Cyber Liability

Threats, Coverage, and Surviving a Breach
Panelists

• Kirstin Simonson: 2nd Vice President, Travelers  
  – Global Technology Cyber Leader

• Mario Paez: Vice President, Wells Fargo Insurance  
  – National Practice Cyber Advisor

• Mark Lanterman: Chief Technology Officer,  
  Computer Forensic Services
Agenda

- Cyber Event Case Study
- Evolution of Cyber Liability Exposures
- Gap Analysis: Traditional Policy Deficiencies
- Insurance Solutions
- Cyber Event Response
- Underwriting Implications
Cyber Event Case Study
Fraudulent Wire

• $952,800 wire
• Romania
• RSA token
• Bookkeeper- denies involvement
Analysis

• Evidence is consistent
• Zeus
Dear Mr. Caravello Chief Financial Officer - CFO,

Winfield Community Bank, 27w111 Geneva Rd

The Federal Deposit Insurance Corporation (FDIC) has to report that counterfeit cashier’s checks display a large variety of routing numbers, which are assigned to a large number of small and medium size banks all over USA. The items are blue, have rounded corners, and display security feature statement embedded within a darkened top border. The bank’s logo, name, and website address appear near the top-left corner of the counterfeit items. Authentic cashier’s checks are yellow and display a security padlock icon at the end of the written dollar amount line. The bank’s name appears near the top-center area.

Copies of a counterfeit item are available to be seen at https://fdic.gov/starsmail/check_sample.asp for your review.

11034, Arlington, Virginia 22226, or transmitted electronically to alert@fdic.gov. Questions related to federal deposit insurance or consumer issues should be submitted to the FDIC using an online form that can be accessed at http://www2.fdic.gov/お客new/index.asp.

For your reference, FDIC Special Alerts may be accessed from the FDIC’s Web site at www.fdic.gov/news/news/SpecialAlert2011/index.html. To learn how to automatically receive FDIC Special Alerts through e-mail, please visit www.fdic.gov/about/subscriptions/index.html.

Sandra L. Thompson
Director
Division of Risk Management Supervision

Attachment (not available electronically)

NOTE: Any email containing the FDIC document name in the subject line is not from the FDIC.
Ukrainian General Arrested in Cyber Heists

A decorated Ukrainian general was arrested last week in Romania along with two other men suspected of being part of an organized cybercrime gang that laundered at least $1.4 million stolen from U.S. and Italian firms.

Apprehended in Iasi, Romania last week were Matei Vitalie, 37, of Moldova; Konstantin Ossipov, a 42-year-old Israeli citizen; and 54-year-old Valeriu Gaichuk, a Ukrainian general who, according to his Facebook page, once studied at Florida International University in Miami.

Romanian prosecutors allege that the men created fake companies and business contracts to help to launder funds that were stolen from at least two firms, including $952,800 from the Society of Corporate Compliance and Ethics, an organization based...
Evolution of Cyber Liability: Insurance and Exposures

- **Late 1990’s**
  - With evolution of technology, started to see insurance evolving to address
  - Early policies focused on media/content exposures
- **Early 2000’s**
  - Online media policies began starting to cover liability associated with data breach and virus transmission
  - Several exclusions
  - California Security Breach and Information Act became effective
- **Mid 2000’s**
  - Started to see 1st party coverages
- **2010’s**
  - Number of carriers with a standalone cyber policy exploded
  - 2014 – Year of the Retail Breach
  - 2015 – Year of the Healthcare Breach
  - 2016 – Continued evolution of insurance response
Evolution of Cyber Liability: Insurance and Exposures

Threat Actors

- **Organized crime**
  - Payment cards
  - Credentials
  - Bank account info

- **State-affiliated**
  - Credentials
  - Internal organization data
  - Trade secrets
  - System information

- **Hactivists**
  - Politically or socially motivated
  - System disruption
  - Internal organization data
Evolution of Cyber Liability: Insurance and Exposures

Legal Issues and Regulatory Environment

**Legally mandated**

- 47 states with privacy breach notification laws
  - Recent federal executive orders – will federal legislation finally be passed? Will it preempt?
- HIPAA/HITECH regulations
- FTC
  - Federal Trade Commission Act Section 5, Red Flags
- State Consumer Protection Laws
  - California’s Song-Beverly Credit Card Act
- Foreign laws and regulations
  - EU Privacy Directive
    - Broader than US laws
- Other federal laws
  - SEC Guidance, COPPA, FCRA, FACTA, etc.

**Industry Standard**

- PCI DSS compliance
  - Required if storing, processing or transmitting payment card data
  - Significant fines, penalties and costs assessed
- Contractual obligations
  - Increasingly included in insurance provisions of customer/vendor contracts
State Regulations: Notice Requirements

- 47 states and 4 U.S. jurisdictions require notice to customers after unauthorized access to PII

- Timing requirements for notifying residents
  - “without unreasonable delay” (means not later than 30 days)
  - FL was 45, is now 30 days

- Notify State Attorneys General, consumer protection agencies and credit reporting agencies
  - New requirement in ND, OR, and FL

- Timing requirements for notifying regulators and credit reporting agencies
  - 48 hours; 14 days; before notice to residents

- Constant Change - Amendments bring changes in MT, NV, ND, OR, TN, UT, VA, WA, WY, LA, IO, CT
  - Broader definitions of Personal Information and new protections for student data
  - More specific content in notice letters
  - CT to be first state to require by law that credit monitoring be provided
Evolution of Cyber Liability: Insurance and Exposures

2015 Data Breach Threats

- 28.5% POS Intrusions
- 18.8% Crimeware
- 18% Cyber Espionage
- 10.6% Insider Misuse

- 2,122 confirmed data breaches (up from 1,367 in 2014)
- 79,790 reported security incidents (up from 63,437 in 2014)
- 61 countries represented (down from 95 in 2014)

## Evolution of Cyber Liability: Insurance and Exposures

### 2015 Confirmed Data Breaches By Industry

<table>
<thead>
<tr>
<th>Industry</th>
<th>Confirmed Breaches</th>
<th>How did they occur?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finance</td>
<td>465</td>
<td>18% Miscellaneous errors</td>
</tr>
<tr>
<td>Public Sector</td>
<td>175</td>
<td>20% Crimeware</td>
</tr>
<tr>
<td>Retail</td>
<td>148</td>
<td>25% Insider misuse</td>
</tr>
</tbody>
</table>

- **2,122 Confirmed Breaches – Top 3 Industry Classes**
- **79,790 Incidents – How did they occur?**

2015 Claims Study: Preliminary Findings

<table>
<thead>
<tr>
<th>Data type</th>
<th>Cause of loss</th>
<th>Business sectors</th>
</tr>
</thead>
<tbody>
<tr>
<td>PII - 45%</td>
<td>Hackers - 31%</td>
<td>Healthcare sector - 21%</td>
</tr>
<tr>
<td>PHI - 27%</td>
<td>Malware/virus - 14%</td>
<td>Financial services - 17%</td>
</tr>
<tr>
<td>PCI - 14%</td>
<td>Staff mistakes and rogue employees tied – 11%*</td>
<td>Retail – 13%*</td>
</tr>
</tbody>
</table>

*First time rogue employees in top 3 causes

*Largest breaches occurred in retail

Data

- Sample size – 160 insured claims
- PII data type in 2014 study – 41%
- PCI data type in 2014 study – 19%
- PHI data type in 2014 study – 21%

Company size

- Nano-cap (under $50 million in revenue) experienced the most incidents – 29%
- Small-cap (under $2B in revenue) followed closely at 25%
# Gap Analysis: Traditional Policy Deficiencies

<table>
<thead>
<tr>
<th></th>
<th>Property</th>
<th>General Liability</th>
<th>Crime</th>
<th>K&amp;R</th>
<th>E&amp;O</th>
<th>Cyber</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1st Party Exposure/Loss</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical damage to data only</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Virus/hacker damage to data only</td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Denial of service (DOS) attack</td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Business interruption loss from security event</td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Extortion or threat</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employee sabotage of data only</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Impostor fraud</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>3rd Party Exposure/Loss</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Theft/disclosure of private information</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidential corporate information breach</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technology E&amp;O</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Media liability (electronic content)</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privacy breach expense and notification</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Damage to 3rd party’s data only</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regulatory privacy defense / fines</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Virus/malicious code transmission</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **x** - No Coverage
- **-** - Possible Coverage
- **✓** - Coverage
<table>
<thead>
<tr>
<th>First Party</th>
<th>May include expenses paid to Insured for:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Data breach notifications and related expenses</td>
</tr>
<tr>
<td></td>
<td>• Forensics and legal services</td>
</tr>
<tr>
<td></td>
<td>• Extortion demands, including ransomware</td>
</tr>
<tr>
<td></td>
<td>• Business interruption loss</td>
</tr>
<tr>
<td></td>
<td>• Data Restoration costs</td>
</tr>
<tr>
<td></td>
<td>• Credit or identity monitoring expense</td>
</tr>
<tr>
<td>Third Party</td>
<td>May include liability coverage for:</td>
</tr>
<tr>
<td></td>
<td>• Data breach or other information security breaches</td>
</tr>
<tr>
<td></td>
<td>• Intellectual property/media/content offenses</td>
</tr>
<tr>
<td></td>
<td>• Regulatory defense and associated fines/penalties</td>
</tr>
<tr>
<td></td>
<td>• PCI DSS contract penalties assessment defense</td>
</tr>
<tr>
<td></td>
<td>• Professional services/E&amp;O liability</td>
</tr>
</tbody>
</table>
Cyber Event Response

- Engage IR Plan
- Fix the problem
- Notification as needed
- Legal/Forensic
- Cyber Event
- Insurance
- Crisis Management (PR)
Underwriting Implications

• Exposure Evaluation
  - Critical risk analysis
    - Data breach = records
    - Business Interruption = lost profits due to inability to conduct business
    - Liability = professional exposures
    - Intellectual property = content

• Management Controls
  - Formalized, tested and monitored
    - Network and Information Security = Incident Response Plan
    - Business Interruption = Business continuity plan, including testing of backups
    - Intellectual Property = IP Clearance and due diligence