Welcome to Advisen’s Cyber Risk Insights Conference!
Welcoming Remarks

David Bradford
Co-Founder & Chief Strategy Officer
Advisen
Thank you to our Advisory Board

Elisabeth Case, Marsh
Nick Economidis, Beazley
James J. Giszczak, McDonald Hopkins LLC
Brad Gow, Endurance
Paul Pendolino, FM Global
Meredith Schnur, Wells Fargo Insurance
Melissa Ventrone, Thompson Coburn LLP [2016 Conference Chair]
Julian Waits, Sr., PivotPoint Risk Analytics
Thank you to our Sponsors!
Opening Remarks

Melissa Ventrone
Chair, Data Privacy & Security Group
Thompson Coburn LLP
[2016 Conference Chair]
Keynote Address

William Cook
Partner
Reed Smith
Lessons From the Darknet

Bill Cook
May 11, 2016
“No Battle Plan Survives Contact With the Enemy”

Field Marshal Helmuth von Moltke the Elder,
Prussian General Staff, 1864
War of German Unification
Design an Incident Response Plan That Really Works

• **Stick to the plan**
• Determine your particular risk
• Don’t “Cry wolf” – a measured reaction
• Who are your regulators
• What’s your bench strength
  • Outside counsel
  • Insurance
  • Forensic support (on retainer)
  • FBI / US Secret Service / Local Law Enforcement
• **Remediate**
• Scrub for the next time – make a record
Your particular risk

- Personal Information
- Inside job
- Fund transfer intercept schemes
- Trade secrets and proprietary information
- Access to vendors and other relationships: Target
- Compromised SCADA systems
- Ransomware
Where did they come from?

Phishing

Social engineering – Linked In, Facebook, Twitter, etc.

Exploit server operations (root access control)

Vendors/business partners
Phishing

Fewer than 20 attempts to achieve near 100% probability of success

FBI: 20 minutes from training class to successful phishing attack

To Do: Training, Training, Training
Loss of personal information

PHI more popular than PII

  Can’t change as much

  PII is more recoverable from Darknet

Average cost per lost record (201%):

  $297 per record ( + or -)

Waiting for chip impact
The Inside Job

Trusted/long time employees

Change of life events

Weak controls on email transfers and “work from home” status
Fraudulent Wire Transfers

• Started with Phishing

• Hijacked victim email account led to CFO email account

• Hacker saw discussion of “big transfer” – here $12 million payment to vendor

• Fake email addresses that are very similar to the victim’s are used to fool the recipient
  
  • joe@victimcompany.com vs. joe@viotimcompany.com
  
  • (Also CFO@bank.com v. CFO@bank.com.uk)

• False email from victim company CFO sent $12 million to a changed payee and new bank account in Hong Kong

• Saved by the fund transfer banker

• To Do: Work with your transfer agents – Red Flags
February – March 2012 twenty three (23) pipeline companies attacked by Chinese

Looking for SCADA access (admin.net vs. operations.net

DOJ sudden interest in April 2016

Mind the “air gap”

    Air gap beat by thumb drive & vendor

Supervisory control and data acquisition – remote maintenance and control
Ransomware: DDOS v. Cryptolock (2,453)

- **Source:** Phishing and website vulnerabilities
- **DDOS attack**
- **Crytolock encrypts entire system**
- **Directs victim to pay at website**
- **Or – resort to backup files or cloud storage**
- **Pre-attack prep**
  - Training
  - Anti-virus, email defense, network defense, application defense, anti-malware

Breach notification?
Post – Incident Scrub

- “OK, what did we learn from this?”

- Put conclusions in writing – save it – keep it where you can find it.
  - What did you do?
  - What didn’t you do?
  - How did your insurance respond?
  - Did your lack of budget have an impact?
  - Remediation plan? And follow-up schedule?
  - Set training.
Victim Banks v. Target (May 2015)

• Plaintiffs demanded prior incident response activity
• Court orders Target to turn over internal Target documents about POS data breaches since 2005
• Two major events to be disclosed
• Due diligence? Negligence? Red Flags from Forensic Vendor ignored.
Risk: Legal / Regulatory exposure

- Class action lawsuits claiming loss of data privacy
- Actions for violations of PCI guidelines that protect credit cards

**Regulatory actions**
- GLB – CFPB – *In re Dwalla Inc.* (March 2, 2016) $100,000 fine for failure to put security systems in place – failure to meet stated security standards – misrepresentation only, no intrusion or actual loss
- PCI potential breach results
  - $500,000 fine from each of 5 credit card issuers
  - Loss of credit card processing ability
  - Mandatory on-site audits
  - Class action exposure
- FTC and SEC
- AG Task Forces
What the Data Says: Cyber Trends
What the Data Says: Cyber Trends

Jim Blinn
EVP & Global Product Manager
Advisen
<table>
<thead>
<tr>
<th>Case Type / Case Status</th>
<th>Event</th>
<th>Response Costs</th>
<th>Economic Loss</th>
<th>Litigated Cases</th>
<th>Fines &amp; Penalties</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital Data Breach, Loss, or Theft</td>
<td>12,097</td>
<td>91</td>
<td>227</td>
<td>545</td>
<td>138</td>
<td>13,098</td>
</tr>
<tr>
<td>Privacy Violations</td>
<td>1,959</td>
<td>3</td>
<td>1,742</td>
<td>136</td>
<td></td>
<td>3,840</td>
</tr>
<tr>
<td>Improper Disposal/Distribution, Loss or Theft (Printed Records)</td>
<td>2,837</td>
<td>7</td>
<td>24</td>
<td>139</td>
<td>61</td>
<td>3,068</td>
</tr>
<tr>
<td>System/Network Security Violation or Disruption</td>
<td>1,420</td>
<td>22</td>
<td>61</td>
<td>32</td>
<td>9</td>
<td>1,544</td>
</tr>
<tr>
<td>Phishing, Skimming</td>
<td>777</td>
<td>2</td>
<td>85</td>
<td>42</td>
<td>5</td>
<td>911</td>
</tr>
<tr>
<td>Identity Theft/Fraudulent Use or Access</td>
<td>140</td>
<td>1</td>
<td>378</td>
<td>172</td>
<td>18</td>
<td>709</td>
</tr>
<tr>
<td>Improper Collection of Digital Data</td>
<td>283</td>
<td>284</td>
<td>42</td>
<td></td>
<td></td>
<td>609</td>
</tr>
<tr>
<td>Digital Asset Loss or Theft</td>
<td>115</td>
<td>1</td>
<td>17</td>
<td>26</td>
<td>2</td>
<td>161</td>
</tr>
<tr>
<td>Cyber Extortion</td>
<td>86</td>
<td>1</td>
<td>36</td>
<td>1</td>
<td>1</td>
<td>125</td>
</tr>
<tr>
<td>Undetermined/Other</td>
<td>28</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>28</td>
</tr>
<tr>
<td>Industrial Controls &amp; Operations</td>
<td>10</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td>11</td>
</tr>
<tr>
<td>Total</td>
<td>19,752</td>
<td>126</td>
<td>831</td>
<td>2,983</td>
<td>412</td>
<td>24,104</td>
</tr>
</tbody>
</table>
Cyber Event Geographic Distribution

**Country Case Count**

<table>
<thead>
<tr>
<th>Country</th>
<th>Case Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA</td>
<td>15,665</td>
</tr>
<tr>
<td>GBR</td>
<td>1,345</td>
</tr>
<tr>
<td>CAN</td>
<td>488</td>
</tr>
<tr>
<td>AUS</td>
<td>285</td>
</tr>
<tr>
<td>IRL</td>
<td>141</td>
</tr>
<tr>
<td>JPN</td>
<td>137</td>
</tr>
<tr>
<td>IND</td>
<td>111</td>
</tr>
<tr>
<td>NZL</td>
<td>106</td>
</tr>
<tr>
<td>DEU</td>
<td>89</td>
</tr>
<tr>
<td>CHN</td>
<td>87</td>
</tr>
<tr>
<td>Others</td>
<td>1,298</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>19,752</strong></td>
</tr>
</tbody>
</table>

**Cyber Event Count by Country**

- USA: 79%
- GBR: 7%
- CAN: 2%
- AUS: 1%
- IRL: 1%
- JPN: 1%
- IND: 1%
- NZL: 0%
- DEU: 0%
- CHN: 7%
- Others: 7%
Cyber Risk Heat Map
Industry Composition

- Finance and Insurance: 17%
- Health Care and Social Assistance: 14%
- Public Administration: 10%
- Educational Services: 10%
- Information: 9%
- Retail Trade: 7%
- Professional, Scientific, and Technical Services: 6%
- Manufacturing: 5%
- Administrative and Support and Waste Management and Remediation Services: 5%
- Accommodation and Food Services: 5%
- Other: 3%
Cyber Event Count
(>1M records exposed)
Relationship Between Affected Count and Response Cost
## Types of Data Lost by Industry

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Health Care and Social Assistance</td>
<td>42.33%</td>
<td>56.13%</td>
<td>1.09%</td>
<td>0.45%</td>
</tr>
<tr>
<td>Information</td>
<td>26.99%</td>
<td>55.06%</td>
<td>12.56%</td>
<td>5.38%</td>
</tr>
<tr>
<td>Administrative and Support and Waste Management and Remediation Services</td>
<td>45.10%</td>
<td>50.72%</td>
<td>3.31%</td>
<td>0.86%</td>
</tr>
<tr>
<td>Professional, Scientific, and Technical Services</td>
<td>40.02%</td>
<td>48.80%</td>
<td>8.38%</td>
<td>2.79%</td>
</tr>
<tr>
<td>Public Administration</td>
<td>42.88%</td>
<td>45.39%</td>
<td>7.58%</td>
<td>4.16%</td>
</tr>
<tr>
<td>Other Services (except Public Administration)</td>
<td>46.80%</td>
<td>43.30%</td>
<td>7.22%</td>
<td>2.68%</td>
</tr>
<tr>
<td>Utilities</td>
<td>50.00%</td>
<td>43.24%</td>
<td>6.76%</td>
<td>0.00%</td>
</tr>
<tr>
<td>Arts, Entertainment, and Recreation</td>
<td>46.59%</td>
<td>43.18%</td>
<td>2.84%</td>
<td>7.39%</td>
</tr>
<tr>
<td>Wholesale Trade</td>
<td>46.67%</td>
<td>41.85%</td>
<td>6.67%</td>
<td>4.81%</td>
</tr>
<tr>
<td>Retail Trade</td>
<td>55.92%</td>
<td>40.93%</td>
<td>2.27%</td>
<td>0.89%</td>
</tr>
<tr>
<td>Construction</td>
<td>53.00%</td>
<td>39.00%</td>
<td>8.00%</td>
<td>0.00%</td>
</tr>
<tr>
<td>Educational Services</td>
<td>58.64%</td>
<td>37.23%</td>
<td>2.79%</td>
<td>1.33%</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>51.19%</td>
<td>37.20%</td>
<td>6.15%</td>
<td>5.45%</td>
</tr>
<tr>
<td>Transportation and Warehousing</td>
<td>56.52%</td>
<td>32.37%</td>
<td>8.70%</td>
<td>2.42%</td>
</tr>
<tr>
<td>Management of Companies and Enterprises</td>
<td>50.81%</td>
<td>32.26%</td>
<td>11.29%</td>
<td>5.65%</td>
</tr>
<tr>
<td>Real Estate and Rental and Leasing</td>
<td>64.14%</td>
<td>28.97%</td>
<td>4.83%</td>
<td>2.07%</td>
</tr>
<tr>
<td>Mining, Quarrying, and Oil and Gas Extraction</td>
<td>34.78%</td>
<td>26.09%</td>
<td>21.74%</td>
<td>17.39%</td>
</tr>
<tr>
<td>Finance and Insurance</td>
<td>69.38%</td>
<td>24.93%</td>
<td>4.39%</td>
<td>1.30%</td>
</tr>
<tr>
<td>Accommodation and Food Services</td>
<td>75.00%</td>
<td>22.18%</td>
<td>2.02%</td>
<td>0.81%</td>
</tr>
<tr>
<td>Agriculture, Forestry, Fishing and Hunting</td>
<td>85.71%</td>
<td>14.29%</td>
<td>0.00%</td>
<td>0.00%</td>
</tr>
</tbody>
</table>
Year-Over-Year Frequency Increase
# Control System Hacks

<table>
<thead>
<tr>
<th>Company</th>
<th>Year</th>
<th>Type</th>
<th>Location</th>
<th>Affected Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prykarpattyaoblenergo</td>
<td>2015</td>
<td>Power Grid</td>
<td>Ukraine</td>
<td>80,000</td>
</tr>
<tr>
<td>US Power Company</td>
<td>2012</td>
<td>Turbine Control System</td>
<td>USA</td>
<td>-</td>
</tr>
<tr>
<td>Siemens</td>
<td>2010</td>
<td>Industrial Control System</td>
<td>USA</td>
<td>-</td>
</tr>
<tr>
<td>Pentagon</td>
<td>2011</td>
<td>Data Theft</td>
<td>USA</td>
<td>24,000</td>
</tr>
<tr>
<td>Mitsubishi</td>
<td>2011</td>
<td>Manufacturing Plant</td>
<td>Japan</td>
<td>-</td>
</tr>
</tbody>
</table>
## Business E-mail Compromise Scams

<table>
<thead>
<tr>
<th>Company</th>
<th>Year</th>
<th>Industry</th>
<th>Total Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ubiquiti Networks Inc.</td>
<td>2015</td>
<td>Tech Firm</td>
<td>$46.7M</td>
</tr>
<tr>
<td>XOOM Corp</td>
<td>2014</td>
<td>Tech Firm</td>
<td>$30.8M</td>
</tr>
<tr>
<td>The Scoular Company</td>
<td>2015</td>
<td>Commodities Trader</td>
<td>$17.2M</td>
</tr>
<tr>
<td>Medidata</td>
<td>2014</td>
<td>Tech Firm</td>
<td>$4.8M</td>
</tr>
<tr>
<td>Wright Hotels</td>
<td>2015</td>
<td>Property Developer</td>
<td>$1M</td>
</tr>
<tr>
<td>AFGlobal Corporation</td>
<td>2014</td>
<td>Steel Piping</td>
<td>$480K</td>
</tr>
<tr>
<td>Owens, Schine &amp; Nicola</td>
<td>2008</td>
<td>Law Firm</td>
<td>$197K</td>
</tr>
<tr>
<td>Taylor &amp; Lieberman</td>
<td>2012</td>
<td>Accounting Firm</td>
<td>$99K</td>
</tr>
</tbody>
</table>
## Cyber D&O Cases

<table>
<thead>
<tr>
<th>Company</th>
<th>Year</th>
<th>Type</th>
<th>Status</th>
<th>Total Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>The TJX Companies</td>
<td>2007</td>
<td>Derivative</td>
<td>Settled</td>
<td>$0.5M</td>
</tr>
<tr>
<td>Heartland Payment</td>
<td>2009</td>
<td>SCAS &amp; Derivative</td>
<td>Dismissed</td>
<td>-</td>
</tr>
<tr>
<td>Systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>News Corporation</td>
<td>2011</td>
<td>SCAS &amp; Derivative</td>
<td>Settled</td>
<td>$139M</td>
</tr>
<tr>
<td>Target Corporation</td>
<td>2014</td>
<td>Derivative</td>
<td>Pending</td>
<td>-</td>
</tr>
<tr>
<td>Wyndham Corp.</td>
<td>2014</td>
<td>Derivative</td>
<td>Dismissed</td>
<td>-</td>
</tr>
<tr>
<td>The Home Depot</td>
<td>2014</td>
<td>Derivative</td>
<td>Pending</td>
<td></td>
</tr>
<tr>
<td>Xoom Corporation</td>
<td>2015</td>
<td>SCAS</td>
<td>Pending</td>
<td></td>
</tr>
<tr>
<td>MobileIron</td>
<td>2015</td>
<td>SCAS</td>
<td>Pending</td>
<td></td>
</tr>
</tbody>
</table>
Cyber Penetration Rate

Penetration Rate by Company Size

Company Size (S)

Penetration Rate

0%  5%  10%  15%  20%  25%  30%  35%  40%

0<500K  500K<1M  1M<2.5M  2.5M<5M  5M<10M  10M<25M  25M<100M  100M<300M  300M<1B  1B<5B  5B+
Pretiums at Renewal

Pretiums at Renewal: ADVx Index

- Middle Market Composite
- Large Market Composite
- Cyber Liability
Average Cyber Limits & Premiums

![Graph showing average limits and premiums by company size.](graph_url)
Change in Limits at Renewal

![Bar chart showing percent change at renewal for Umbrella and Cyber categories from 2007 to 2015.]
About Advisen Ltd.
Advisen is leading the way to smarter and more efficient risk and insurance communities. Through its information, analytics, ACORD messaging gateway, news, research, and events, Advisen reaches more than 150,000 commercial insurance and risk professionals at 8,000 organizations worldwide. The company was founded in 2000 and is headquartered in New York City, with offices in the US and the UK.

+1 (212) 897-4800 | info@advisen.com | www.advisenltd.com

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**.
The Risk Manager’s Perspective
The Risk Manager’s Perspective

Mark Kollar
CEO and Lead Underwriter
Edgewater Holdings, Ltd.
(Moderator)
The Risk Manager’s Perspective

- Mark Kollar, CEO and Lead Underwriter, Edgewater Holdings, Ltd. (Moderator)

- Graeme Harper, SVP Global Insurance, FIS Global

- Rich Moore, Managing Director, Alvarez & Marsal
The Risk Manager’s Perspective
Morning Break

Coming up next...
“The Underwriting Process Laid Bare”
Thank you to our Sponsors!
The Underwriting Process Laid Bare
The Underwriting Process Laid Bare

Meredith Schnur
Senior Vice President
Professional Risk Practice
Wells Fargo Insurance
(Moderator)
The Underwriting Process Laid Bare

- Meredith Schnur, Senior Vice President, Professional Risk Practice, Wells Fargo Insurance (Moderator)
- Michael Carr, Technology Practice Leader, Argo Group
- Nick Economidis, Underwriter, Beazley
- Adam Kopcio, Vice President, Professional Risk, Endurance
- Julian Waits, Sr., President & CEO, PivotPoint Risk Analytics
The Underwriting Process Laid Bare
The Claims Process
The Claims Process

Kevin Sullivan
Managing Director
Marsh
(Moderator)
The Claims Process

- Kevin Sullivan, Managing Director, Marsh (Moderator)
- Jill Linhardt, Executive Vice President, NAS
- Brian Robb, Claims Director, CNA
- Todd Rowe, Partner, Tressler LLP
- David Standish, Complex Claim Director, Cyber / Media / Technology, AIG
The Claims Process
Conference Luncheon

Join us for our lunch roundtable discussion in the Rialto Room!

Coming up after lunch...
“Who Owns Cyber Risk?”
Thank you to our Sponsors!
Who Owns Cyber Risk?
Who Owns Cyber Risk?

Ben Beeson
Cyber Risk Practice Leader
Lockton Companies
(Moderator)
Who Owns Cyber Risk?

- Ben Beeson, Cyber Risk Practice Leader, Lockton Companies (Moderator)
- Doug Backes, Vice President, Manager of Staff Claims, FM Global
- Bill Jennings, Crime Manager, Beazley
- Kirstin Simonson, 2VP, Cyber Lead, Travelers
- Vernon Suckerman, Vice President, Underwriting Manager, XL Catlin
Who Owns Cyber Risk?
Regulation Update

• Elisabeth Case, Senior Vice President, Commercial E&O Practice Leader, Marsh
• James Giszczak, Chair, Data Privacy and Cybersecurity Practice, McDonald Hopkins LLC
• Jeff Greene, Director NAM Government Affairs & Senior Policy Counsel, Symantec
• Matt Prevost, Cyber/Technology E&O Product Manager, Chubb
Afternoon Break

Coming up next...
“Extortion”
Thank you to our Sponsors!
Extortion
Extortion

Andy Obuchowski
Practice Leader, Digital Forensics & Incident Response Services, RSM US LLP
(Moderator)
Extortion

- Andy Obuchowski, Practice Leader, Digital Forensics & Incident Response Services, RSM US LLP (Moderator)
- Jeffrey J. Carpenter, Director, Incident Response and Digital Forensics Practice, SecureWorks
- Bill Hardin, Vice President, Charles River Associates
- John Merchant, Division Head, Cyber & Professional Liability, Nationwide
- Vinny Troia, Founder, Principal Security Consultant, Night Lion Security
Extortion
Cyber War Game
Breach Simulation
Cyber War Game Breach Simulation

Winston Krone
Managing Director,
Kivu Consulting
(Moderator)
Cyber War Game Breach Simulation

- Winston Krone, Managing Director, Kivu Consulting (Moderator)
- Steven Anderson, VP, Product Executive - Privacy & Network Security, QBE
- Austin Murphy, Director, Incident Response Services, CrowdStrike
- Randy Samborn, Senior Vice President, LEVICK
Cyber War Game Breach Simulation

Bing Pulse Polling

ENTER NOW:

i.engage.ms/AdvisenEvents
Scenario 1:

While getting your first cup of coffee, you receive a phone call from the US Secret Service.

An agent says he has evidence that at least one of your IT systems had been compromised and they believe customer personally identifiable information may have been stolen.

He has asked for a meeting with someone on your executive staff as soon as possible.

Question: Who do you call?

1. CISO - this is an IT problem at this stage
2. Chairman of the Board of Directors - take it right to the top
3. Communications advisor - we need to protect our reputation
4. Outside legal counsel - we just don’t want to get sued
5. Insurance broker - we have cover, let’s get this rolling
Scenario 2:

The possible theft of customer information has got out to the media.

CNN reporter Abby Salander calls. An anonymous source has informed her that your company has been victim of a hacking attack.

She is preparing a live piece to camera from outside your offices and wants a statement immediately.

Question: How do you respond to the press?

1. Refuse to comment
2. Say your priority is your customers and consumers so you can’t talk to the media right now
3. Tell them everything you know at this stage - you don’t know who the attackers are, your IT systems are in disarray and you hope it’s a hoax
4. Give them a holding statement that expresses concern but gives no further detail
5. Say you cannot comment due to an ongoing investigation
Scenario 3:

You realize that this is real - your PII has been stolen, systems outages are happening.

You are undergoing a data breach. It’s time to call in the expert external advisors to help with crisis response.

Question: Who do you call?

1. We have retainers in place and call the numbers listed in our crisis response plan
2. We have insurance. They should be appointing external advisors on our behalf.
3. We’ll find the best advisors from a google search. Insurance will pay for them. We will notify them later
4. Call the insurers: who do they recommend from their list of approved service providers?
Key Takeaways
Join us for our reception sponsored by Experian™