“Disruptive Technology”... The New Frontier

Michael Serricchio, Marsh Captive Solutions
Karl Pedersen, Marsh FINPRO
Steve McElhiney, EWI Re, Inc.
Moderator: Alan Kandel, A.M. Best Rating Services, Inc.

March 14, 2017
Agenda

• Disruptive Technology
• What’s Happening and What’s the Trend
• How Do Captives Fit In?
• Cyber Risk and Disruptive Technology: An Experts Perspective
• A Captive owner’s Vision
Michael Serricchio
Marsh Captive Solutions
“Disruptive Technology” 11 Years Ago

• “Playing the Game Differently”
• Creates a New Market
• Transforms or Destroys Current Market
• Products Become
  – Simpler
  – More Affordable
  – More Accessible
  – Customizable
• Drives Growth
• Where do Captives fit in???
Technology is Going to Advance and There is No Stopping it, Even if it Ruins an Industry...
Conference In-Session Polling

1. Search “CICA International Conference” in your app store or if you have already downloaded the Conf. App, open it.

2. Select the SCHEDULE Icon

4. Select Tuesday, March 14th

5. Select 10:00am - “Disruptive Technology”… The New Frontier

6. Look for LIVE POLLS and select “Question 1”

*Please refrain from answering additional polling questions until prompted.*
Polling Question #1

• What is “Lemonade”?
  A. Technology Platform for Beverage Distributors
  B. Sweet and tasty summertime beverage
  C. Online Peer to Peer (P2P) Insurance Platform
  D. Captive Insurance Software Technology to Assist with Claims handling
Your poll will display here

View this slide in slideshow mode to display results

Click “enable content” if PowerPoint displays a security warning

This slide is compatible with:
- PowerPoint 2010 (Windows)
- PowerPoint 2007 (Windows)

Using a different version of PowerPoint?
Return to your poll and download the correct slide
Available for:
- PowerPoint 2013 SP1 (Windows)
- PowerPoint for Mac 2011 (Mac)

Having trouble viewing the poll?
[View This Poll on the Web]
Get help online at polls.cvent.com/help
...The Good News is That it Often Creates a New Industry
“You don’t know when the transition period will start. The idea is to understand that it will... and become prepared for it.”

-Dr. Timothy Bishop
Future Studies, University of Houston
## Industry Benchmarking
### Captive Use by Industry (2016)

<table>
<thead>
<tr>
<th>Industry</th>
<th>Gross Premiums Written in USD</th>
<th>% of Captives (#)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial Institutions</td>
<td>$19,862,427,164</td>
<td>24%</td>
</tr>
<tr>
<td>Communications, Media &amp; Technology</td>
<td>$4,900,099,427</td>
<td>4%</td>
</tr>
<tr>
<td>Health Care</td>
<td>$2,793,215,961</td>
<td>14%</td>
</tr>
<tr>
<td>Retail/Wholesale</td>
<td>$2,538,371,058</td>
<td>6%</td>
</tr>
<tr>
<td>Life Sciences</td>
<td>$1,516,661,281</td>
<td>2%</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>$1,316,883,753</td>
<td>7%</td>
</tr>
<tr>
<td>Transportation</td>
<td>$933,306,200</td>
<td>4%</td>
</tr>
<tr>
<td>Power &amp; Utility</td>
<td>$853,667,060</td>
<td>4%</td>
</tr>
<tr>
<td>Marine</td>
<td>$812,302,006</td>
<td>2%</td>
</tr>
<tr>
<td>Food &amp; Beverages</td>
<td>$614,577,060</td>
<td>2%</td>
</tr>
<tr>
<td>Aviation, Aerospace &amp; Space</td>
<td>$605,750,831</td>
<td>1%</td>
</tr>
<tr>
<td>Mining, Metals &amp; Minerals</td>
<td>$594,014,521</td>
<td>2%</td>
</tr>
<tr>
<td>Energy</td>
<td>$592,870,203</td>
<td>3%</td>
</tr>
<tr>
<td>Other</td>
<td>$1,971,718,649</td>
<td>25%</td>
</tr>
</tbody>
</table>
Lines of Coverage: Traditional / Non-Traditional

Growth in Non-Traditional coverages 2015-2016:
- Employee Benefits: 142.86%
- Supply Chain: 133.33%
- Cyber Liability: 30.00%
- Political Risk: 26.67%
- Medical Stop Loss: 13.89%

Source: Marsh’s Benchmarking Survey Analysis
Risk Transfer vs. Risk Retention Captive Owners

**EXPOSURES**
- ASSETS
- EMPLOYEES
- CUSTOMERS

**RISKS**
- TECHNOLOGY/CYBER
- CAT RISK (EQ, WIND, FLOOD)
- TIME ELEMENT
- PRODUCT
- WAGE & HOUR
- EPL
- CRIME
- WC
- BENEFITS
- WARRANTY
- GENERAL LIABILITY
- RECALL
- E&O

**TRANSFER RISK**
- Commercial Insurance

**RETAIN RISK**
- Retain
  - In Captive
Karl Pedersen
Marsh FINPRO
“In short, the cyber threat cannot be eliminated; rather, cyber risk must be managed.”

– Director of National Intelligence James R. Clapper
Worldwide Cyber Threats Testimony, Sep. 10, 2015
Cyber Risk is a Dark, Looming Cloud of Uncertainty
There are Many Types of Cyber-Vulnerable Assets

- Corporate IP
- Third-Party Data
- Technology Infrastructure
- Brand & Reputation
- Financial Assets
- Cyber-Exposed Physical Assets
History of Cyber

Exposure and Industry Evolution

Content
- Cyber squatting
- Website defamation
- Viruses
- DDoS
- Privacy
- PII
- PCI
- PHI
- Business Interruption
- Extortion
- IoT
- BI/PD

CMT
- FI
- Retail
- Higher Ed
- Healthcare
- Hospitality
- Power & Utility
- Manufacturing
Current Events in Cyber Risk

- Confidentiality attacks are the most commonly reported (& insured) cyber event
  - Data breaches (usually personal info.)
  - Examples: Target, Anthem, etc.
- Availability & Integrity attacks are rising
  - Business Interruption, Cyber Extortion
  - Targeted or widespread, direct and dependent
  - Examples: Airline groundage’s; Dyn attack; CryptoLocker
- New forms of attack are emerging
  - Doxing (WikiLeaks)
  - Credential Theft (SWIFT attack)

InfoSec Professionals classify attacks into three categories:
- Confidentiality
  - Data Breaches
  - Doxing
- Integrity
  - Data Destruction
  - Data Poisoning
  - Spoofing
- Availability
  - Business Interruption (BI)
  - Dependent BI
  - Data Encryption

The C-I-A Triad
Living with Cyber Risk
A Race Without End

- Cyber Risk is a permanent entry on the enterprise risk register.
- Cyber risk can be managed, but it cannot be eliminated.
- Cyber Risk Management applies classical risk mgmt. to the cyber domain.
- Cyber is technical in nature, but should be managed economically.
- Managing cyber risk engages the entire enterprise, not just IT.

Risk Management Options

Avoidance    Mitigation    Transfer    Acceptance
When It Come to Cyber Risk Management, Everyone Has a Stake
Threats vs. Vulnerabilities

- Threats and Vulnerabilities are related, but very different
  - Threats are the outsider/attacker perspective, Vulnerabilities are the insider/defender perspective
- The Threat environment is limitless
  - Individual attackers have finite resources, and have to choose who to attack
  - But there are so many hackers, the range of potential attacks is essentially limitless
- Vulnerabilities are inevitable
  - In contrast to attackers, defenders have finite resources and constraints
  - Attackers only have to be right once; defenders have to be right every time
- It’s dangerous to ignore Threats
  - People naturally gravitate to a few threats that reflect their experience and fears
  - It’s easier to identify and measure Vulnerabilities, but harder to evaluate Threats, and even harder to link them together
Marsh Cyber Toolkit
Cyber Assessment Methodology

- Almost every firm has gone through an “assessment” of their cyber risk. But what was really assessed?
- Most Cyber “assessments” are technical, and focused on internal controls and associated vulnerabilities.
- Cyber risk is determined by factors beyond the internal control environment.
- Cyber risk is technical in nature, but its effects on business are economic. A true assessment must reflect this.
- Marsh has a suite of analytical tools to help clients assess and analyze their cyber risk.
Quantifying Cyber Risk Impact
Challenges and Strategies

• Quantification is essential for managing cyber risk
  • Communicating risk appetite inside and outside the organization
  • Prioritizing investments in security (technology, people, and processes)
  • Managing the balance between Avoidance, Mitigation, and Transfer
• Quantification also means moving towards objective analysis of threats, risks, and controls
• Quantifying Cyber Risk Impact is uniquely challenging
  • Cyber is a dynamic risk from an active adversary
  • Public data is limited in both scope and quality
  • Common risk factors are non-obvious and not readily observable
# Marsh’s Cyber Risk Management Framework

## A Proven Approach

<table>
<thead>
<tr>
<th>Assess &amp; Analyze</th>
<th>Secure &amp; Insure</th>
<th>Respond &amp; Recover</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understanding your attack scenarios and risk profile is vital to addressing cyber risks. We help you identify assets, quantify the threat environment, assess your controls, and model the potential impact of events.</td>
<td>Managing your cyber risks means preparing your business for the inevitable event. We help you optimize the security controls that protect and detect threats, and transfer exposures off your balance sheet.</td>
<td>Quick, effective response to a cyber event is crucial for your business. We guide and support you through the event, and enhance your protection moving forward.</td>
</tr>
</tbody>
</table>

**Key Concepts:**
- Scenarios must be customized
- Assessment must be objective
- Analysis must be quantified and economic

**Key Concepts:**
- Security & Insurance go hand-in-hand
- Decision making must be coordinated between InfoSec and Risk Management

**Key Concepts:**
- Response is equally important as analysis and prevention
- Experience and expertise are critical to success
Vendors Are a Growing Source of Risk
Marsh Vendor Management Sample

The **Primary Risk** section includes data on your direct vendors’ risk levels and changes in risk levels.

The **Aggregation Risk** section includes data on the commonalities between your vendors based on the use of common service providers.

The **Protocols** section provides step by step recommendations for action based on the results of our analysis.

---

**Primary Risk**

Figure 2-1. Vendor Risk Ratings

**Aggregation Risk**

Table 2-1: Shared Service Provider Matrix

<table>
<thead>
<tr>
<th>Vendor 1</th>
<th>Vendor 2</th>
<th>Vendor 3</th>
<th>Vendor 4</th>
<th>Vendor 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>4</td>
<td>7</td>
<td>12</td>
<td>7</td>
</tr>
<tr>
<td>2</td>
<td>6</td>
<td>8</td>
<td>10</td>
<td>6</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>6</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
<td>5</td>
<td>7</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>5</td>
</tr>
</tbody>
</table>

**Action Protocol**

1. With the relevant business leader(s), review the role of the third party/vendor(s) and its contribution to the business.
2. Review access privileges granted for consistency with business need.
3. Review terms and conditions of service level agreements, including service level agreements, nondisclosure agreements, and other contract instruments regarding cybersecurity obligations.
4. Review available cybersecurity assessments and requirements pertaining to the vendor.
5. Review in your specific technical data (e.g., hosting perimeter protection and firewall configurations).
6. Meet with the vendor to discuss their cybersecurity and learn about their controls and operational metrics that impact.
7. Obtain an independent assessment of the vendor’s cybersecurity posture.
8. Implement additional measures to mitigate risk based on steps 1–7.
9. Incorporate more stringent security requirements on the vendor through contract action and agree on a set of specific remediation activities.
10. Resolicit the vendor’s access to enterprise information resources.
Cyber Insurance Update
Coverage is Broadening

<table>
<thead>
<tr>
<th>CYBER COVERAGE SPECTRUM</th>
<th>CYBER RISKS</th>
</tr>
</thead>
</table>
| BASIC CYBER POLICY ADDRESSES | • Event Management  
|                         | • Data Privacy Breaches  
|                         | • Network Security Liability  
|                         | • Privacy Regulatory Investigations  
|                         | • Cyber Extortion |
| SOME INSURERS ARE SILENT; OTHERS ADDRESS | • Cyber Terrorism (non-physical shutdown) |
| REQUIRES TAILORED CYBER POLICY | • Business Interruption while IT or OT system is down  
|                                  | • OT Security Liability  
|                                  | • Social Engineering (Crime D&O)  
|                                  | • Network Security Regulatory Investigations |
| EITHER P&C, CYBER EXCESS DIC, OR A CYBER GAP EXCLUSION BUY-BACK | • Property damage 1st party  
|                                                                | • Bodily injury / 3rd party property damage  
|                                                                | • Contingent Business Interruption  
|                                                                |   - Patent Infringement  
|                                                                |   - Trade Secret – 1st Party |
Information Security, Privacy Liability & Breach Response: A Risk Management Approach to Preparedness

Steve McElhiney MBA, CPCU, ARE
EWI Re, Inc.
Dallas, TX

smcelhiney@ewirisk.com
Learning Objectives

• By providing a Captive Owner’s perspective, provide session attendees with insights as to how Cyber risks are addressed by an industrial conglomerate (a practitioner’s view).
• To provide additional insights around the evolving nature of Cyber exposures generally.
Contran Controlled Units

- Contran Corp (Private Corporation)
- NL Industries (NYSE & NL)
- Valhi, Inc. (NYSE: VHI) *Holding Co*
- Kronos (NYSE: KRO) *Chemicals*
- CompX (NASDAQ: CIX) *Security Products, Marine*
- Keystone (Private Co) *Steel and Wire*
- Basic Management, Inc. *Utilities and Land Development*
Tall Pines Insurance Company
- Business Model

**Risk into Captive**
- Global Property
- Global Casualty
- Avoid WC
- No third party business (legacy)
- Property/Casualty Opportunistic (Bond Story)

**Reinsurance Overview**
- CAT Modeling/DFA
- Balanced Program (US/UK/Bermuda)
- VT approved RI
- Risk Transfer Analysis
- Strategic Partners EWI Re (UK)

**Reinsurance Process**
- Foreign Risks-locally admitted
- Reinsurance Placement
- Claim recoveries – cash call process
  TPA’s
- Claims In-take
  RSG Claim database
- Forensic accountants (BI –Rita)
Cyber Liability Claims Analysis: The Benefit Of A Post-Loss Review For Pre-Breach Planning

**Pre-Loss Cyber Claim Risk Management**
1. IT SPICE Plan (Scenario Planning to Indemnify Cyber Exposure)
2. Breach Response Escalation Plan
   a. Publicly-Traded Company
   b. Private Company
   c. Not-for-Profit Organization
3. Insurance Purchasing Decision (Cost-of-Risk Trade-Offs)

**Post-Loss Cyber Breach Claim & Litigation Stages**
1. Risk & Loss Assessment – 24 Hours +
2. Damages Assessment –
3. Coverage Assessment Examples
   a. Retail (Target, Neiman. HD)
   b. Healthcare – Anthem, Hollywood Presby
   c. Financial Institutions - JP Morgan Chase

Provides Hypothetical Damage Assessment
Provides Cost of Risk Assessment
Information Security & Privacy Liability Insuring Agreement: Defense expense and compensatory damages for any actual or alleged breach, violation or infringement of any right to privacy, consumer data protection law, or other legal protection for personally identifiable information (including HIPPA & HiTech Acts), including but not limited to breach of a person's right of publicity, false light, intrusion on a person's seclusion, public disclosure of a person's private information, or misappropriation of a person's picture or name for commercial gain.

Computer Information/Network Liability: Negligence claim(s) as a result of a failure to prevent unauthorized access, use or tampering with data or systems, accidental introduction of malicious code in data systems and failure to prevent denial of service attacks or negligent misrepresentation & related IT security failures, & cyber extortion. Breach response expense and Crisis Management expense sub-limits included.

Electronic Multimedia, Advertising Liability & Website Media Content Liability: Libel, slander, defamation, disparagement, invasion of privacy, breach of confidentiality, or public disclosure of private facts including copyright, trademark infringement, cyber squatting violation & others.

Cyber Extortion Coverage (1st Party): A direct or indirect illegal threat from a third-party to damage, destroy or corrupts company website, intranet, network, computer systems, or any programs or data held electronically and/or the dissemination, divulgence, or use of any commercial information for which company is responsible which is not in the public domain and will cause commercial harm if made public – from a third-party who then demands a ransom for their own benefit as a condition of not carrying out this threat.

Information Breach Notification Expense: all reasonable and necessary expenses incurred necessary to comply with the data security breach notification requirements of federal, state or local statute, rule or regulation, or of a judgment, settlement, or other legal obligation. Credit Monitoring Services, Crisis Management & public relations expense, and computer forensic expense included.
Claims & Litigation Stages: Three Areas to Manage

### Phase I
**Post-Breach**
- Risk/Loss Assessment

1. Implement Incident Response Plan
   - a. Key internal personal meeting
2. Engage Outside Vendors
   - a. Outside counsel/Breach Coach Specialist
   - b. Other Outside Vendors
3. Notification (Harm or acquisition trigger by state)
4. Regulatory

### Phase II
**Post-Breach**
- Damages Assessment

1. Analysis of harm to individuals or Corporation (PII, PHI, PCI, IP)
2. Fines & Penalties (AG, Agency, VISA/M-C Breach)
3. Tort & Statutory Liabilities

### Phase III
**Post-Breach**
- Coverage Assessment

1. Traditional Insurance vs Cyber Liability Insurance
2. Claim-Made policy
3. Defense Cost Erosive Policies

---

1. Information Security & Privacy Liability
2. Computer Information & Network Liability
3. Multi-Media & Advertising Liability
4. Cyber Extortion
5. Breach Notification Expense

Breaches by Industry Sector*

- Retail 26%
- Finance & Insurance 20%
- Health Care 15%
- Prof Svcs 8%
- Education 3%
- Hospitality 5%
- Government 7%
- Other 17%

Industrials included

Ref: Data Breach Report 2014, Kamala D. Harris, Attorney General
California Department of Justice, Privacy Enforcement & Protection Division www.oag.ca.gov/privacy
Cyber Liability Risk Categories' & Exposure Matrix
I.T. & e-Business Risk Identification & Assessment

Passive Websites/
I.T. Systems /
Lower Risk Exposure

1. Infringement Risk
2. Defamation Person/Products
3. False Advertising Risk

Interactive Websites/
I.T. Systems /
Moderate Risk Exposure

1. Third-Party Privacy Violations
2. Unauthorized Access
3. Denial of Service Attack
4. Extortion based due to # 2
5. Theft of Intellectual Property
6. Theft of PII & PHI

Active Websites/
I.T. Systems /
Higher Risk Exposure

1. B2B Purchases from Web-site
2. B2C Purchases from Web-site
3. Point-of-Sale (POS)
4. PCI Data Security Standard
5. Compliance & Regulatory Risk
6. Consumer Fraud
7. Repudiation of Access
8. Contractual Liability Exposures
9. Loss of e-Business Income

$ Asset Protection & Preserving Shareholder Value
# Breach Response Escalation Plan – 5 Steps

## Pre-Breach Response Planning
- **Identify Internal Response Team & Incident Lead Person**
- **Establish Analysis & Communication Protocol (The Team)**
- **Complete Data Breach Response Plan**
- **Evaluate Vendor & Customer Notification Requirements**
- **Remediation & Recovery Vendors**
- **Stress Test Response Plan**
- **Fraud Prevention**

## Incident Analysis
- **Contact the Team**
- **Identify Information (PII, PHI, Payment Card compromised)**
- **Breach Containment**
- **Harm Determination Forensic Analysis**
- **Legal Analysis**
- **Security Breach Incident Analysis:**
  - California
  - United States
  - Globally

## Incident Disclosure
- **Analyze Requirements**
- **Consider Alternative Notice Methods**
- **Notify in compliance with laws**
- **Consider third-party vendors for notification**
- **Stagger Notification**
- **Public Reporting**
- **Cyber Insurance Carrier Notification**

## Loss Mitigation
- **Credit Monitoring**
- **Fraud Monitoring**
- **Documentation and discoveries manifest**
- **Customer Service**
- **Human Resources**

## Communication And Remediation
- **External Solutions**
- **Consumer Protection Notification Letter**
- **Customer Hotline Number Established**
- **Breach Website**
- **Senior Management Updates**
- **Human Resource Updates**
- **Cyber Carrier Communications**
- **D&O Carrier Noticed (if material)**
- **Limit Communication**
Conclusion

• Captive Owner’s perspective- how Cyber risks are addressed by an industrial conglomerate
• Evolving nature of Cyber exposures
This presentation contains general information only. CICA and its guest speakers are not, by means of this presentation, rendering insurance, financial, investment, legal, tax or other professional advice or services.

This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Neither CICA nor its guest speakers shall be responsible for any loss sustained by any person who relies on this presentation.