Cyber-Risk Insurance: Understanding Your Exposure and Transferring the Risk

September 29, 2015

Mary Guzman & Jessica Daehler, McGriff Seibels & Williams

WWW.CHICAGOLANDRISKFORUM.ORG
CONTACT DETAILS

Mary Guzman
Senior Vice President, Financial Services Division
McGriff, Seibels & Williams
5605 Glenridge Drive, Suite 500
Atlanta, GA 30342
404-497-7535
mguzman@mcgriff.com

Jessica Daehler
Assistant Vice President, Financial Services Division
McGriff, Seibels & Williams
227 West Monroe Street, Suite 2830
Chicago, IL 60606
847-234-2831
jdaehler@mcgriff.com
TABLE OF CONTENTS

• Data Breach & Privacy Landscape
• Cyber-Risk Is Not Just Privacy Risk Anymore...
• Cyber-Risk Quantification
• Cyber Market Update
• Cyber-Risk Solutions
• Claims & Breach Response
There are two types of companies: those who have been hacked, and those who don’t yet know they have been hacked.

John Chambers, CEO, Cisco
Game changers?

- **Target** - Potentially paves the way for Card Issuers to go directly to “merchants” for reissuance expenses.

- **Anthem** - Anthem agreed to deal with HIPAA/HHS around breach notice/response issues on behalf of all Insured's; however, may be state regulations that trump HIPAA federal statute for plan sponsor; additional fiduciary responsibilities under ERISA may push companies to want to get in front of Anthem’s response time; as a result hundreds of cyber policies have been put on notice.

- **Turkish Pipeline attack, Stuxnet & German steel mill attack**
  - Cyber attacks confirmed to have caused physical damage to infrastructure

- **2014 Sony** - Hack into wide-ranging company data including competitive data and trade secrets. Is this the next evolution of cyber breaches?
REGULATORY ENVIRONMENT

- HIPAA/HITECH
- Card brands
- Various state privacy laws
- FTC
- SEC
- Graham-Leach-Bliley
- NERC CIP
- Various other voluntary assessment tools such as the NIST framework, C2M2, and ISO standards
HISTORICAL BREACHES DATING BACK TO 2013

Source: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
CYBER-RISK IS NOT JUST PRIVACY RISK ANYMORE........
WHICH COMPANIES NEED TO CONSIDER AN INFORMATION SECURITY POLICY?

ALL OF THEM!!!

There are many variations on the risks that are not adequately covered by traditional insurance:

1) Energy Companies
   - Utilities- privacy, business interruption/EE, “failure to supply”
   - Pipelines- business interruption/contingent BI, contractual liability
   - Oil & Gas and E&P – business interruption/EE, **property damage arising out of a cyber event**, 

2) Organizations with a lot of PII or PHI (Financial Institutions, Healthcare, Insurance, Retail, Accounting/Legal, Transportation, Grocery/Drug Stores)
   - Privacy breach response, legal liability to consumers, Card Brands, FIs and other
   - Business Interruption/Extra Expense
   - Reputation Harm (potential link to D&O)

3) Telecommunications/Technology
   - Errors and Omissions liability, Intellectual Property (IP) infringement, first party IP loss (theft, destruction of Trade Secrets)

4) Manufacturing/Distribution
   - Business Interruption/Contingent BI, Breach of Contract, first and third party IP risks

5) Maritime/Port Authority
   - Business Interruption from shutdown, third party Bodily Injury and Property damage, contractual liability

6) Pharmaceutical
   - Intellectual Property / Trade Secret

And the list goes on..................
ENTERPRISE INFORMATION SECURITY RISKS

Enterprise Operation Risk – IT automation throughout organization (applications and networks, etc.)

- Business Interruption loss
  - Income loss from inability to provide services and/or accurately account for sales
  - Extra expenses to
    - Isolate and contain intrusion and conduct forensic analysis
    - Recover and restore compromised digital assets
    - Relicense critical computer applications
    - Other ongoing expenses during period of recovery
  - Extra Expense to utilize Hot Site and/or other back-up resources
- Dependent Business Interruption Risk – cyber disruption at critical supplier or in supply chain
- Legal Liability – failure to meet contractual obligations

Privacy Liability and Regulatory Response

- Incident response costs – notification, credit monitoring, legal fees, forensics
- Privacy litigation – consumer class actions
- Regulatory investigations and remedies (consumer redress funds)
- Third party beneficiary liability – costs to reimburse banks and card companies for their costs to open new accounts or replace cards of victims of your privacy breach
“Traditional” Privacy Liability & Information Security Risks

**First Party Risks and Coverage**
- Business interruption and extra expenses as a result of network or web site outage
- BI/EE for loss of data, recreation of data, uncollectible accounts receivable, corrupted IP
- Cyber extortion – threats to post/sell security vulnerabilities and/or confidential data
- Theft or destruction of Trade Secrets or other IP (Patent and Trade Secret Coverage Excluded under most forms)
- Reputation harm resulting from unusual business churn immediately following an event

**Third Party Risks and Coverage**
- Breach notification and mitigation (credit monitoring) expense, Public Relations, Forensics following the disclosure of Third Party Personally Identifiable Information - most common exposure; most breaches do not result in 3rd party litigation
- A wild card and significant factor driving both cost and limits is the assessment or adjudication process of the Card Brands
- Enterprise wide data privacy wrongful acts whether from internal or external “hacker”, and whether or not records disclosed in electronic or paper format
  - ID theft claims, invasion of privacy claims, damage to reputation/credit
  - Regulatory Defense and investigation, fines and penalties (Red Flags Rule, NERC, HIPAA, others...)
  - Contractual obligations around security and privacy (particularly with regard to PCI compliance)
  - Cost to reissue credit cards (suits from transaction processors or issuing banks)
- Use of your Network to launch an attack or “leapfrog” into third party web sites and/or networks (which may or may not be your clients)
- Media liability, intellectual property infringement (Patent and Trade Secret Excluded under most policy forms)
- Economic harm to your customers due to “down time” of your own application, network, web site upon which your customers rely (Insurance coverage varies by policy form)
THE HIDDEN RISKS OF OUTSOURCING...

- Virtually every company today outsources some component of their IT system to third parties, but most companies have not measured the risks associated therewith. Companies use third parties for everything from web hosting to payroll outsourcing to credit card processing.

- Outsourcing function = Loss of Control, but does NOT release the “data owner” from liability for privacy violations

- FTC Act, Dodd-Frank, Red Flags Rule, PCI Compliance, NERC CIP, HIPAA, and many other state and federal regulations extend to not only you but the vendors you use as well, putting the responsibility for compliance (and the reputation risk) squarely on your shoulders
  - FTC Act gives broad ranging authority around “unfair or deceptive trade practices” regarding use of vendors, enforcement of appropriate privacy and security policies

- Outsourcing can greatly increase your “contingent” business interruption risk

*MSW’s Information Security risk subject matter experts can:*

  - Assist in the categorization of vendors and redevelopment of contract protocols
  - Review insurance for cyber and/or E&O provided by those vendors for adequacy
  - Design custom insurance solutions for you and your vendors
LOSSES FOLLOWING A BREACH

- Breach Notification Costs/Identity Monitoring
- Forensic Investigation Costs / Extra Expense
- Loss/Destruction of Data & Replacement Costs
- Damaged Reputation/Brand: PR costs
- Business Interruption & supply chain disruption / Loss of Profits
- Legal Liability / Litigation Expenses
- Regulatory Liability, Fines and Penalties
- Comprehensive Written Security Program, Audits, System Upgrades
- Drop in stock price/loss of market share
- Potential D&O Suits – Derivative Claims
CYBER-RISK QUANTIFICATION
### PRIVACY LIABILITY & INFORMATION SECURITY CLAIMS: AVERAGE COST PER RECORD

<table>
<thead>
<tr>
<th></th>
<th>Cost Per Record</th>
<th>Financial Impact: 1,000,000 Records</th>
<th>Financial Impact: 3,000,000 Records</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ponemon Institute</strong></td>
<td>$60</td>
<td>$60,000,000</td>
<td>$180,000,000</td>
</tr>
<tr>
<td><em>(Direct Costs Only)</em></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>MSW Clients’ Claim Average</strong></td>
<td>$42</td>
<td>$42,000,000</td>
<td>$126,000,000</td>
</tr>
<tr>
<td><strong>NetDiligence Breach Cost Calculator:</strong></td>
<td>$18</td>
<td>$18,000,000</td>
<td>$54,000,000</td>
</tr>
<tr>
<td>Event Management Expenses</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>BillGuard and 24/7 Wallstreet</strong></td>
<td>$67 (includes $18 of breach response expenses + $48 of fraud expenses)</td>
<td>$67,000,000</td>
<td>$201,000,000</td>
</tr>
</tbody>
</table>

**Note:** We’ve chosen to show the Direct Costs Only estimates from the Ponemon Study because the Ponemon Institute combines Direct & Indirect Costs into a single number; this includes reputation harm after a breach, unusual business churn, and other events which are difficult to quantify and usually not covered by traditional insurance. Direct Costs include costs which are typically insurable, such as forensics; notification costs; providing credit monitoring and ID restoration services; legal expenses; business interruption; extra expense; digital asset restoration; and regulatory investigations or proceedings. Note: The Ponemon Studies only capture data breaches of 100,000 or fewer records and they exclude the mega breaches from the study as outliers, thus the cost per affected person is a much lower number and economies of scale do not apply.

The “MSW Client’s Claim Average” cost per record represents our own client base’s average cost per record on breaches since early 2012. These claims were typically significant events, costing in excess of $100M in total loss per event, and involved substantial PCI Assessments and complex forensic investigations, which has a considerably negative impact on the cost per record.

The NetDiligence Breach Cost Calculator provides a solid baseline of an average cost per record for a breach, but may not accurately reflect the total cost of loss when factoring in a significant PCI Assessment or complex forensic investigation requiring multiple forensic auditors.

BillGuard and 24/7 Wallstreet calculated based on 15% of compromised cards having fraudulent activity on them and an average fraudulent amount of $322 per card.

*There is no perfect science to determining the impact of any given breach as they’re all different. It is also important to understand the cost per record decreases over larger numbers of compromised records.*
TIPS IN ASSESSING INFORMATION SECURITY EXPOSURE

- What sensitive information do you handle, manage, store, destroy or otherwise control – consider your own information, third party information and employee, dependent/beneficiary information
- Identify significant third party vendors providing data and systems management services; review contracts for controls/remedies and retained risk
- Does your organization have a person responsible for privacy compliance, information security officer and/or other executive level oversight of IT/OT security?
- Do you have a formal Incident Response Plan and is the plan been regularly tested and amended?
- Have you pre-negotiated contracts with qualified vendors to assist you in your breach response?
- What kind of indemnities do you provide to clients whose non-public information you transmit, store, process, etc?
TIPS IN ASSESSING INFORMATION SECURITY EXPOSURE

- Have you identified your “critical” systems/applications/data/networks and conducted an information security threat analysis?
- Have you conducted a business impact analysis (e.g. MFL or MPL as a result of an extended period of interruption?)
- What vendors or suppliers are you reliant upon to provision your own products and services?
- What kind of impact would result from a competitor or other third party gaining access to your IP and/or R&D information?
- Are you a party to a Merchant Services Agreement and have you evaluated the financial obligations stipulated therein as respects a breach to credit/debit card data?
- Do you have a PCI DSS compliance obligation (merchant level) and have you been assessed by a QSA for compliance? Have you implemented PCI 3.1?
- Does your organization encrypt sensitive information at rest and in transit? Do you use tokenization, data masking and other techniques/technologies to protect PII?
- How would you rate your company’s security maturity? Have you had an external assessment conducted? Has your organization implemented a national standards framework such as NIST, ISO, SANS, E2-C2M2 or industry specific standard and been independently audited for same?
CYBER MARKET UPDATE
The Worldwide Cyber Insurance Market Is Growing Rapidly

U.S. Cyber Premiums

- “Cyber is a new risk and it is a concern, Lloyd’s is at the heart of cyber attacks, providing coverage right now. It’s going to grow dramatically”
  - Inga Beale, CEO, Lloyd’s of London, Oct. 2014
- “Cyber Insurance: Maybe next year turns into I need it now”
  - Betterley Report, June 2014
- “Before, we were selling 1.2 policies for every 10 inquiries; since recent hackings it is 4.2 for every 10 inquiries.”

Betterley Report on Cyber/Privacy Insurance market

- Some carriers reporting loss ratios in the 400% or higher range resulting in massive market correction
• Total liability capacity nears $800 million with $500 million being largest single program (usually blended with E&O, Bankers Professional or other line); less capacity available for BI/EE and many towers thin out as follow form capacity not available for all insuring agreements or exposures (intellectual property, etc.)

• The cyber market is experiencing an intense hardening, primarily in the retail / hospitality space. The market impact felt as a result of the string of breaches since December 2013, led by Target & Home Depot, has led to more cumbersome underwriting requirements and tightening capacity

• End-to-End encryption is now required for many retailers; some markets insist on a signed warranty affirming that all systems have been tested/scrubbed for BlackPOS or any similar malware; some underwriters expecting P2PE plan in addition to EMV implementation.

• Approach from Insurers varies significantly as respects sub-limits on notification, credit monitoring, forensics, fines/penalties and business interruption coverage. Some excess carriers retreating from certain industries or limiting capacity on retail risks.

• Some insurers require that their claims/response team must manage breach response on behalf of the Insured; some provide more flexibility (McGriff clients often prefer to manage their own breach response)
CYBER-RISK SOLUTIONS
### CYBER POLICY COVERAGE COMPONENTS

<table>
<thead>
<tr>
<th>Coverage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Income / Extra Expense</td>
<td>Reimbursement for loss of income and/or extra expense resulting from an interruption or suspension of computer systems due to a network security breach.</td>
</tr>
<tr>
<td>Data Asset Protection</td>
<td>Recovery of costs and expenses you incur to restore, recreate, or recollect your data and other intangible assets that are corrupted or destroyed by a computer attack.</td>
</tr>
<tr>
<td>Cyber Extortion</td>
<td>The costs of consultants and extortion monies for threats related to interrupting systems and releasing private information.</td>
</tr>
<tr>
<td>Breach Response</td>
<td>The costs of complying with the various breach notification laws and regulations, legal expenses, call centers, credit monitoring, forensic services, identity /fraud monitoring, and public relations.</td>
</tr>
<tr>
<td>Privacy Liability</td>
<td>Defense and liability for the failure to prevent unauthorized access, disclosure or collection of confidential information, or for the failure of others to whom you have entrusted such information. Coverage can also include liability for not properly notifying of a privacy breach and includes corporate proprietary information.</td>
</tr>
<tr>
<td>Network Security Liability</td>
<td>Defense and liability for the failure of system security to prevent or mitigate a computer attack. This could include a malicious virus or a denial or service attack. This coverage also includes the failure of written policies and procedures addressing technology use.</td>
</tr>
<tr>
<td>Privacy Regulatory Defense</td>
<td>Costs to defend an action or investigation by regulator due to a privacy breach, including indemnification for any fines or penalties assessed.</td>
</tr>
<tr>
<td>Media Liability</td>
<td>Defense and liability for online libel, slander, misappropriation of name or likeness, plagiarism, copyright infringement, disparagement, negligence in content to those that relied on content.</td>
</tr>
</tbody>
</table>
MSW CYBER-RISK SOLUTIONS

• SME Cyber Program
  – For companies with revenues < $250m

• Cyber-Suite Gold
  – Fortune 1000 / Revenues > $1B

• MSW Proprietary All-Cyber Risk form
  – Full 1st and 3rd, no sublimits, few exclusions
  – Best in Class

• Critical Asset Protection Cyber-Risk form
  – Comprehensive Cyber Risk Management & Risk Transfer solution
BREACH RESPONSE STEPS

STEPS

☑ Activate panel counsel and breach response resource team
☑ Re-establish the key personnel with authority to act on behalf of company
☑ Gather intel on breach (forensics, etc...)
☑ Map out potential breach response costs and method for loss cost data capture
☑ Formulate/execute regulatory response plan and draft notice details/timeline
☑ Keep Board apprised of breach details and response strategy
☑ Prepare/provide notice (include goodwill notification)
☑ Simultaneously prepare for secondary or layered attacks
☑ Manage the press (Brian Krebbs) as well as how to manage communications internally with employees; consider use of and/or response to social media traffic
☑ Coordinate with law enforcement (utilize their resources/but do not rely on)
☑ Document event management and use in future training and to shore up deficiencies in response plan
IDENTIFYING KEY BREACH RESPONSE PARTNERS

- Legal
- Forensic (2 may be necessary...)
- Notification
- Credit Monitoring
- Call Center
- Public Relations
APPENDIX
NOTABLE BREACHES

Target 2013 Breach
- Records Disclosed: 110,000,000
- Customer Class Actions: $10,000,000 settlement
- Card Brand Litigation: $19 million settlement with MasterCard (rejected); $67 million settlement pending approval by participating Banks
- Bank Litigation: Target bid to dismiss rejected by judge; case ongoing.
- Expenses paid to date: $256m (1Q2015)

Anthem 2015 Breach
- Records Disclosed: 80,000,000
- Cyber attackers (suspected Chinese) gained access to Anthem customer and employee PII/PHI
- Names, birthdays, social security numbers, street addresses, email addresses, employment information, income data
- FBI, State’s Attorney’s investigations
- 50+ class action lawsuits filed to date, no settlements yet
OPM (US Government) 2015 Breach
- Records Disclosed: 40,000,000 (and counting...)
- Systems breached in December 2014, but OPM became aware April 2015
- SS#s, full names, fingerprints, birth dates, home addresses, background investigation records current, former and prospective Federal employees and contractors, contain information about mental health and financial history
- Information of non-applicants, primarily references, spouses or co-habitants of applicants
- $133m paid for Breach Notification & Identity Theft Protection Services

Sony Pictures 2014 (Breach #2)
- Perpetrators hacked into wide-ranging company data held including:
  - Unreleased movie scripts
  - Trade Secrets
  - Compensation of Executives & Actors
  - Personal emails
  - Employee SS#, compensation, address, health check records
- Suspected nation-state perpetrator or possible disgruntled employee?
- Forensics, IT Repairs, Loss of Data, Loss of Movie Profits, PR expenses, Employee Litigation, Loss of Competitive Advantage, Lost jobs