Cyber Security & Data Breaches: The Big New Exposure for Ds & Os?
CYBER SECURITY AND DATA BREACHES: THE BIG NEW EXPOSURE FOR Ds & Os?

MODERATOR:

John Black, Esq., Executive Principal, Skarzynski Black LLC

PANELISTS:

Shanda Davis, D&O Product Manager, Travelers
Todd Greeley, Esq., Vice President, Berkshire Hathaway Specialty Insurance
Douglas W. Greene, Esq., Attorney at Law, Lane Powell PC
Jeffrey R. Lattmann, Executive Managing Director, Beecher Carlson
Overview of Data Breaches and Cybercrime
Nature of Data Breaches and Cybercrime

Most Common Causes of Breaches

- POS Intrusions (14%)
- Web App Attacks (35%)
- Insider Misuse (8%)
- Physical Theft/Loss (1%)
- Miscellaneous Errors (2%)
- Crimeware (Malware other than cyber-espionage or POS) (4%)
- Card Skimmers (9%)
- Cyber-espionage (22%)

2014 Verizon Data Breach Investigations Report
ANSWER: 1.48 million.

Identify Theft Resource Center
ANSWER: $16 million

ANSWER:
According to Mandiant, the median number of days for a company to detect a compromise of its network was 229.
ANSWER:
Twitter – only 250,000 user names and emails were compromised
# U.S. Privacy Laws

## State

<table>
<thead>
<tr>
<th>Data Breach Notification</th>
<th>Social Security Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>(47 states +)</td>
<td>(34 states)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Payment Card</th>
<th>Reasonable Security Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Wash. &amp; Minn.)</td>
<td>(9 states/Massachusetts Reg. 17)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Encryption</th>
<th>Disposal/Destruction</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Nev. &amp; Mass.)</td>
<td>(29 states)</td>
</tr>
</tbody>
</table>

## Federal

<table>
<thead>
<tr>
<th>Federal Trade Commission</th>
<th>Dept. of Health and Human Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section 5 of the Federal Trade Commission Act</td>
<td>Health Insurance Portability and Accountability Act (HIPAA)</td>
</tr>
<tr>
<td>• “Notice and choice”</td>
<td>Health Information Technology for Economic Clinical Health Act (HITECH)</td>
</tr>
<tr>
<td>• “Harm-based” – reasonable security</td>
<td></td>
</tr>
<tr>
<td>• “Privacy by design”</td>
<td></td>
</tr>
</tbody>
</table>

Gramm-Leach Bliley Act (GLBA)
Children’s Online Privacy Protection Act (COPPA)
Regulatory Exposures

• **FTC Investigations and Charges:**
  – Section 5(a) of Federal Trade Commission Act, prohibiting unfair and deceptive practices affecting commerce
  – Gramm-Leach Bliley Act (GLBA)

• **HHS Investigations and Charges:**
  – HIPAA/HITECH

• **State Attorney General Investigations and Actions:**
  – HIPAA/HITECH violations
  – State unfair and deceptive trade practices laws
  – State breach notification laws
  – Other state cyber breach legislation (Massachusetts Reg. 17, e.g.)
Disclosure Obligations

• SEC’s October 2011 Disclosure Guidance:  
  Issuers are obligated to disclose material cyber risks, including:
  - If one or more cyber incidents materially affect products, services or customer or vendor relationships, issuers should disclose in “Description of Business.”
  - Cyber incidents may result in diminished future cash flows that should be considered when preparing financial statements.
  - SEC expects issuers to evaluate their cybersecurity risks for disclosure under Item 503(c) of Regulation S-K.

• Breach notification laws:  
  - 47 states require notification if personally identifiable information was or may have been acquired by unauthorized persons.
  - HITECH requires notification if private health information was or may have been acquired by unauthorized persons.
Civil Liability for Data Breaches and Cybercrime

- **Class-Action Lawsuits** against corporations by customers/clients for mishandling personal information.
- **Derivative Suits** against directors and officers for breach of fiduciary duty for failing to adequately oversee cyber security.
- **Securities Class-Action Lawsuits** alleging false or misleading statements about cyber risks.
Case Studies on Cybersecurity Issues Affecting D&O Liability
Heartland Payment Systems

• Heartland was the fifth-biggest payments processor in the U.S.

• Heartland announced in January 2009 that unknown intruders had broken into its systems and stolen card data.

• More than 130 million credit and debit cards were believed to have been compromised in the intrusion.

• At the time, that was the largest ever criminal breach.

• Heartland eventually paid more than $110 million to Visa, MasterCard, American Express and other card associations to settle claims related to the breach.
TJ Maxx

• In 2007, thieves stole more than 45 million customer credit and debit card numbers

• TJX said its computer systems were first breached in July 2005, but it didn’t find out about the breach until late 2006 - the thefts took place over eighteen month period without anyone knowing.

• The breach ended up costing TJX $256 million
Wyndham

• Data breaches occurred on 3 separate occasions that led to fraudulent charges on customers’ accounts and the export of credit card information to an Internet domain address registered in Russia.

• 619,000 consumer payment card account numbers were compromised; $10.6 million in fraudulent charges.

• Wyndham did not disclose the breach until 2.5 years after the third breach occurred.

• Wyndham was hit with a derivative suit and FTC charges.
Target

• Attackers stole card data by installing malicious software on point-of-sale devices in the checkout lines at Target stores

• The malware got into Target’s system through a heating, air conditioning and refrigeration firm that did business with Target and had Target network credentials

• More than 110 million customers were affected

• Target hit with derivative suits
View from the Corporate Boardroom
Best Practices for Boards to Consider

• Board-Level Risk Management Committee
• CISO
• Employee Training
• Breach Planning
• Vendor Oversight
• Cyber Insurance
• Other
Issues for D&O Underwriting and Broking

- Impact on Application and Screening Risks
- Impact on Policy Form
- Issues Concerning Specific Industries
  - Restaurants/Hospitality
  - Retailers
  - Financial Services
  - Health
  - Education
Frequency of Incident Classification Patterns Per Victim Industry

<table>
<thead>
<tr>
<th>INDUSTRY</th>
<th>POS INTRUSION</th>
<th>WEB APP ATTACK</th>
<th>INSIDER MISUSE</th>
<th>THEFT/LOSS</th>
<th>MISC. ERROR</th>
<th>CRIMEWARE</th>
<th>PAYMENT CARD SKimmer</th>
<th>DENIAL OF SERVICE</th>
<th>CYBER ESPIONAGE</th>
<th>EVERYTHING ELSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accommodation</td>
<td>75%</td>
<td>1%</td>
<td>8%</td>
<td>1%</td>
<td>1%</td>
<td>1%</td>
<td>&lt;1%</td>
<td>10%</td>
<td>-</td>
<td>4%</td>
</tr>
<tr>
<td>Education</td>
<td>&lt;1%</td>
<td>19%</td>
<td>8%</td>
<td>15%</td>
<td>20%</td>
<td>6%</td>
<td>&lt;1%</td>
<td>6%</td>
<td>2%</td>
<td>22%</td>
</tr>
<tr>
<td>Finance</td>
<td>&lt;1%</td>
<td>27%</td>
<td>7%</td>
<td>3%</td>
<td>5%</td>
<td>4%</td>
<td>22%</td>
<td>26%</td>
<td>&lt;1%</td>
<td>6%</td>
</tr>
<tr>
<td>Healthcare</td>
<td>9%</td>
<td>3%</td>
<td>15%</td>
<td>46%</td>
<td>12%</td>
<td>3%</td>
<td>&lt;1%</td>
<td>2%</td>
<td>&lt;1%</td>
<td>10%</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>14%</td>
<td>8%</td>
<td>4%</td>
<td>2%</td>
<td>9%</td>
<td>&lt;1%</td>
<td>24%</td>
<td>30%</td>
<td>9%</td>
<td></td>
</tr>
<tr>
<td>Retail</td>
<td>31%</td>
<td>10%</td>
<td>4%</td>
<td>2%</td>
<td>2%</td>
<td>2%</td>
<td>6%</td>
<td>33%</td>
<td>&lt;1%</td>
<td>10%</td>
</tr>
<tr>
<td>Transportation</td>
<td>15%</td>
<td>16%</td>
<td>7%</td>
<td>6%</td>
<td>15%</td>
<td>5%</td>
<td>3%</td>
<td>24%</td>
<td>8%</td>
<td></td>
</tr>
<tr>
<td>Utilities</td>
<td>38%</td>
<td>3%</td>
<td>1%</td>
<td>2%</td>
<td>31%</td>
<td>&lt;1%</td>
<td>14%</td>
<td>7%</td>
<td>3%</td>
<td></td>
</tr>
</tbody>
</table>

Verizon 2014 Data Breach Investigations Report
Predictions
Questions for the Panel