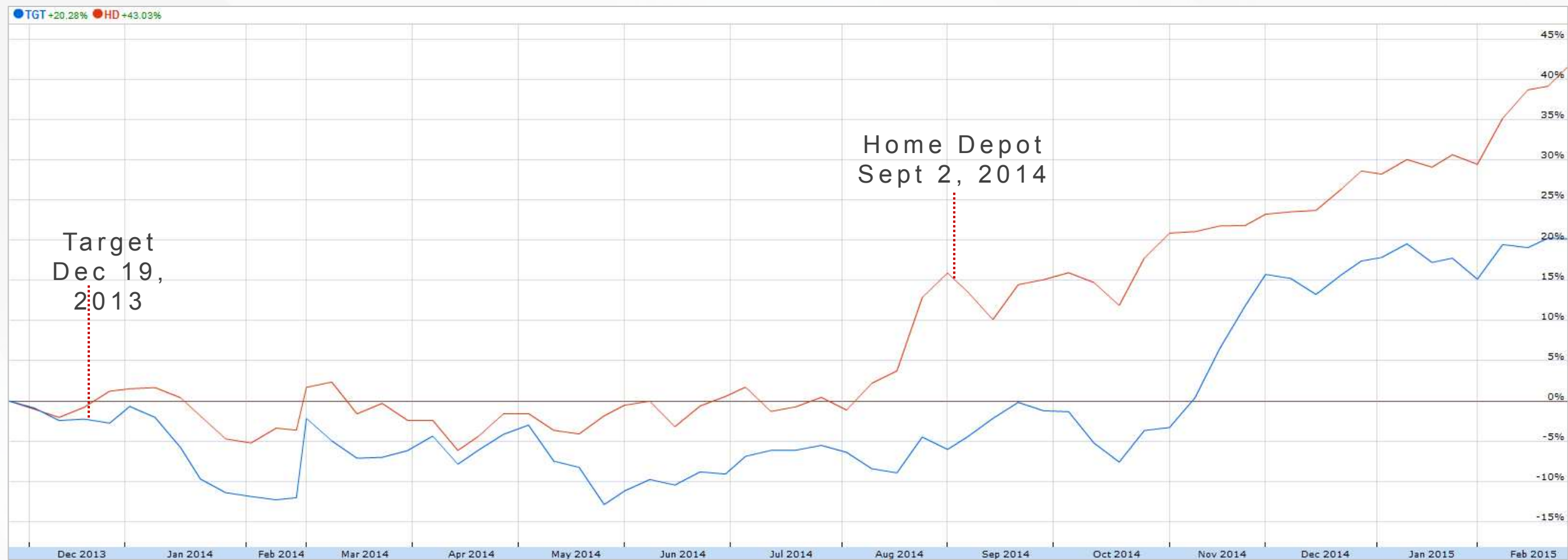


Bo Holland
Founder & CEO, AllClear ID
Moderator

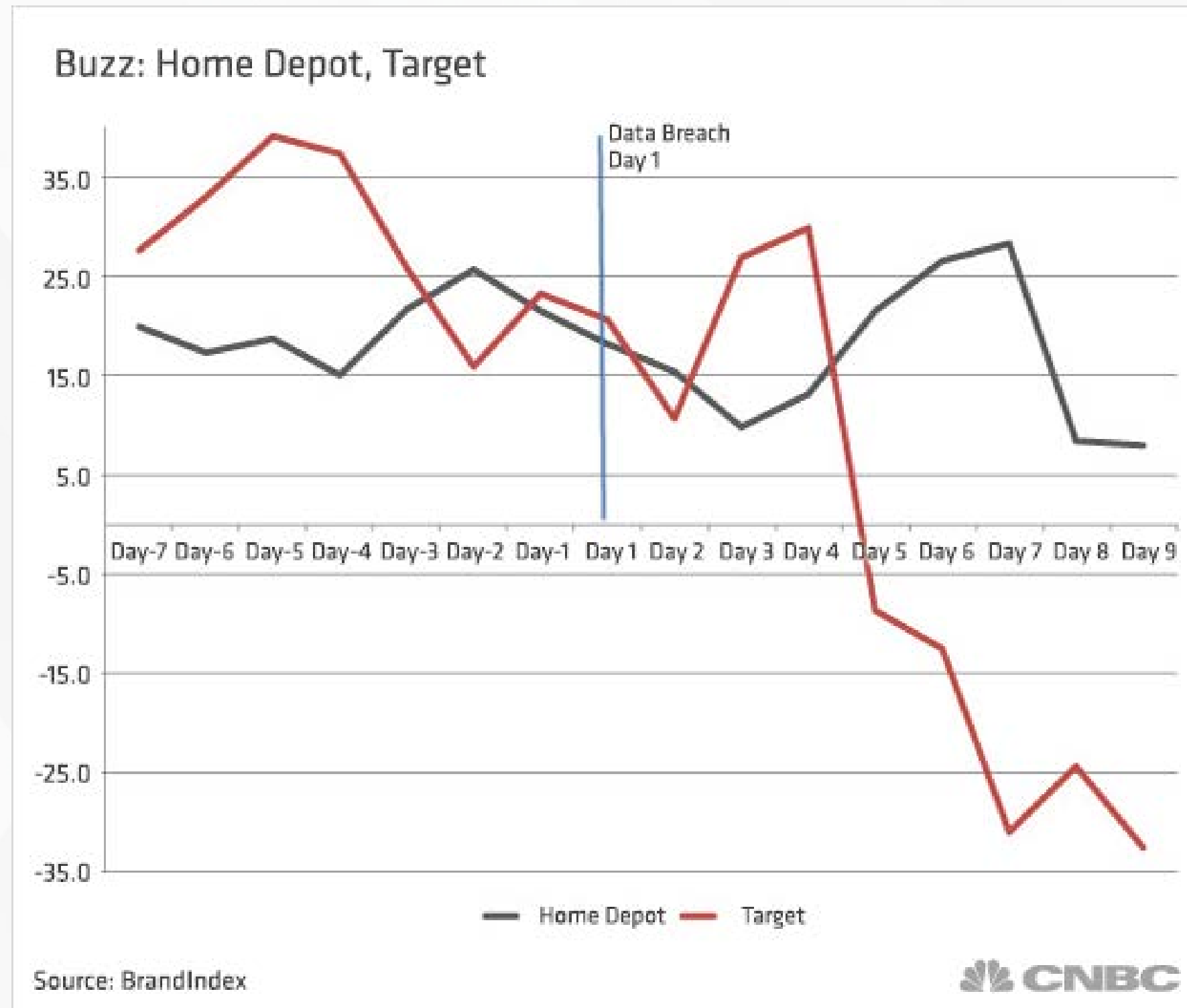
Reputational Risk

- **Bo Holland**, Founder and CEO, AllClear ID (Moderator)
- **George Little**, Partner, Brunswick Group
- **Michael Palotay**, Senior Vice President, Underwriting, NAS Insurance
- **Steve Rosen**, Managing Partner, President, Public Relations, Star Group

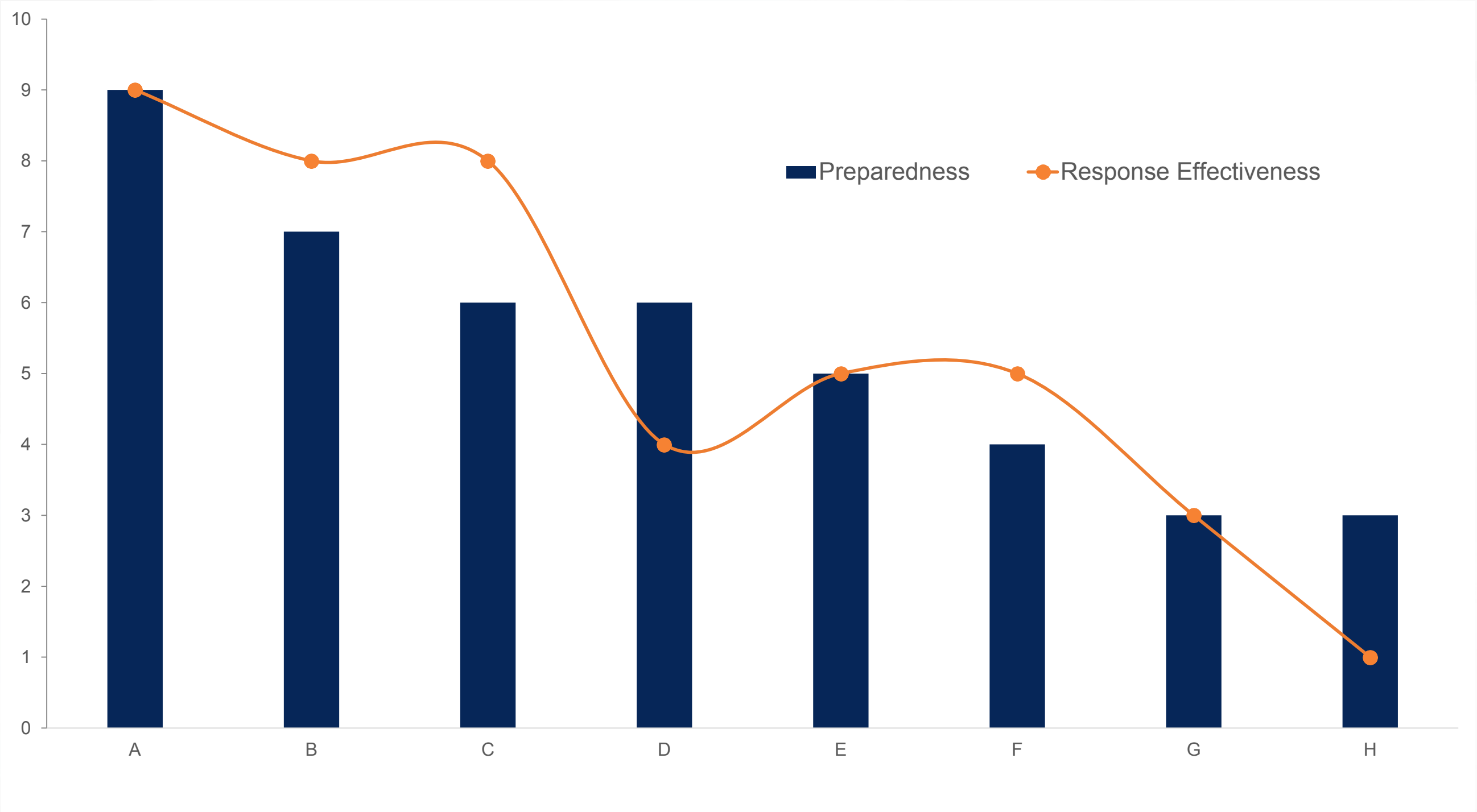
Impact on Stock Price: Home Depot vs. Target



Brand Perception: Home Depot vs. Target



Preparedness & Breach Response Effectiveness



Brian Krebs
Investigative Security Reporter

Will you be ready?
BRIAN KREBS
IS CALLING



Reputational Risk



Harnessing the Numbers



@Advisen #CyberRisk

Harnessing the Numbers



Wayne Wickham
Knowledge Manager, Advisen
Moderator

Harnessing the Numbers

- **Wayne Wickham**, Knowledge Manager, Advisen (Moderator)
- **Neil Furukawa**, Chief Operating Officer, CyberPoint International
- **John Plaisted**, Senior Vice President, Global Analytics Practice, Marsh
- **Mark Synnott**, Managing Director, Executive Vice President, Willis Re
- **Peter Ulrich**, Senior Vice President, RMS

Harnessing the Numbers



Thank you to our Sponsors

 **NAS** insurance

 **KIVU**

 **AllClearID**

 **beazley**

 **TRAVELERS**

 **McGladrey**

Who goes there?!



@Advisen #CyberRisk

Who goes there?!



Rebecca Bole

Director of Editorial Strategy & Products, Advisen
Moderator



**This is Rebecca Bole,
Advisen's Director of
Editorial Strategy &
Products and host of
the Cyber Risk
Awards!**

Weds June 17 in NYC

Who goes there?!

- **Rebecca Bole**, Director of Editorial Strategy & Products, Advisen (Moderator)
- **Gary Golomb**, Co-Founder, Awake Networks
- **John McGloughlin**, CEO, GuardSight

Who goes there?!



Regulatory Update: The West Coast



@Advisen #CyberRisk

Regulatory Update: The West Coast



Kimberly Horn

Claims Manager, Technology, Media & Business, Beazley

Regulatory Update: The West Coast

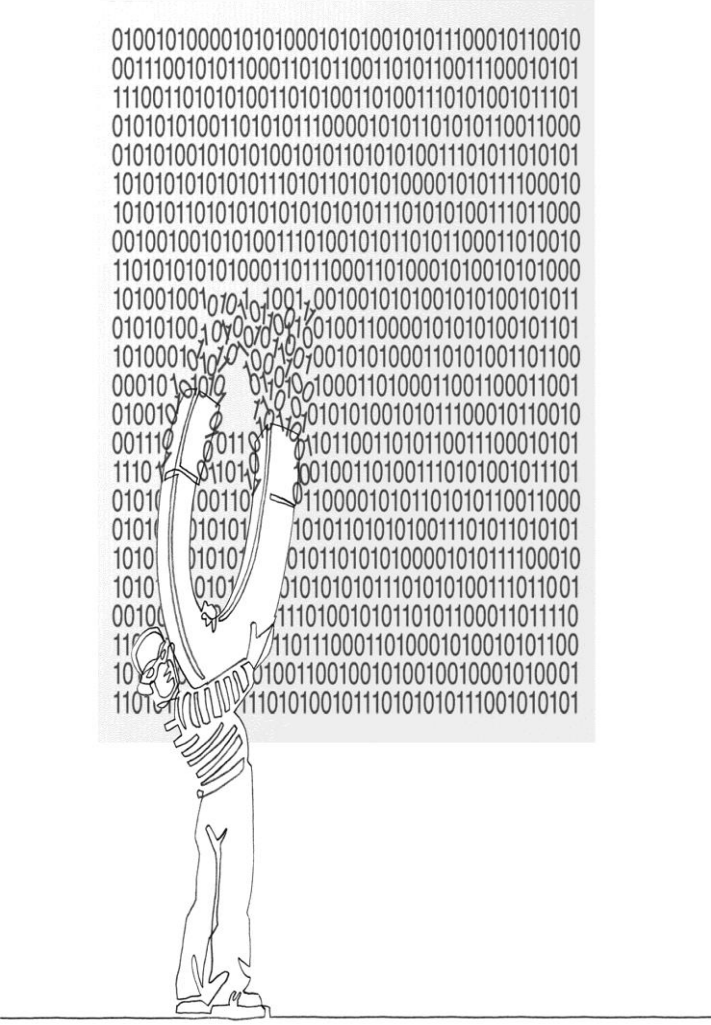
How Do Recent Regulatory Developments on the West Coast Sit With President Obama's Call For a National Breach Law?

**Kimberly Horn
Beazley
March 3, 2015**

beazley

Topics

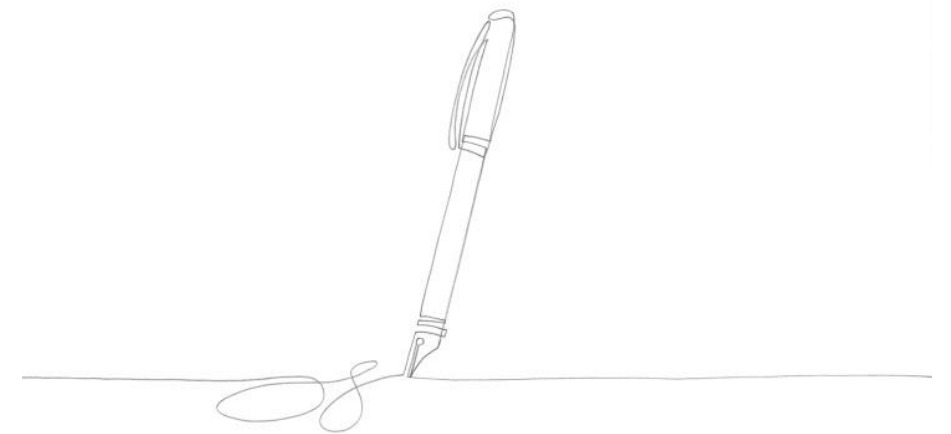
- I. The Current Legislative and Regulatory Landscape**
- II. Statutory Developments on the West Coast**
- III. National Data Breach Notification Standard**
- IV. What are the West Coast Regulators Up to?**
- V. Regulatory Hot Buttons**
- VI. Other Regulators to Watch**
- VII. Q&A**



```
01001010000101010001010010101100010110010
00111001010100011010110011010110011100010101
1110011010100110101001101001110101001011101
0101010011010101110000101011010110011000
01010100101010010101101010011101011010101
101010101010111010110101010000101011100010
1010110101010101010111010100111011000
00100100101010011101001010101100011010010
1101010101000110111000110100010100101000
1010010010101001001001001010010100101011
0101010010101001001001001001010100101101
10100010101010010010101000110101001101100
0001010101010101000110100011001100011001
01001010101010101010101011100010110010
0011101010101010101010101110001010101
11101010101010101010101011101001011101
010101010101010101010101011000101011000
01010101010101010101010101110101010101
10101010101010101010101010111100010
10101010101010101010101010111011001
0010010101010101010101010111010001101110
1101010101010101010101010111000110101100
1010101010101010101010101010001010001
1101010101010101010101010111001010101
```

The Current Legislative and Regulatory Landscape

- There is currently no nationwide data breach notification statute
 - HITECH is the exception for breaches of PHI
- 47 states (plus D.C., Puerto Rico and the Virgin Islands) have individual data breach notification statutes that vary
 - Most modelled on the pioneering California statute, which came into effect in 2003
 - States without notification statutes: Alabama, New Mexico and South Dakota
- Residency dictates
 - The residency of the affected individuals dictates applicable law
- Enforcement varies
 - State regulators: investigations and fines
 - Private rights of action



The Current Legislative and Regulatory Landscape (cont.)

- Unencrypted electronic personal information
- Standard definition of personal information, with some variation
- Statutes triggered upon discovery of unauthorized acquisition or use
- Risk of harm trigger in some states
- Written notice requirements vary
 - Notice to affected individuals, relevant regulators, consumer reporting agencies
- Typically, disclosure of the breach must be made

... in the most expeditious time possible and without unreasonable delay ...

- Fixed deadlines in some states

The Current Legislative and Regulatory Landscape (cont.)

Standard Definition of “Personal Information”

- First name or initial and last name plus one or more of the following data elements:
 - SSN;
 - driver’s license number or state-issued ID card;
 - account number, credit card number or debit card number combined with any security code, access code, PIN or password needed to access an account
- Personal information does not include:
 - publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media

Statutory Developments on the West Coast

California

Amendments to General Breach Notification Statute

Effective January 2014: “Personal Information” Definition Expanded

- Includes “a username or email address, in combination with a password or security question and answer that would permit access to an online account”
- For username/email/password breaches, electronic notice permitted
 - Directing person to change his or her password and security question or answer, as applicable, or to take other appropriate steps to protect the online account in question and all other accounts for which that person uses the same credentials

Statutory Developments on the West Coast (cont.)

Effective January 2015: Expanded Application & Remedial Measures

- Companies that “maintain” personal information now trigger the law
 - Implementation of reasonable security procedures and practices to protect PI
- Prohibition on the sale, advertisement and offer to sell SSNs
- Offer to provide identity theft prevention and mitigation services

“
... an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected individuals for not less than 12 months ...
”

Statutory Developments on the West Coast (cont.)

California

Amendments to Medical Information Breach Notification Statute

- California has a separate statute that governs breaches involving medical information
 - Only applies to licensed healthcare providers

Effective January 2015: Notification Deadline Extended

- Affected patients and the Department of Public Health must be notified no later than **15 business days** after the unauthorized access, use or disclosure has been detected
- Penalties remain unchanged: \$100 per day penalty (not to exceed \$250K per reported event) for failure to notify affected patients or CDPH within the 15 day time period

Statutory Developments on the West Coast (cont.)

Oregon

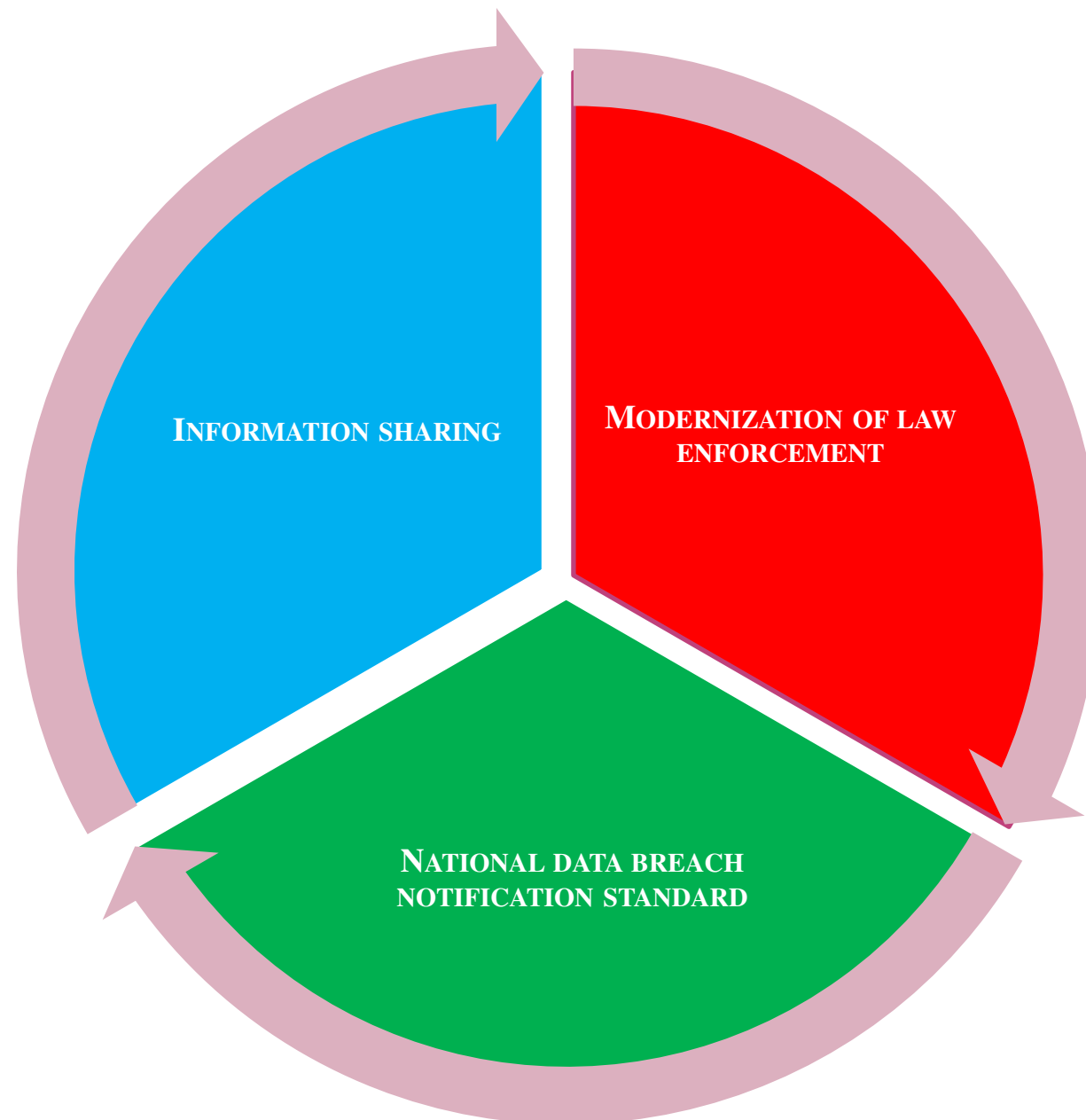
- Personal Information: standard definition + passport number or other US government issued ID number
- Persons Covered: any person that owns, maintains or otherwise possesses data
- Trigger: statute does not apply to encrypted **or redacted** PI; includes a risk of harm test
 - Is the breach reasonably likely to result in harm to the consumer?
- Penalties: violations of the notification law can garner a penalty of not more than \$1000 per violation, and no more than \$500K total
- Other Reporting Obligations: breaches affecting more than 1000 consumers require notice to all consumer reporting agencies.

Statutory Developments on the West Coast (cont.)

Washington

- Personal information: standard definition
- Persons Covered: any person that owns or licenses computerized data
- Trigger: statute does not apply to encrypted PI; includes a risk of harm test
 - Is the breach reasonably likely to subject customers to a risk of criminal activity?
- Private Right of Action: permitted
- Other Reporting Obligations: licensees must provide notice to WA Insurance Commissioner

The Obama Administration's Cyber Security Agenda



National Data Breach Notification Standard

Personal Data Notification & Protection Act

Goals of the Legislation

- Standardizing the current patchwork of 47 individual state laws
- Creating a single, clear and timely notice requirement

Key Provisions

- Sensitive Personally Identifiable Information (“SPII”): very broadly defined
- 30 day notification deadline, with option for FTC-approved extension
- Risk of harm assessment to be reported to the FTC within 30 days of discovery
- Notification to federal law enforcement and national security authorities
- Media notification in any state with more than 5,000 affected individuals
- FTC to enforce compliance with the statute; state AGs can commence civil actions and levy fines

National Data Breach Notification Standard (cont.)

Conclusions

- Applies to a much broader set of information
 - SPII more broad than any current definition of Personal Information
 - SPII definition can be modified by the FTC
- Uncertainty surrounding the risk assessment and the FTC's role
- Likely debate over preemption
- Would the law really allow for a one size fits all notice?
 - States would still be allowed to require notices to include information on state-provided victim protection assistance

What are the West Coast Regulators Up to?

- State Attorneys General
 - Of the 3 West Coast AGs (CA, WA, OR), California is by far the most aggressive
 - Dedicated Privacy Enforcement and Protection Unit
 - Lawsuit vs. Kaiser for untimely notification
- California Department of Health
 - Fines for late notice
 - Fines up to \$25K per patient for unlawful disclosure or unauthorized access or use
- The Office of Civil Rights
 - Healthcare “covered entities” and their business associates are regulated by HIPAA, and OCR is charged with enforcing the privacy and security of health information
 - OCR can levy fines, institute strict compliance protocols, schedule audits and refer matters to the DOJ
 - OCR is divided nationally into 10 regions, with some offices more aggressive than others



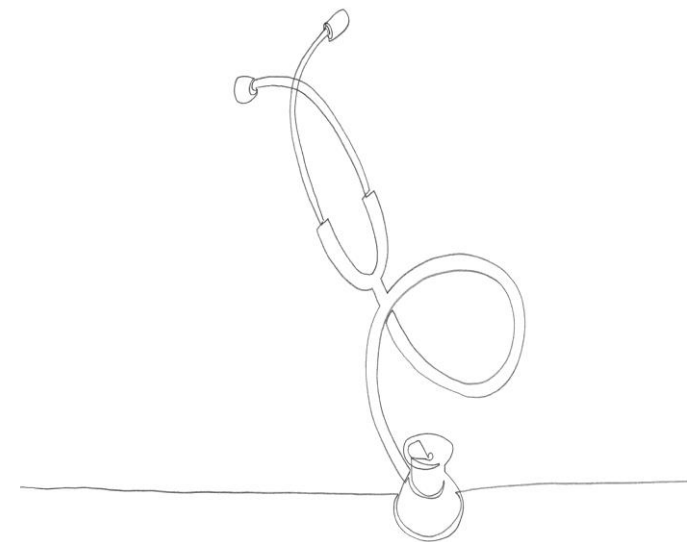
U.S. Department of
Health & Human Services

Regions



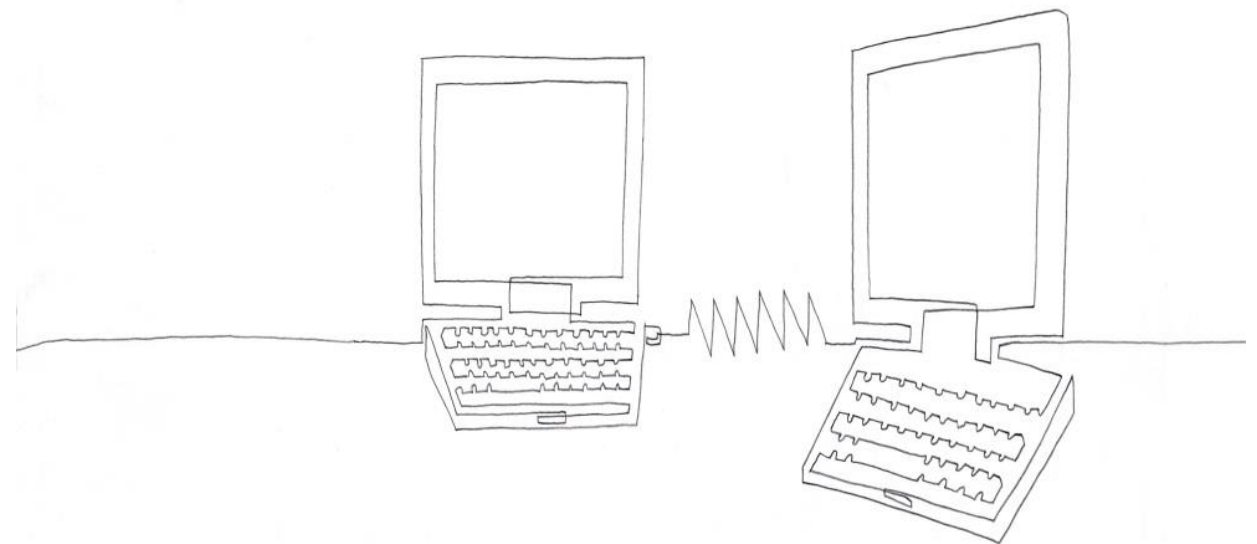
OCR Resolution Agreements: Regions 9 &10

- **Shasta Regional Medical Center (\$275K)**
- **UCLA Health Services (\$865K)**
- **Providence Health & Services (\$100K)**
- **Management Services Organization of Washington (\$35K)**
- **Idaho State University (\$400K)**
- **Skagit County, Washington (\$215K)**
- **QCA Health Plan, Inc. (\$250K)**
- **Alaska Medicaid (\$1.7M)**
- **Phoenix Cardiac Surgery, P.C. (\$100K)**
- **Hospice of North Idaho (\$50K)**
- **Anchorage Community Health Services, Inc. (\$150K)**



Regulatory Hot Buttons

- Risk Assessments and Risk Management Plans
- Vendor Management
- Incident Report and Process
- Encryption of Devices
- Third Party Access to PHI
- Inventory of PHI and ePHI
- Staff Education and Sanctions
- Business Associate Agreements
- Accounting of Disclosures
- Old Data
- Security Rule Compliance



Other Regulators to Watch

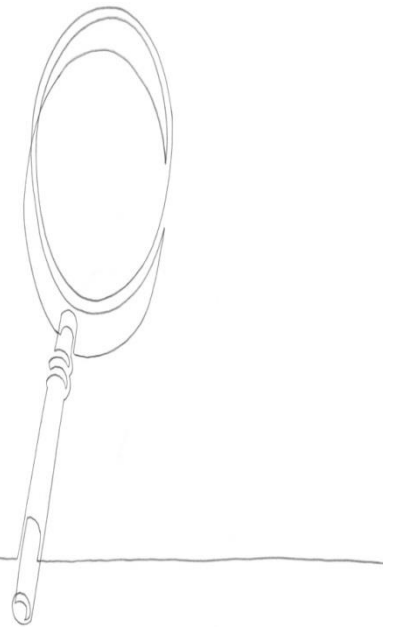
FTC

- Authority derived from Section 5 of the Federal Trade Commission Act (15 U.S.C. § 45)
 - Prohibits “unfair or deceptive acts or practices in or affecting commerce”
 - Similar to state AGs, the FTC’s mandate is essentially to police unfairness and deception aimed at consumers
- Misleading privacy policies are the most common pitfall
 - Representations about the level of security and protective measures employed to protect data
- Informal vs. formal inquiries
 - Inquiries typically being with informal requests for information; can lead to a formal Civil Investigative Demand
- Consent orders
 - Monetary fines, injunctive relief, compliance audits
- To date, FTC not involved in healthcare-related breaches (OCR has jurisdiction)

Other Regulators to Watch (cont.)

SEC

- The SEC's mandate is to ensure that publicly traded companies are properly disclosing cyber risks and incidents to potential investors
 - What aspects of the business give rise to material cyber risks?
 - What controls and procedures are in place?
 - What are the potential costs and consequences?
- Cybersecurity plans and practices are also a focus
 - Is management protecting the company and its value?
- Increased frequency of SEC inquiries in the wake of data breach
- Informal vs. formal inquiries
 - More recently, we are seeing a more aggressive approach, with the SEC utilizing its subpoena power in connection with formal demands



Q & A Session



The True Claims Trends



@Advisen #CyberRisk

The True Claims Trends



Garrett Koehn

President Northwestern US, Regional Director
CRC Insurance Group [2015 Conference Chair]
Moderator

The True Claims Trends

- **Garrett Koehn**, President Northwestern US, Regional Director, CRC Insurance Group (Moderator)
- **Matt Donovan**, National Underwriting Leader – Technology and Privacy, Hiscox
- **Tim Francis**, Enterprise Lead for Cyber Insurance, Travelers
- **Thomas Kang**, Cyber Product Manager, Hartford Financial Products
- **Jim McQuaid**, U.S. Head of Cyber Media and Technology, Financial Lines Claims, AIG

The True Claims Trends



Missing photo: Thomas Kang

Operational Risk and the Cyber Threat



@Advisen #CyberRisk

Operational Risk and the Cyber Threat



David Bradford

President, Research & Editorial division, Advisen
Moderator

Operational Risk and the Cyber Threat

- **David Bradford**, President, Research & Editorial division, Advisen (Moderator)
- **John Bruce**, CEO, CO3 Systems
- **David Cass**, SVP & Chief Information Security Officer, Elsevier
- **Ben Walther**, Senior Security Engineer, Warner Brothers
- **Joe Weiss**, Senior Member, Applied Control Solutions

Operational Risk and the Cyber Threat



Live Cyber Incident Simulation Exercise

March 2, 2015 – San Francisco



@Advisen #CyberRisk



What was the exercise?

Yesterday, Advisen hosted a cyber incident simulation exercise that saw a selected teams of experts – representing the various stakeholders in a real event – work through a mock cyber incident in real time.

An observation team critiqued the handling of the incident and now report back some best practices and key takeaways from the exercise.



@Advisen #CyberRisk

Who took part?

Red Team: A group of cyber security experts who devised the mock incident to be as realistic as possible and to test the 'corporation' to its limits. Also acted as external resources to the Blue Team in crisis response

Blue Team: A select group representing the key cyber stakeholders within the corporation under attack. This team – made of board members and operations executives played roles on the day

The Scenario

- Aston Maureen global car manufacturing company
- SF headquartered – dozens of worldwide locations
- 30,000 employees – \$25 billion revenue
- Produces very high-end to commuter vehicles
- Extreme luxury KITT car is custom-ordered and personalized to buyer. Bought by wealthiest people in the world
- Monday, 9am: FBI find intellectual property (relating to engineering/manufacturing process) on a remote computer...

What do you do next?

Who do you call?

Head of IT

GC/outside counsel

Incident response team

PR

Insurance broker

Monday, 4pm

Brian Krebs calls, enquiring about an anonymous report of a vulnerability being exploited in Aston Maureen's manufacturing facilities.
Krebs requests that you reply within 2 hours

What's your response?

- a) Tell Mr Krebs everything you know, but caveat that you are still investigating
- b) Respond with "no comment"
- c) Call your attorney and follow his/her advice
- d) Don't respond at all
- e) Get forensic, legal, crisis management help ASAP

Krebs – Blue Team response

Selected option e)

Who do they contact first?
When should they notify carrier?



Escalation of the crisis: 48 hours

- An employee has posted customer data and payroll data for the Board of Directors on social media
- The California attorney general, SEC and FTC all called – seeking notification commitment
- Receive word from Chinese manufacturing plants that computer glitches have slowed production to 60% of normal capacity
- 200 Aston Maureen vehicles have been stolen in the past 48 hours, affecting the high-end KITT model

What do you do?

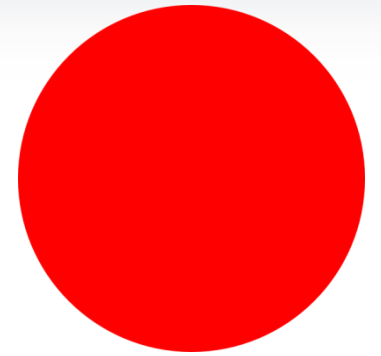
What are you thinking about?
Ask these questions after each inject description,
build tension...



What's driving the company's response?

Notification laws
Life-and-death of business
IP
Safety of vehicles/customers

Live Cyber Incident Simulation Exercise

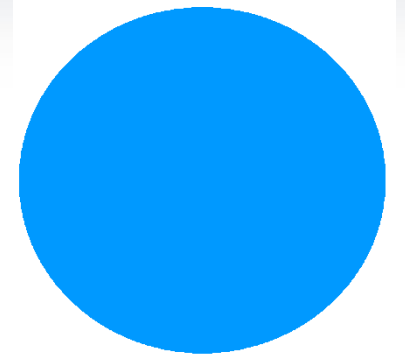


Red Team Participants

- Fausto Molinet, Delta Risk
- Ian Stewart, Wilson Elser
- Liz Wittenberg, AIG



Live Cyber Incident Simulation Exercise



Blue Team Participants

- Joseph Abrenio, Delta Risk
- Brian DaCosta, Kivu Consulting
- David Dahlquist, Advisen
- Lara Forde, ePlace Solutions
- Bo Holland, AllClear ID
- Stephanie Sparks, Hoge Fenton



@Advisen #CyberRisk

Observation Team

- **Jim Giszczak**, Member, McDonald Hopkins
- **Garrett Koehn**, President Northwestern US, Regional Director, CRC Insurance Group
- **Randy Krause**, President & CEO, ePlace Solutions
- **Winston Krone**, Managing Director, Kivu Consulting



Observation Team



Closing Remarks



Garrett Koehn

President Northwestern US, Regional Director
CRC Insurance Group
[2015 Conference Chair]

Thank you to our Sponsors

 **NAS** insurance

 **KIVU**

 **AllClearID**

 **beazley**

 **TRAVELERS**

 **McGladrey**