McGRIFF, SEIBELS & WILLIAMS, INC.

AAPA Finance Seminar – New Orleans

Cyber Risk – Liability & Property

April 2014

AGENDA

I. Cyber Risk Insurance – What is it??

II. How does a breach happen?

III. The Numbers

IV. Claims Examples

V. Types of Coverage

VI. Insurance Coverage Examples

VII. Critical Asset Program (CAP) Design & Features

VIII. Emerging Trends – Related Risk

IX. Questions

Cyber Risk Insurance – What is it?

- Traditional liability and property insurance products have not kept pace with the development of Cyber Risk Exposures, so specialty insurers have responded with insurance products called Cyber Risk Insurance. These Cyber Risk Insurance policies vary, but typically are a package of coverages incorporating both first party and third party coverage parts. Not only is the Cyber Risk insurance segment new, it is rapidly changing. Coverage terms, underwriting criteria and pricing are changing at a fast pace.

- Cyber Risk Insurance is designed to provide protection from exposures arising from confidential data and the use of technology. Part of the risk arises from confidential data in both electronic and paper form, such as the personal information of customers and employees. Additional protection is provided for damage to or destruction of data or systems from virus or hacking, or for theft of private information or money.

- The obvious and primary exposure is data breach, an unintended loss, release or theft of data, and Cyber Risk Insurance policies are designed to cover some level of direct costs associated with a breach, plus legal expenses and settlements if a lawsuit ensues. Other covered exposures are liability from data breaches, regulatory costs and penalties, media liability, damage or destruction of corporate data and systems, and theft of money. However, coverage forms are not consistent among insurers, and not all policies provide the same coverage.

Cyber Risk Insurance– What is it?

- Some customers may think that their Cyber Risk exposures are covered within their CGL. Cyber Risk coverage is not typically provided in standard policies. In some cases Cyber Risk coverage is added as an endorsement to standard policies, but typically the limit is not adequate and the coverage is not as comprehensive as a standalone policy. Cyber Risk Insurance coverage needs go much further than what may be included within a CGL and typically include both first and third party Cyber Risk coverages.

- Many people confuse cyber liability insurance and technology professional liability insurance.

- Technology professional liability: Technology professionals comprise organizations that develop and implement technology for both consumers and businesses. For example, a technology professional could be a software developer, a microchip designer or an IT consultant. Technology professional liability is designed to cover specifically the errors & omissions of these types of organizations.

How does a breach happen?

- Lost or stolen laptops often containing protected information for numerous individuals
- Theft – internal & external
- Inadequate destruction of data
- Lost back up storage devices
- Stolen computer servers
- Hacking/Phishing
- Denial of Service
- Cyber Extortion
- Cloud Computing

The Numbers - Costs Associated With A Breach

- Data indicates that in less than two years unsecured protected information data breach has impacted over 20 million people.
- Estimates of the costs associated with breach response following a stolen laptop can be as high as $258 per record.
- $130.1 billion cost to businesses
- 40 new malicious programs per minute
- 14 victims worldwide every second
- Third party liabilities from suits by individuals impacted by the breach
- Estimates in excess of $250 to notify each individual
- Loss of reputations and public confidence
- Taxing of internal resources in information technology, legal, public relations and other support departments

Claims Examples

Employee Error

- An employee misplaced a client file somewhere between the office and an off-site meeting. The file contained customer names, addresses, social security numbers and bank account information. The company must notify the affected individuals and pay for credit monitoring; identity theft cannot be ruled out.
- An employee lost a laptop while traveling. The laptop contained names, addresses, birth dates and social security numbers for company employees. The company paid for one year of credit report monitoring to affected employees to mitigate future issues.
- A woman looking for coupons in a large recycling bin found records containing social security numbers and medical histories. The papers came from a local medical office, and included details about more than 60 patients, including drugs they were taking, and whether they were seeing psychiatrists. The papers were tossed in a recycle bin by an employee with an otherwise long and stellar service record. The incident constituted a breach of HIPAA and resulted in governmental fines against the medical office.
- An employee of a private high school mistakenly distributed via e-mail the names, social security numbers, birthdates and medical information of students and faculty, creating a privacy breach. Overall, 1,250 individuals' information was compromised.
- A non-profit community action corporation printed two 1099 forms on one piece of paper. An employee was supposed to separate the forms and send each to its rightful owner; but instead, the forms were sent as-is. The mistake sent tax forms and social security numbers to unintended recipients: approximately 50% of the landlords who work with the community action corporation received their forms along with the private information of the others.

Claims Examples

Malicious or Criminal Activity

- An international computer hacking group gained access electronically to the computerized cash registers of a restaurant chain and stole credit card information of 5,000 customers, starting a flood of fraudulent purchases around the world.
- A business is hacked by a local teenager who steals social security numbers and bank account details from customer files. He sells the information to an Internet website, which uses the information to create false identities for criminals to use. The business incurs notification and credit monitoring expenses; and the legal expenses and damages from potential lawsuits could easily bring total costs into the hundreds of thousands of dollars.
- An auto dealership was the target of identity thieves when 2 men broke into the dealership after hours, stealing files containing financial information for customer transactions, including credit reports, bank statements and social security numbers. The thieves were eventually apprehended, but not before making illegal purchases with stolen identities of dealership customers.
- A regional retailer contracted with a third party service provider. A burglar stole two laptops of the service provider containing the data of over 800,000 clients of the retailer. Under applicable notification laws, the retailer – not the service provider – was required to notify affected individuals. Total expenses incurred for notification and crisis management to customers was nearly $5,000,000.
- An employee learns that she may be terminated and in response steals names, addresses, social security numbers and other personal information from customer files. She sold them to her cousin, who used the identities to fraudulently obtain credit cards. The affected individuals filed suit against company for identity theft.
- A U.S. based information technology company contracted with an overseas software vendor. The contracted vendor left certain "administrator" defaults on the company's server and a "Hacker for Hire" was paid $20,000 to exploit the vulnerability. The hacker demanded an extortion payment otherwise he would post the records of millions of registered users on a blog available for all to see. The extortion expenses and extortion monies are expected to exceed $2,000,000.

Claims Examples

Non-Breach Claims

- A financial firm fell victim to criminals using the Zeus virus, and lost a significant sum of money from one of its bank accounts. Hackers used the virus to steal the company's online banking access information, and wired funds out of its bank account to a foreign bank account. The money has not been recovered.
- A virus is introduced, and shuts down an order processing systems causing damages to the insured company and its customers, resulting in both first and third party claims.
- Data residing with a third party vendor is lost and no external backup is available. The data can be replicated, but the cost to replace the data is significant.

Cyber Risk & Insurance Agents E&O

- According to reports, back-up tapes with 1.7 million patient records from medical providers affiliated with a state university medical center were stolen from a service provider's employee's car. The university incurred more than $3.0 million in costs associated with the breach, and litigation has ensued between the university, the service provider, and the service provider's insurer. **It appears that no Cyber Risk Insurance was in place, and the insurance agent has been brought into the litigation for failing to provide Cyber Risk Insurance.**

Cyber Risk – Types of Coverage

- **First-party (property) insurance**

  First-party cyber property coverage is to cover the material cost of a breach including crisis management, business interruption expenses, computer restoration expenses, etc.

- **Third-party liability insurance**

  Lawsuits which allege that a data holder breached its duty to properly protect the private information (including health information) of a customer, client, or patient are becoming more common. Although the history of cyber lawsuits has not yet fully evolved, it is clear the public has lost patience with the almost constant barrage of data breaches. Courts are becoming more friendly to plaintiffs, and the time is coming when defendants can expect large judgments against them.

  Cyber loss exposures are not restricted to data residing within an organization. Data that an insured is required to protect may reside with others, such as with information technology consultants, web hosts, and data storage vendors. The growth of "cloud" computing means that data is housed outside an organization with more frequency than ever before. While properly drafted contracts and insurance requirements can help reduce the risk for the owner of the data, cloud computing contracts are notoriously difficult to alter, and almost always favor the vendor.

  Cyber Liability coverage is almost always written on a claims-made basis, with defense costs included within the policy limits.

Cyber Risk – Types of Coverage

- **Fines and penalties**

  Cyber policies can cover the cost of investigating and defending data breach investigations that are brought by governmental regulators. They can also cover fines, penalties, and forensic investigations levied by the payment card industry.

  Governmental fines coverage generally includes civil monetary fines and penalties as well as payments to consumer redress funds. Many cyber policies contain an exclusion of fines and penalties not insurable by law, but "most favored venue" wording is often added to limit its effect.

  A lesser-known type of fines and penalties coverage can be obtained for the obligations a credit card merchant has under its agreement with credit card issuers, such as MasterCard, Visa, and American Express. Card issuers are entitled to fine a merchant for security breaches and may require a costly forensic investigation of the merchant's security protections before resuming acceptance of purchases made on their cards from that merchant.

Cyber Risk – Types of Coverage

- **Data breach response costs**

  Although breach response coverage was conceived as an ancillary coverage, it has become the most valued cyber coverage. As businesses and other organizations learn of the frequency and cost of data breaches, they realize that the exposure is significant in terms of cost, and imminent in terms of likelihood. Most cyber policies cover the following breach response expenses:

  - Forensic costs to examine the factors that led to the breach
  - Costs to secure the site of the breach
  - Costs to notify persons whose private information may have been breached
  - Credit monitoring and call-center services for those persons
  - Crisis management services (provided by law firms, public relations firm, breach response firms, and others) related to the breach, including costs to understand, evaluate, respond to, and communicate with regulators and the public

  With the reporting breach costs of $250 and more per person affected, these costs quickly add up. Many organizations have "personally identifiable information" (PII) and "personal health information" (PHI) on tens of thousands or more individuals. Although small businesses collect less of this information, the cost of notifying even 500 individuals could impact the financial stability of many of these firms.

Cyber Risk – Types of Coverage

- **Value-added risk management services**

  Insurers offering cyber policies recognize that there are value-added risk management services that can help an insured avoid—or at least mitigate—data loss. Providing these services also is a good way to strengthen the bond between insurer and insured, and to give the insurance agent or broker additional benefits to offer the insured.

  The value-added risk management services are provided by third-party vendors selected by the insurer. They are generally provided at no additional cost, and use of the services is voluntary. The following services are commonly included:

  - Information portals—such as the eRisk Hub provided by NetDiligence, which includes reference material, news updates, and other information and tools that may be helpful in avoiding a breach
  - Breach incident response plan templates
  - Written information security plan (WISP) templates
  - Network penetration testing
  - White papers
  - Educational webinars put on by the insurer
  - Access to data breach experts, which is comparable to free consultations with employment attorneys in the employment practices insurance product line, is less commonly available. However, the availability of this service is expected to increase in the near future.

Insurance Coverage Example

Cyber insurance is not “standard”. Companies will all have their own version and I expect ISO will come out with one in the near future. Below is an example of one:

Travelers CyberRisk coverage is offered as a stand-alone policy or as a cohesive part of their management liability suites of coverages. CyberRisk provides a combination of coverage options to help protect your client from emerging cyber threats and includes access an information portal of risk management tools.

First-party insuring agreements cover such things as the material costs of a breach, including forensic analysis, fees to determine the nature and extent of the breach as well as notification costs that are legally mandated in 46 states and include:

- Crisis management event expense
- Security breach remediation and notification expense
- Computer program and electronic data restoration expenses
- Business interruption and additional expenses

Liability insuring agreements cover costs associated with the liability of a claim or suit related to a breach and include:

- Network and information security liability
- Communications and media liability
- Regulatory defense expenses,

CRITICAL ASSET PROTECTION (CAP): PROGRAM DESIGN & FEATURES

- A collaboration with leading cyber risk specialists, combining risk transfer with risk management solutions under one comprehensive program
- Eligible clients: any critical infrastructure entity
- $100 million line slip backed by leading cyber insurance markets from UK, US and Europe
- Applicants contract with top tier holistic enterprise security firm, Tailored Solutions and Consulting (TSC) for in-depth cyber risk assessment, the cost of which is credited against bound premium. Value of the assessment is $75,000+. TSC staff have top level government security clearances and own/manage the secure portal which will house the confidential report (accessible only by Insured's designees)
- Upon binding, the Insured entity is provided with up to $40,000 in risk management budget to enhance security measures, further harden digital asset protections and/or to refine breach response plans
- Provides access to leading privacy and energy law firms for security/privacy breach and litigation representation at reduced rates, with Insured retaining option to pre-select its own counsel
- Provides access to leading cyber/information security breach response and mitigation vendors

CAP INSURANCE COVERAGE FEATURES

FIRST PARTY

- Full limits for all privacy and security breach response costs (including forensics)
- Coverage for hacking events plus “operational or administrative error”
- Optional coverage available (with additional underwriting)
  - Dependent Business Income loss
  - Insured’s cost to purchase replacement power from spot market
  - Trade Secret coverage
- Network Asset Protection
  - Loss of digital assets
  - Interruption and Extra Expense (non-physical damage)
- Cyber Extortion

THIRD PARTY

- Privacy regulatory defense and penalties (with affirmative coverage for fines, penalties, including industry fines (PCI) and regulatory fines, and more importantly, for “assessments” as levied by Card Brands resulting from a breach)
- Affirmative coverage for third party failure to supply which results in business interruption to a third party or breach of contract
- Media Liability

FEATURES IN FULL FORM

- Cyber terrorism
- Accommodation for matters in scope under Executive Order 13636
- Defined policy terms for SCADA, EMS and critical infrastructure to clarify program intent
- Two year prior acts
- Fewer program exclusions and/or broadened language through coverage carve-backs, including:
  - Breach of contract (important for PCI compliance, PPA agreements and other obligations)
  - Punitive damages
  - Unfair/deceptive trade practices
  - Infrastructure under Insured’s control

EMERGING TREND- PROPERTY DAMAGE RESULTING FROM CYBER ATTACK

- Property markets attaching exclusionary language for cyber events similar to CL 380 Exclusion, though most with carve-backs for resulting/ensuing explosion, fire, and mechanical breakdown
- Terrorism (PV) markets beginning to put absolute cyber exclusions on stand-alone placements
- Certain subsector in E&P and upstream already have full exclusion

CL380 Exclusion: Cyber Attack Exclusion

1.1 Subject only to Clause 1.2 below, in no case shall this Policy cover loss damage liability or expense directly or indirectly caused by or contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system.

1.2 Where this clause is endorsed on policies covering risks of war, civil war, revolution, rebellion, insurrection, or civil strife arising therefrom, or any hostile act by or against a belligerent power, or terrorism or any person acting from a political motive, Clause 1.1 shall not operate to exclude losses (which would otherwise be covered) arising from the use of any computer, computer system or computer software programme or any other electronic system in the launch and/or guidance system and/or firing mechanism of any weapon or missile.

- MSW collaborating with leading Terrorism and Cyber markets to craft custom solution for physical damage to tangible property resulting from cyber event

McGRIFF, SEIBELS & WILLIAMS, INC.

Questions?

Cindi Heffernan, CPCU
cheffernan@mcgriff.com
206-669-6289