Welcome to the World’s Largest Cyber Risk Insights Conference!
Opening Remarks

Bill Keogh
CEO
Advisen
Thank you to our 36 sponsors
Thank you to our Advisory Board!

Ben Beeson of Lockton
Alan Brill of Kroll
Anne Corona of Aon
Dan Cosgrove of Swiss Re Corporate Solutions
Erica Davis of Zurich
Brad Gow of Endurance
Tracie Grella of AIG
Chris Keegan of Beecher Carlson
John Mullen of Lewis Brisbois
Bob Parisi of Marsh
Bob Wice of Beazley
Opening Remarks

Chris Keegan
Senior Managing Director
Cyber Technology National Practice Leader
Beecher Carlson
2014 Conference Chair
Keynote Address

Tom Ridge
First US Secretary of Homeland Security
Chairman of Ridge Insurance Solutions
Advisen Cyber Market Overview

David Bradford
President, Research & Editorial division
Advisen

Slides are available to Cyber Risk Network Members Only
Thank you to our 36 sponsors
One of the benefits of joining the Cyber Risk Network…

Our Conference Slide Decks are only available to Cyber Risk Network Members

Slides are available to Cyber Risk Network Members Only
Agenda

• Loss trends
• Cyber insurance
Agenda

• Loss trends
• Cyber insurance
Cyber Event Counts over Time

Source: Advisen

Slides are available to Cyber Risk Network Members Only
Cyber Event Type Composition over Time

Digital Data Breach, Loss, or Theft
Improper Disposal/Distribution, Loss or Theft (Printed Records)
Identity Theft/Fraudulent Use or Access
Improper Collection of Digital Data
Cyber Extortion
System/Network Security Violation or Disruption
Privacy Violations
Phishing, Skimming
Digital Asset Loss or Theft

Source: Advisen
Types of Data Lost

- Personal Financial Identity: 50.32%
- Personal Privacy: 37.52%
- Corporate Loss of Business Income: 6.49%
- Corporate Loss of Digital Assets: 5.68%

Source: Advisen
Types of Data Lost over Time

Personal Financial Identity

Personal Privacy

Corporate Loss of Business Income

Corporate Loss of Digital Assets

Source: Advisen
Sources of Data Loss

- Server: 31.48%
- Printed Records: 15.47%
- Website: 15.13%
- Laptop: 11.70%
- Other*: 26.21%

Source: Advisen
Source: Advisen
Agenda

• Loss trends
• Cyber insurance
<table>
<thead>
<tr>
<th>Revenue Range</th>
<th>Penetration Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>0&lt;500K</td>
<td>2.32%</td>
</tr>
<tr>
<td>500K&lt;1M</td>
<td>2.78%</td>
</tr>
<tr>
<td>1M&lt;2.5M</td>
<td>3.53%</td>
</tr>
<tr>
<td>2.5M&lt;5M</td>
<td>4.93%</td>
</tr>
<tr>
<td>5M&lt;10M</td>
<td>5.38%</td>
</tr>
<tr>
<td>10M&lt;25M</td>
<td>7.35%</td>
</tr>
<tr>
<td>25M&lt;100M</td>
<td>10.76%</td>
</tr>
<tr>
<td>100M&lt;300M</td>
<td>19.80%</td>
</tr>
<tr>
<td>300M&lt;1B</td>
<td>22.13%</td>
</tr>
<tr>
<td>1B&lt;5B</td>
<td>24.35%</td>
</tr>
<tr>
<td>5B+</td>
<td>26.63%</td>
</tr>
</tbody>
</table>

Source: Advisen
Penetration Rate by Insured Size over Time

Source: Advisen
Average Cyber Limits and Premiums by Revenue Range

- Source: Advisen

Slides are available to Cyber Risk Network Members Only
Premiums at Renewal over Time: Index

Source: Advisen

Slides are available to Cyber Risk Network Members Only
“...and the Survey says” sponsored by Zurich

Erica Davis
Vice President & Assistant National Manager for Specialty E&O
Zurich North America
Survey says...!

Results of the 2014 survey
Presented by
Erica Davis, Zurich
“Jennifer Lawrence and Other Celebs Hacked as Nude Photos Circulate on the Web…”

“Celeb lawyer takes on Google over hacked, nude photos…”
About The Survey & The Respondents
In your experience, are cyber risks viewed as a significant threat to your organization by:

- Board of Directors
- C-Suite Executives
- Suppliers/Customers
In the event of a data breach, which department in your organization is PRIMARILY responsible for assuring compliance with all applicable federal, state, or local privacy laws including state breach notification laws?

- Sales: 6%
- Customer Service: 9%
- Information Technology (IT): 21%
- General Counsel: 11%
- Risk Management/Insurance: 6%
- Compliance: 9%
- Chief Privacy Officer: 38%
- Don’t Know: 0%
- None: 0%
Which department is PRIMARILY responsible for spearheading the information security risk management effort?

- Information Technology (IT): 69%
- Risk Management/Insurance: 3%
- Other (please specify): 11%
- Chief Privacy Officer: 2%
- General Counsel’s Office: 5%
- Don't Know: 11%
- Treasury or CFO’s Office: 2%
- Internal Audit: 2%
- Human Resources (HR): 2%

OCTOBER 28, 2014 | NEW YORK
Emerging Risks

Social media
Mobile devices
Cloud Computing
Does your organization purchase cyber liability insurance?

<table>
<thead>
<tr>
<th></th>
<th>2011</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>35%</td>
<td>44%</td>
<td>52%</td>
<td>52%</td>
</tr>
<tr>
<td>No</td>
<td>60%</td>
<td>50%</td>
<td>38%</td>
<td>35%</td>
</tr>
</tbody>
</table>
Morning Break

It’s time to choose your track!

TRACK 1
Cyber Risk Management & Insurance
SLIDES 36-59

TRACK 2
Emerging Risks & the Future of Cyber Insurance
SLIDES 60-114

TRACK 3
Industry Spotlight: Healthcare
SLIDES 115-182
TRACK 1
Cyber Risk Management & Insurance
Thank you to our 36 sponsors
Track Chair

David Bradford
President, Research & Editorial Advisen
The Buyer’s Perspective
The Buyer’s Perspective

Joe DePaul
Senior Vice President, FINEX
North America Cyber and E&O Team
Willis
Moderator
The Buyer’s Perspective

- **Joe DePaul**, Senior Vice President, FINEX North America Cyber and E&O Team, Willis (Moderator)
- **David Conca**, Director, Risk Management, Univision Communications Inc.
- **Roc Starks**, SVP, Director, Corporate Insurance, Citizens Bank
- **Eric Vorenkamp**, Owner, Vorenkamp LLC
The Buyer’s Perspective

Joe DePaul
Willis

David Conca
Univision

Roc Starks
Citizens Bank

Eric Vorenkamp
Vorenkamp
Managing Cyber Exposures in a Global Economy
Managing Cyber Exposures in a Global Economy

Tracie Grella
Global Head of Professional Liability
AIG Financial Lines
Moderator
Managing Cyber Exposures in a Global Economy

- **Tracie Grella**, Global Head of Professional Liability, AIG Financial Lines (Moderator)
- **Hans Allnutt**, Partner, DAC Beachcroft
- **Stacey Regan**, Deputy Treasurer, GE
- **Willy Stoessel**, Head of Cyber, Technology & Construction, Swiss Re Corporate Solutions
Managing Cyber Exposures in a Global Economy

Tracie Grella
AIG

Hans Allnutt
DAC Beachcroft

Stacey Regan
GE

Willy Stoessel
Swiss Re Corporate Solutions
The Future of Cyber Insurance Underwriting
The Future of Cyber Insurance Underwriting

Mike Brown
Cyber Liability Managing Director
Guy Carpenter
Moderator
The Future of Cyber Insurance Underwriting

- **Mike Brown**, Cyber Liability Managing Director, Guy Carpenter (Moderator)
- **Steve Boughal**, Chief Underwriting Officer, Hartford Financial Products, The Hartford
- **Brad Gow**, Senior Vice President, Professional Liability, Endurance
- **Paul Miskovich**, Senior Vice President, Global Head of Cyber, AXIS Insurance
- **Matt Prevost**, Vice President, Professional Risk, ACE
The Future of Cyber Insurance Underwriting

Michael Brown
Guy Carpenter

Steve Boughal
The Hartford

Brad Gow
Endurance

Paul Miskovich
AXIS

Matt Prevost
ACE
Coverage Considerations
Coverage Considerations

Roberta Anderson
Partner
K&L Gates
Moderator

Twitter: @RobertaEsq
Coverage Considerations

- Roberta Anderson, Partner, K&L Gates (Moderator)
- Evan Fenaroli, Underwriting Supervisor, Management & Professional Liability, Philadelphia Insurance
- Tim Francis, Second Vice President, Bond & Financial Products, Travelers
- Catherine Rudow, Vice President, Specialty Casualty, PartnerRe US
• Which first and third party coverages do buyers generally value most?
• Are some coverages misunderstood or undervalued?
• How have policies changed in the past several years and what are the emerging trends?
• Are brokers generally able to advise their clients well on cyber insurance protection?
• How do cyber policies interact with general liability, crime, D&O, E&O, and other policies?
• How does cyber coverage vary by industry? Do insurers generally do a good job of responding to differences in exposures posed by different industries?
• What coverage issues can arise for a company that outsources some or all of its IT?
• Are there common coverage pitfalls? Where do coverage disputes tend to arise?
• How do cyber endorsements to other types of policies compare with stand-alone cyber policies?
• What are the three things insurance buyers should most focus on when buying cyber insurance?
Coverage Considerations

Roberta Anderson
K&L Gates
Philadelphia

Evan Fenaroli
Travelers

Tim Francis
PartnerRe

Catherine Rudow
Philadelphia
TRACK 2

Emerging Risks & the Future of Cyber Insurance
Thank you to our 36 sponsors
Track Chair

Graeme Newman
Director
CFC Underwriting
2015 Cyber Risk Conference London Chair
Standards and Guidelines: What they mean for Risk Managers and Underwriters
Standards and Guidelines: What they mean for Risk Managers and Underwriters

Ben Beeson
Vice President, Cyber Security and Privacy
Lockton
Moderator
Standards and Guidelines: What they mean for Risk Managers and Underwriters

- Ben Beeson, Vice President, Cyber Security and Privacy, Lockton (Moderator)
- John Coletti, Chief Underwriting Officer, Cyber & Technology, XL
- Ira (Gus) Hunt, President & CEO, Hunt Technology, LLC
- Shane McGee, Chief Privacy Officer, FireEye, Inc.
- Lisa Sotto, Chair, Privacy and Cybersecurity Practice, Hunton & Williams LLP
Standards and Guidelines: What they mean for Risk Managers and Underwriters

Ben Beeson
Lockton

John Coletti
XL

Ira (Gus) Hunt
Hunt Technology

Shane McGee
FireEye

Lisa Sotto
ACE
The Internet of Things: Liability at the Intersection of Digital and Physical
The Internet of Things: Liability at the Intersection of Digital and Physical

Alan Brill
Senior Managing Director
Kroll
Moderator
According to IDC...

- The IoT market will reach $7.1 trillion by 2020.
- It will connect cars, medical devices, refrigerators, thermostats and countless other things to the Internet, where cloud services can provide enhanced analytics and operational controls.
- What are the issues relating to security, privacy, compliance and risk management/transfer?
The Internet of Things:
Liability at the Intersection of Digital and Physical

- Alan Brill, Senior Managing Director, Kroll (Moderator)
- Dr. Rey Leclerc Sveinsson, Vice President – Senior Cyber Risk Engineering, Swiss Re Corporate Solutions
- Graeme Newman, Director, CFC Underwriting
- Rick Welsh, Head of Cyber Insurance, AEGIS
The Internet of Things: Liability at the Intersection of Digital and Physical
Cyber Operational Risks
Cyber Operational Risks

Rebecca Bole
Director of Editorial Strategy & Products
Advisen
Moderator
Cyber Operational Risks

- **Rebecca Bole**, Director of Editorial Strategy & Products, Advisen (Moderator)
- **Sandor Boyson**, Director, Supply Chain Management Center & Research Professor at the Robert H. Smith School of Business at University of Maryland
- **John Howie**, Principal, Howie Consulting LLC
- **Michael Palotay**, Senior Vice President of Underwriting, NAS Insurance
- **Andy Roth**, Partner & Chair, Global Privacy and Cybersecurity Group, Dentons
Cyber Operational Risks

Rebecca Bole
Advisen

Sandor Boyson
University of Maryland

John Howie
Howie Consulting

Michael Palotay
NAS

Andy Roth
Dentons
Malicious Disruption Of IT Supply Chains

- Symantec’s 2013 Internet Security Threat report, based on its network monitoring across 157 countries, found supply chain as the latest threat vector:

- It noted an increase in attacks targeting the supply chain – “cybercriminals find these contractors and subcontractors susceptible to attacks and they are often in possession of valuable intellectual property. By going after manufacturing companies in the supply chain, attackers gain access to sensitive information of a larger company”

Targeting Production: Seagate

- Seagate’s hard drive assembly line in Thailand was taken over by a foreign intelligence service who embedded “report back mechanisms” in the hard drives.
- These hard drives were sent to Seagate Taiwan and then onto DOD, where they copied all the classified files stored on them, and transmitted the files via the internet back home to the foreign intelligence service.
- The brand risks to Seagate stemming from this kind of attack is obviously enormous, including revenue loss from being put on DOD vendor watch lists.
- **Risk Mitigation:** Double down on background checks of key executives with broad hiring authority

Source: sandor boyson, supply chain management center, r.h. smith school of business, university of maryland, 2014
Amazon

- Amazon have suffered numerous failures at their Northern Virginia Data Center cluster
  - Many popular sites and services rely on Amazon:
    - AirBnB
    - Flipboard
    - Instagram
    - Netflix
    - Vine
- To its credit, Amazon have long provided guidance about how to architect applications to avoid single points of failure
  - Most companies simply chose to ignore them
Targeting Distribution: Dell

• In 2010, Dell Power Edge 410 servers were shipped with malware pre-installed on the motherboards and required sixteen changes in supply chain procedures to block the attack pathways.

• Quality deficiency costs & warranty liability risks were substantial.

• Risk Mitigation:
  – Audit whether the CIO and V.P. Of Supply Chain regularly communicate, coordinate and take cooperative action to track down and close off vulnerabilities in the IT supply base.
  – Maintain a real time view on process integrity across a distributed IT supply chain e.g. deploy a CTV surveillance network monitored by a central operations center for critical work areas in the trans-national supply chain.

Source: Sandor Boyson, Supply Chain Management Center, R.H. Smith School of Business, University of Maryland, 2014
Microsoft Azure

• Microsoft Azure suffered significant outages in 2012 and 2013
  – Essentially shut down service world-wide for ALL customers
    • No way to architect around failures
Dentsply

- Dentsply- a medical device manufacturer- took a $200 million revenue hit from the March 11, 2011 Fukushima nuclear reactor accident and Tsunami.

- Dentsply’s sole source supplier for critical, high end dental components was 2 miles from the reactor and was wiped out.

- The supplier’s onsite electronic repository of component designs was destroyed and had not been backed up either by the supplier or Dentsply.

- Dentsply’s affected product could not simply be moved to an alternate supplier- the product had to be designed and manufactured again from scratch.

- **Risk Mitigation**: Map and identify single points of failure, including unique IT databases supporting the design, manufacture and distribution of high revenue products; seek redundancy of supply or better protection/mirroring of unique online assets.

Source: sandor boyson, supply chain management center, r.h. smith school of business, university of maryland, 2014
Disruption of Service

• IT supply chains extend to the Cloud
  – Many companies are in the Cloud, and most have at least examined moving to it

• Core business processes and systems now run outside of your control (ERP, CRM, Email, custom LOB applications)
  – What happens when service goes down?
    • Either due to failure of cloud provider or of network connection between you
Planning for Failure

• Technical failure of cloud services is inevitable
  – Technology is very complex and not all of it is automated

• What about business failure?
  – Have you looked at the ‘health’ of your cloud provider?
    • Many are not growing the bottom line (or constantly report losses)
    • Is cloud service even their focus?
Modeling Cyber Risks
Modeling Cyber Risks

Bob Parisi
Managing Director and National Cyber Practice Leader
Marsh
Modeling Cyber Risks

Advisen Cyber Risks Insights Conference

October 28th 2014

“There are three types of lies -- lies, damn lies, and statistics.”
— Benjamin Disraeli
Other key findings:

- **78%** were not highly difficult involving little to no resources or customization of software.
- **75%** were not targeted at a specific individual or company.
- **29%** of attacks utilized social tactics (email, phone calls, or social network information).
- **14%** of attacks involved insiders; **50%** of those were former employees using old credentials.
- **66%** of breaches took months (62%) or years (4%) to discover.
- **69%** of breaches were discovered by an external party (9% by customers).
Nearly 85% of Board members acknowledged familiarity with basic Information Security standards such as ISO 27001/2; however only 35% knew where their organization stood as regards complying with basic information security standards.

In the first six months of 2013, there were over 800 regulatory filings that mentioned cyber related risks. This represents a 106% increase from the same time in 2012.

Three industries accounted for nearly two-thirds of all client events: healthcare (38%), educational institutions (13%) and financial institutions (9%). A closer review of the data shows that healthcare and higher education suffer dramatically in the cyber risks confronting them.

Our 2013 cases show that approximately 78% of healthcare cyber crises were tied to human error and 22% involved an act of malicious intent. By contrast, over 75% of cyber events in the higher education market were traced back to a malicious act.

Are criminals more drawn to stealing data from educational institutions?

Educational institutions pose unique challenges from a security perspective. Educational institutions are populated with innovative, technically adept users within cultures that promote adaptation and change. The collaborative, open nature of most institutions makes the implementation of security protocols a challenge. In addition, while both sectors are regulated by federal privacy laws, the Health Insurance Portability

Source: Supply Chain Resilience 2013, The Business Continuity Institute

2013 KROLL CLIENT DATA BREACHES BY INDUSTRY

<table>
<thead>
<tr>
<th>Sector</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Healthcare</td>
<td>36%</td>
</tr>
<tr>
<td>Retail</td>
<td>6%</td>
</tr>
<tr>
<td>Technology</td>
<td>3%</td>
</tr>
<tr>
<td>Food &amp; Beverage</td>
<td>1%</td>
</tr>
<tr>
<td>Chemicals</td>
<td>1%</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>1%</td>
</tr>
<tr>
<td>Energy</td>
<td>1%</td>
</tr>
<tr>
<td>Nonprofit</td>
<td>1%</td>
</tr>
<tr>
<td>Transportation</td>
<td>1%</td>
</tr>
<tr>
<td>Entertainment</td>
<td>1%</td>
</tr>
</tbody>
</table>

* Source: Kroll 2013 case study analysis from U.S.-based clients.
Cyber Attacks and Main Street

• Cybercriminals unleash 3.5 new threats targeting small and medium businesses every second.*

• The number of online attacks specifically targeting small businesses surged 600 percent in 2010.*

• Small businesses are now the target of 31 percent of all attacks, a threefold increase from 2011.**

• 29 percent of the small businesses experienced a computer-based attack.*** The consequences of those attacks included:
  - managing potential damage to their reputations (59 percent);
  - theft of business information (49 percent);
  - the loss of angry or worried customers (48 percent) and
  - network and data center downtime (48 percent).

Source:
*TrendMicro, **Symantec, ***Ponemon
So what do we use as our yardstick?
IDEAL Cyber – Privacy Event Model:

Approaching Cyber Risk...

Quantifying the data breach epidemic.

Data breaches are an increasingly prominent and costly security challenge across the spectrum of U.S. companies, and they are growing in size and frequency. New types of breaches occur millions of cyber attacks each week. A successful breach can put people’s personal records that will be later sold on an illicit market.

With today’s data moving freely among organizations and consumers on mobile devices, the cloud, and new points of vulnerability, data breaches have never been more common.

Prudent risk management requires organizations to quantify the potential for this growing threat. However, determining accurate projections can be challenging. Many projections that are currently available include uninsured costs on limited data.

The IDEAL Privacy model utilizes historical breach information and current inputs in order to allow clients to make data-driven decisions while assessing risks.

Privacy IDEAL – Frequency

What is the probability that XX will have an event over the next 12 months?

Factors influencing Probability

- Industry
- Breach Cost
- Data Security

Privacy IDEAL – Range of Potential Outcomes

Factors influencing Security

- Industry
- Breach Cost
- Data Security

Privacy IDEAL – Cost Analysis

Factors influencing Cost

- Industry
- Breach Cost
- Data Security

Note: Costs due not include business interruption due to the high degree of variability.
Stochastic Modeling
Monte Carlo Simulation

I'm afraid he can't come to the phone, he's in the middle of a Monte Carlo simulation.

Deals Department

BRMM BRMM!

Rally!

Goddard Cartoon ©PharmaVentures; all rights reserved.
“The future ain’t what it used to be.”

-- Yogi Berra

Robert A. Parisi, Jr.
Managing Director, FINPRO
Product Leader for Network and Privacy Risk

Marsh
1166 Avenue of the Americas
New York, NY 10036

Office: 212.345.5924
Email: robert.parisi@marsh.com

For More Information: www.marsh.com
This document and any recommendations, analysis, or advice provided by Marsh (collectively, the “Marsh Analysis”) are intended solely for the entity identified as the recipient herein (“you”). This document contains proprietary, confidential information of Marsh and may not be shared with any third party, including other insurance producers, without Marsh’s prior written consent. Any statements concerning actuarial, tax, accounting, or legal matters are based solely on our experience as insurance brokers and risk consultants and are not to be relied upon as actuarial, accounting, tax, or legal advice, for which you should consult your own professional advisors. Any modeling, analytics, or projections are subject to inherent uncertainty, and the Marsh Analysis could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. The information contained herein is based on sources we believe reliable, but we make no representation or warranty as to its accuracy. Except as may be set forth in an agreement between you and Marsh, Marsh shall have no obligation to update the Marsh Analysis and shall have no liability to you or any other party with regard to the Marsh Analysis or to any services provided by a third party to you or Marsh. Marsh makes no representation or warranty concerning the application of policy wordings or the financial condition or solvency of insurers or reinsurers. Marsh makes no assurances regarding the availability, cost, or terms of insurance coverage.
Litigation Trends
Litigation Trends

Laurie Kamaiko
Partner
Edwards Wildman Palmer LLP
LITIGATION TRENDS
Litigation Trends - Agenda

♦ Litigation Arising From Data Breaches
   ♦ Claimants, Defendants, Claims
   ♦ Hurdles
   ♦ How hurdles are (attempted) to be overcome

♦ Other Types of Litigation Now Here and on the Horizon
   ♦ Business Practices in collection, sharing, usage of personal information
   ♦ Disclosure of Practices

♦ What can we do to prepare and minimize exposure
Litigation Arising From Data Breaches
Overview

- Consumer Class Actions
  - Hurdles
  - Overcoming of Hurdles
- Other types of Plaintiffs
  - Shareholders
  - Banks and Credit Unions
  - Business Partners
  - Regulators
- Potential Defendants
  - Breached entities
  - Vendors of breached entity
    - Holders of information
    - Access to information
    - Security/design consultants
  - Professional Advisors
- D & Os
Traditional Theories of Liability Asserted by Consumers in Breach Litigation

Dozens of different causes of action identified

Liability theories generally focus on:
- Response to the Breach
  - Failure to adequately respond
  - Failure to timely notify
  - Misrepresentation of cause or effect
  - Violation of consumers protection statutes and other statutes

- Pre-breach Security
  - Inadequate security: people, processes and policies
  - Misrepresentation of security
  - Failure to warn of inadequate security
Hurdles of Consumer Litigation

Standing: Supreme Court in *Clapper* (February 2013) upheld indispensability of its requirements
Federal jurisdiction requires “case or controversy” →
- Injury in fact:
  - Actual or imminent injury, not conjectural or hypothetical
  - Threatened injury must be certainly impending
  - “Substantial risk” may be sufficient
- Causation: between conduct/breach and injury – “fairly traceable”
- Redressability: injury likely to be redressed by favorable outcome
Allegations must be particularized, plausible and not just conclusory
Cognizable claim required
  - Do the allegations state a cause of action
  - Does that c/a require actual injury beyond substantial risk
Standing Hurdles Sometimes Successfully Overcome

So what if no identity theft or out of pocket loss?

- Many cases don’t survive “standing” challenge
- But plaintiffs have had some success in some courts overcoming hurdles
  - Showing Injury as “substantial risk” even when not actual
  - Facts matter (e.g., evidence of some misuse of some PI)
  - Jurisdiction matters (e.g. 9th or 11th Circuits better for consumers)
Plaintiffs’ attempts to avoid dismissal for lack of actual injury include developing new theories and asserting claims for:

- Consumer protection statute violated
  - statutory damages; multiple damages
  (but some statutes require injury in addition to violation)
- Misrepresentation in Privacy Policy or Terms of Use /Deceptive Advertising or Labeling/Fraud
- Violation of a right to privacy
- Unjust enrichment, e.g., price for service provided to consumer included data security and that not delivered
- Lost value, e.g., does PI have value that is reduced by its theft

And if plaintiff defeats defendant’s motion to dismiss → Settlement
Its Not Just Consumers Suing Anymore

Litigation arising from Breaches now includes:

♦ Shareholder suits
  ♦ Wasting of corporate assets; breach fiduciary duty
♦ Bank/Credit Union suits for losses from card breaches
  ♦ Negligence; Misrepresentation; Third Party Beneficiary of PCI Agreements and other contracts promising data security; unfair and deceptive practices
♦ Disputes between breached merchants and their payment processors, card brands, acquiring banks
♦ B to B suits
  ♦ Negligence/contribution; indemnity; breach of contract
♦ Regulatory Enforcement Actions – state and federal
  ♦ Once a breach, also scrutinize pre-breach compliance
And it’s Not Just Breaches that Give Rise to Litigation

Non-Breach Claims Arising from Business Practices in Collection and Usage of Personal Information – And Adequacy of Disclosure of Those Practices

♦ Statutory violations that are not data breaches per se
♦ Online behavioral advertising/consumer tracking
♦ Wrongful collection/sale of PI
♦ Zipcodes as PI when recorded by retailers without need for card transaction (California, Massachusetts - other states on horizon?)
♦ Adequacy of Privacy Policies and company compliance with representations in Privacy Policies and Terms of Use
♦ Privacy violations, e.g., Call Recording, TCPA
♦ Increased regulatory scrutiny: HHS, SEC, FTC, FDA, etc.
  ♦ Including whether data assessments and security in compliance with standards of the industry, NIST, PCI-DSS, etc.
Filings by Types of Claim - from Advisen

Cyber Litigation Frequency Index

- Digital Data Breach, Loss, or Theft
- Improper Disposal/Distribution, Loss or Theft (Printed Records)
- Improper Collection of Digital Data
- Identity Theft/Fraudulent Use or Access
- System/Network Security Violation or Disruption
- Privacy Violations

Graph showing trends from 2005 to 2013.
Litigations Compared to Events 2005-2013

Case Count over Time

<table>
<thead>
<tr>
<th>Year</th>
<th>Count of Litigated Cases</th>
<th>Count of Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>2005</td>
<td>73</td>
<td>292</td>
</tr>
<tr>
<td>2006</td>
<td>139</td>
<td>674</td>
</tr>
<tr>
<td>2007</td>
<td>133</td>
<td>791</td>
</tr>
<tr>
<td>2008</td>
<td>179</td>
<td>1031</td>
</tr>
<tr>
<td>2009</td>
<td>185</td>
<td>1325</td>
</tr>
<tr>
<td>2010</td>
<td>209</td>
<td>1250</td>
</tr>
<tr>
<td>2011</td>
<td>276</td>
<td>1415</td>
</tr>
<tr>
<td>2012</td>
<td>224</td>
<td>1565</td>
</tr>
<tr>
<td>2013</td>
<td>216</td>
<td>1998</td>
</tr>
</tbody>
</table>
Litigation Frequency by Industry

Relative Litigation Frequency by Industry (once there is a breach)

<table>
<thead>
<tr>
<th>Industry</th>
<th>Event Count</th>
<th>Litigation Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transportation, Communications, Electric, Gas</td>
<td>649</td>
<td>199</td>
</tr>
<tr>
<td>Wholesale and Retail Trade</td>
<td>1244</td>
<td>364</td>
</tr>
<tr>
<td>Mining And Construction</td>
<td>86</td>
<td>22</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>700</td>
<td>139</td>
</tr>
<tr>
<td>Services</td>
<td>5772</td>
<td>990</td>
</tr>
<tr>
<td>Finance, Insurance, And Real Estate</td>
<td>1948</td>
<td>326</td>
</tr>
<tr>
<td>Agriculture, Forestry, And Fishing</td>
<td>21</td>
<td>1</td>
</tr>
<tr>
<td>Public Administration</td>
<td>2030</td>
<td>177</td>
</tr>
</tbody>
</table>
Defendants Can Prepare and Minimize Exposures

- Class action waivers in arbitration provision consumer accepted
  - Breach associated with service that is subject of waiver?
  - Enforceable?
- Demonstrate reasonable security and procedures in place pre-breach and carried out post breach
- Breach was from systems of unaffiliated vendor/third party
- Not financially beneficial for class action attorney
  - Remediation already offered to prospective plaintiffs
  - Remediation of breached entity’s system already done
- Business practices regarding PI collection, usage, disclosure evaluated for compliance pre-breach, along with Privacy Policies and Terms of Use
- Be Prepared – Assume next time it may be you: Are you prepared?
Questions or Comments?

Laurie A. Kamaiko
Steering Committee, Privacy & Data Protection Group
Edwards Wildman Palmer LLP
750 Lexington Avenue
New York, New York 10022
+1.212.912.2768
lkamaiko@edwardswildman.com
TRACK 3

Industry Spotlights
Thank you to our 36 sponsors
Industry Spotlight: Healthcare
Industry Spotlight: Healthcare

Kimberly Holmes
Vice President, Product Development
OneBeacon Professional
Spotlight Chair
State Privacy Laws & Your Business Associates: Key Considerations to Minimize Liability in the Evolving Class Action Landscape

- Kimberly Holmes, Vice President, Product Development, OneBeacon Professional (Spotlight Chair)
- Sheila Hagg-Rickert, Healthcare Risk Management Consultant
- Winston Krone, Managing Director, Kivu Consulting
- Stuart Panensky, Partner, Traub Lieberman Straus & Shrewsberry LLP
- Jeremy Henley, Director of Breach Services, ID Experts
State Privacy Laws & Your Business Associates: Key Considerations to Minimize Liability in the Evolving Class Action Landscape

Kimberly Holmes
OneBeacon

Sheila Hagg-Rickert
Consultant

Winston Krone
Kivu

Stuart Panensky
Traub Liebermann

Jeremy Henley
ID Experts
A Few States to Consider...
Confidentiality of Medical Information Act
Claimants can recover compensatory damages, punitive damages not to exceed three thousand dollars ($3,000), attorneys' fees not to exceed one thousand dollars ($1,000), and the costs of litigation.

Cal. Civ. Code § 1798.82
Security Breach Notification
- New amendments: September 2014
- Expressly provides for private right of action
- Entities covered:
  - Businesses that “maintain” data;
- Requires BA to maintain minimum standards;
- If offering credit monitoring, must meet minimum standards.
Massachusetts

**Mass. Gen L. 93H § 1**
- Must notify Attorney General and other state regulators, consumer agencies
- A/G “may” seek $50,000 fine
- ** Affirmative duty to redact, burn, pulverize or shred paper and destroy and erase electronic media to protect personal information.

**201 CMR 17.00 et seq.**
- Requires persons and entities inside and outside of MA
  - develop a security policy
  - maintain extensive computer system security requirements
  - encrypt all records containing personal information transmitted over wireless networks or stored on portable devices
  - require third-party service providers (e.g., payroll providers, outsourcers) to maintain compliant security measures
  - train employees on compliance
Texas Medical Privacy Act

- Effective 9/1/2012
- Covers Persons and Entities that Assemble, Transmit, Collect, Use PHI
- Requires Specific Written Consent for Use for Marketing Purposes
- Creates Regulatory Audit Authority to Ensure Compliance
- Purports to Cover Violators from Other States Doing Business in Texas if No Applicable State Statute

- AG’s Office to Set Up Website and Complaint System
- Required Employee Training Tailored to Specific PHI Activities Within 90 Days of Hire
- Penalties of up to $5000 for Negligent Violation, $25000 for Knowing Violation, $250,000 for Violation for Financial Gain, Up to $1.5 Million for Repeat Violations
Florida Information Protection Act

- Effective 7/1/2014
- Includes User IDs, Passwords, Security Questions and Account Numbers in Protected Information
- Generally Have 30 Days to Notify Impacted Individuals of Breach
- Can Avoid Notification Requirement if Can Demonstrate to Department of Legal Affairs that Breach Unlikely to Cause Harm
- Can Notify via Email

- Must Notify Department of Legal Affairs if >500 Florida Residents Affected
- No Specific Private Cause of Action Created, But Statute Indicates that Breach May constitute a Deceptive Trade Practice
- Civil Penalties of $1000 Per Day for Each Day Up to 30 Days and $50,000 for Each 30-Day Period Thereafter to a Maximum of $500,000 for Failure to Notify
Recent class action settlements –

Stanford Hospital (CA)
Avmed (FL)
California case—Stanford Hospital

- Medical provider impacted by BA relationship
- $4 million settlement
- 20,000 affected class
- No “actual” injury
- No HITECH (federal) fines
- Patients received $100 each
California case law - Sutter Health

- Dismissed Class Action
- No cognizable harm found
- “It is the medical information, not the physical record (whether in electronic, paper, or other form), that is the focus of the Confidentiality Act. While there is certainly a connection between the information and its physical form, possession of the physical form without actually viewing the information does not offend the basic public policy advanced by the Confidentiality Act.”
USDC Southern District of FL: Curry v. AvMed 
(Case No. 10-cv-24513), February 21, 2014

- Stemmed from theft of two unencrypted laptops containing information about 1.2 million health plan customers in 2009
- Class action. Only some members of class have suffered identify theft.
- $3 million settlement includes:
  - $250,000 in specific damages for victims of identify theft
  - $750,000 in attorney’s fees
  - $10 per year for every year of premiums paid prior to the theft (up to a maximum of $30) for 460,000 customers representing the portion of premium AvMed should have paid for enhanced data security as the refund of a premium overpayment
  - Required implementation of specific data security initiatives:
    - Staff training
    - Data encryption
    - Better password protocols
    - Enhanced physical security
    - Revised policies and procedures
Aside from Defense Expenses…
What other Costs?
Causation in Healthcare Breaches… Business Associates are often front & center…
Multi-state liability for breaches of PHI
A Forensic Review: What’s the “true” cause and extent of a breach?
Key Steps & Parameters For HC Organizations to Consider: Vetting Rights & Responsibilities with Business Associates
Pre- Breach Steps to Put In Place: A Risk Management perspective
How to Proactively Help Your Defense and Breach Response Teams Help YOU
State Privacy Laws all Differ – Are there any “one size fits all” steps to put in place for pre-breach preparedness?
Multistate Considerations
Pre and Post Breach

Jeremy Henley
Director of Breach Services
ID Experts
Get the right players in the huddle
Most Incidents are Not Breaches

Only 2% of incidents are Breaches!

Significant Incident Volume = Risk and Requires Operational Changes

How many incidents are occurring just in healthcare?

- HHS says they have received reports for over 93,000 breaches in their system
- If we assume only 2% are breaches that is.......  

4,650,000 incidents
Fast Money vs. Big Money
National Impact of Medical ID Theft

- $20,000 average cost of medical ID theft incident
- 1.6 million victims of medical ID theft — and growing
- $70-234 billion lost each year to healthcare fraud

Patient care and health at risk due to altered records
Data Breach Response
Do you want to win?

VS.

PRO BOWL

VS.

SUPER BOWL
Summary

• Get the right players in the huddle
• Incident Management is evolving
• Medical ID Theft is serious
• Superbowl teams beat Pro-Bowl teams

Jeremy Henley
Director of Breach Services

760.304.4761
Jeremy.henley@idexpertscorp.com
Industry Spotlight: Healthcare

Kimberly Holmes
Vice President, Product Development
OneBeacon Professional Spotlight Chair
Industry Spotlight: Financial Institutions
Industry Spotlight: Financial Institutions

George Allport
Vice President & Financial Fidelity
Product Manager
Chubb
Spotlight Chair
Financial Institutions: Developing a Risk-Aware Organization

Mary Beth Borgwing
President, Cyber and Risk Practice
Advisen
Moderator
Ongoing evolution of cyber security threats

- Unsophisticated attackers (script kiddies)
  - Experimentation
  - You are attacked because you are on the internet and have a vulnerability

- Sophisticated attackers (hackers)
  - Monetization
  - You are attacked because you are on the internet and have information of value

- Corporate espionage (insiders)
  - Your current or former employee seeks financial gain from selling your intellectual property

- State-sponsored attacks (advanced persistent threats), hacktivism, identify thefts
  - You are targeted because of who you are, what you do, or the value of your intellectual property
  - Cyber attacks to promote political ends
  - Increased theft of personally identifiable information (PII)

Risk

1980s/1990s  -->  20XX
Cyber Litigation Frequency Index - Global

- Privacy Violations
- System/Network Security Violation or Disruption
- Digital Data Breach, Loss, or Theft
- Improper Disposal/Distribution, Loss or Theft (Printed Records)
- Improper Collection of Digital Data

Graph shows trends from 2005 to 2013.
Cyber Breaches by Banks over Time

- Citigroup Inc.
- JPMorgan Chase & Co.
- TD Bank
- Bank of America
- Wells Fargo & Company
- Barclays PLC
- Westpac Banking Corporation
- HSBC
- Wachovia Bank
## Advisen Loss Insight: Total Records Exposed at Banks

<table>
<thead>
<tr>
<th>Bank</th>
<th>Affected Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>JPMorgan Chase &amp; Co.</td>
<td>80,859,642</td>
</tr>
<tr>
<td>Citigroup Inc.</td>
<td>55,333,748</td>
</tr>
<tr>
<td>Wells Fargo &amp; Company</td>
<td>50,821,390</td>
</tr>
<tr>
<td>TD Bank</td>
<td>366,970</td>
</tr>
<tr>
<td>GMAC LLC</td>
<td>200,802</td>
</tr>
<tr>
<td>Westpac Banking Corporation</td>
<td>103,446</td>
</tr>
<tr>
<td>Regions Financial Corporation</td>
<td>100,000</td>
</tr>
<tr>
<td>Hansabank</td>
<td>50,000</td>
</tr>
<tr>
<td>Barclays PLC</td>
<td>37,003</td>
</tr>
<tr>
<td>Korea Exchange Bank</td>
<td>15,000</td>
</tr>
</tbody>
</table>
Advisen Loss Insight: Top 20 Companies by Cyber Event Count

<table>
<thead>
<tr>
<th>Company Name</th>
<th>Case Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Inc.</td>
<td>52</td>
</tr>
<tr>
<td>Facebook, Inc.</td>
<td>44</td>
</tr>
<tr>
<td>Microsoft Corporation</td>
<td>31</td>
</tr>
<tr>
<td>Bank of America Corporation</td>
<td>31</td>
</tr>
<tr>
<td>JPMorgan Chase &amp; Co.</td>
<td>28</td>
</tr>
<tr>
<td>Apple Inc.</td>
<td>26</td>
</tr>
<tr>
<td>Citigroup Inc.</td>
<td>23</td>
</tr>
<tr>
<td>Td Bankc</td>
<td>20</td>
</tr>
<tr>
<td>Yahoo! Inc.</td>
<td>19</td>
</tr>
<tr>
<td>AT&amp;T Inc.</td>
<td>18</td>
</tr>
<tr>
<td>Wal-Mart Stores, Inc.</td>
<td>14</td>
</tr>
<tr>
<td>United States Postal Service</td>
<td>14</td>
</tr>
<tr>
<td>American Express Company</td>
<td>13</td>
</tr>
<tr>
<td>Twitter, Inc.</td>
<td>12</td>
</tr>
<tr>
<td>Wells Fargo &amp; Company</td>
<td>12</td>
</tr>
<tr>
<td>Best Buy Co., Inc.</td>
<td>12</td>
</tr>
<tr>
<td>Purdue University</td>
<td>11</td>
</tr>
<tr>
<td>McDonald's Corporation</td>
<td>11</td>
</tr>
<tr>
<td>eBay Inc.</td>
<td>10</td>
</tr>
<tr>
<td>Pfizer Inc.</td>
<td>10</td>
</tr>
</tbody>
</table>
Financial Institutions: Developing a Risk-Aware Organization

- Mary Beth Borgwing, President, Cyber and Risk Practice, Advisen (Moderator)
- Michael Livni, Chief Information Security Officer, Valley National Bank
- David Notch, Director, Information Protection & Business Resilience, KPMG
- Yonesy Nunez, Information Security Leader – Int’l, Wells Fargo
- John Bird, Consulting Portfolio Partner, Verizon
- Dr. Aleksandr Yampolskiy, CEO and Founder, Security Scorecard
The 80 / 20 Dilemma

Traditional Toolset
- Legacy
- Point-in-time, fragmented analysis
- Detect < 5% of threats

Budget

80

Results

Security 2.0 Toolset
- Information sharing
- Federated Knowledgebase
- Real-time threat intelligence
- Hackers-view
- Security 2.0 Toolset

80

find out which of your partners have risk!

www.securityscorecard.com
Action Must be Taken While Data is Most Valuable

1. Security Event
2. Data Ready for Analysis
3. Analysis Completed
4. Decision Made
5. Action Taken

Event Analytics Speeds Action and Increases Business Value

find out which of your partners have risk!

www.securityscorecard.com
Peer into real-time worldwide threat activity

find out which of your partners have risk!

www.securityscorecard.com
The map below shows the countries that were most severely impacted by the Poodle SSL vulnerability. The data set comes from an analysis of all IPv4 devices connected to the public facing internet. Search by IP address to see if your servers were affected in the early hours of the disclosure. For more information on this data set and OSINT surrounding other vulnerabilities, visit http://blog.securityscorecard.com

find out which of your partners have risk!
www.securityscorecard.com
Financial Industry Performance

[Graph showing financial industry performance over time with dates from 4/28/14 to 10/27/14, with the y-axis ranging from 10 to 100 and the x-axis showing dates in a reverse chronological order.]
Produce Detailed and Executive Reports

Scorecard Overview

chase.com ScoreCard

67th Percentile
Financial Services industry chase.com
http://www.chase.com

<table>
<thead>
<tr>
<th></th>
<th>Quantity of IPs discovered</th>
<th>E-mail addresses detected</th>
<th>Malware Events Detected</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2415</td>
<td>1502</td>
<td>61</td>
</tr>
</tbody>
</table>

Executive Overview

Insecure Ports

- You: 3
- Industry: 3

Malware Discovered (30-Day)

- You: 0
- Industry: 0

Application Security Vulnerabilities

- You: 0
- Industry: 0

Leaked Passwords

- You: 1292
- Industry: 0

Malware Discovered (Year)

- You: 61
- Industry: 0

find out which of your partners have risk!
www.securityscorecard.com
## Financial Institutions: Developing a Risk-Aware Organization

<table>
<thead>
<tr>
<th>Name</th>
<th>Institution/Company</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mary Beth Borgwing</td>
<td>Advisen</td>
</tr>
<tr>
<td>Michael Livni</td>
<td>Valley National Bank</td>
</tr>
<tr>
<td>David Notch</td>
<td>KPMG</td>
</tr>
<tr>
<td>Yonesy Nunez</td>
<td>Wells Fargo</td>
</tr>
<tr>
<td>John Bird</td>
<td>Verizon</td>
</tr>
<tr>
<td>Dr. Aleksandr Yampolskiy</td>
<td>SecurityScorecard</td>
</tr>
</tbody>
</table>
Risk Mitigation and Response
Risk Mitigation and Response

Robert Dowling
Product Manager
Cyber Risk Management Solutions
Dynetics
An ounce of prevention is worth ... a pound of cure.
You can pay me now or ...

pay me later.
The best time to tell your spouse you love them is ...

before someone else does!
The best time to respond to a breach is ...

BEFORE it happens!
Factors that Reduce Costs of Breach

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CISO appointed</td>
<td>$(10)</td>
</tr>
<tr>
<td>BCM involvement</td>
<td>$(13)</td>
</tr>
<tr>
<td>Incident response plan</td>
<td>$(17)</td>
</tr>
</tbody>
</table>
Ponemon 2014 Cost of Cyber Crime

- “Findings suggest companies using security intelligence technologies were more efficient in detecting and containing cyber attacks. As a result, these companies enjoyed an average cost savings of $5.3 million when compared to companies not deploying security intelligence technologies.”

- “Deployment of enterprise security governance practices moderates the cost of cyber crime. ...This so-called “cost savings” for companies deploying good security governance practices is estimated at $1.7 million, on average.”
Cyber Insurance Application

- Have you had any prior breaches?
- Do you have a firewall?
  - How often do you review the rules?
  - When was the last time a rule was changed?
- Do you perform virus scans of emails, downloads, and portable devices?
- Do you have restrictions regarding access to sensitive information of a 3rd party?
- Do you have a process for managing computer accounts, including the removal of outdated access accounts?
- Do you have physical security controls in place to control access to computer systems?
- Do you have access control procedures that address access to critical and sensitive computer systems?
- Do you have a written business continuity plan with procedures?
- Do you perform annual test of back-up and recovery procedures for mission critical systems?
- Do you encrypt sensitive data at rest?
- Do you encrypt sensitive data in transit?
Typical Findings

Can’t identify all devices on the network
Limited visibility to activity on the network
Lack of network segmentation
Activity logs not maintained
Employees susceptible to social engineering attacks
3 Key Risk Indicators (KRI\textsubscript{s})

**Business Impact**
- Analyzes importance of information & systems
- Evaluates loss of confidentiality, integrity or availability
- Considers a variety of direct and indirect costs
  - Recovery, Response & Remediation
  - Business Interruption
  - Legal Fees & Settlements
  - Opportunity Costs (Damaged Reputation, Lost IP)

**Cyber Threat Level**
- Open Source Intelligence
- Most likely threats
- Characterizes threat sophistication
- Relevance based on client’s
  - Technology
  - Industry
  - Geography
  - Politics

**Cybersecurity Level**
- Evaluates multiple perspectives
  - Technical
  - Procedural
  - Cultural
- May include advanced techniques
  - Threat-representative penetration testing
  - Social engineering to assess employee responses
- Validates regulatory compliance
  - NIST, HIPAA, PCI, CIP, SSAE16, GLBA, SOX, etc
Industry Spotlight: Financial Institutions

George Allport
Vice President & Financial Fidelity
Product Manager
Chubb
Spotlight Chair
Scary Reputation Unprotected Costume Horror

Goblin Phishing Violations Happy

TreatWeb Wolf Devices Halloween

Virus Pumpkin Spider

Spooky Malware Social

Cyber Privacy Breaches

Detection or Identity Evil

Caution Poisoned Theft

Sinister Ghost

October Monster Fraud

Media Risk Trick
Thank you to our 36 sponsors
Keynote Address Introduction

Mary Beth Borgwing
President, Cyber and Risk Practice
Advisen
Moderator
Keynote Address

Tom Finan
Senior Cybersecurity Strategist and Counsel, US Department of Homeland Security
Data Breach Table Top
Data Breach Table Top

Paul Nikhinson
Privacy Breach Response Services Manager
Beazley Breach Response Services
Moderator
Data Breach Table Top

- Paul Nikhinson, Privacy Breach Response Services Manager, Beazley Breach Response Services (Moderator)
- Alan Brill, Senior Managing Director, Kroll
- Michael Bruemmer, Vice President, Data Breach Resolution, Experian
- Bo Holland, Founder & CEO, AllClear ID
- John Mullen, Managing Director and Chair of the US Data Privacy and Network Security Group, Lewis Brisbois
Data Breach Table Top

Paul Nikhinson
Beazley

Alan Brill
Kroll

Michael Bruemmer
Experian

Bo Holland
AllClear ID

John Mullen
Lewis Brisbois
Closing Remarks