Major Challenges to the Insurance Marketplace in 2016


2) Risk Aggregation

3) Limited Capacity

4) Limited Ability To Cover All Corporate Assets.

5) Actuarial Data – How To Price Risk.
Cyber Insurance Marketplace

Major Focus on Data Privacy

No coverage/policy uniformity in the marketplace

Total capacity between the USA and London remains at approximately $500,000,000 and total gross premium is $5 billion.
Cyber Insurance Marketplace

Indemnity

1. Reimbursement policies allow the insured to hire vendors (with consent from the carrier)
2. Will vary by carrier and include outside counsel, IT forensics and public relations experts.
3. Breach Response expenses are sometimes subject to a sub-limit and will erode the policy aggregate limit

Vendor Panels

1. Automatic vendors provided by carriers – established breach panels
2. Some carriers offer notification costs outside of the aggregate limit
3. Some carriers offer notification costs per affected individual rather than monetary sublimits.
Aggregation refers to the consequences of concentrated and cascading cyber risks where key aggregation attributes such as internet failure, compromised service providers, or a number of companies in the same (or different) sectors using the same IT system where something happens to that system and affects all of the companies in that industry.

As cloud computing becomes more ubiquitous, one successful attack or the failure of a cloud host could cause losses to thousands of parties who hold their data within the cloud.
A Lack of Actuarial Data

- A lack of sufficient metrics with respect to frequency and severity of loss, not just to PII, PHI and IP, but also to physical assets as a result of cyber events makes pricing risk a challenge.

- The evolving nature of the threat (DDoS, APT, Ransomware) and the environment (virtualization, the Internet of Things, and the Cloud), compounds the problem of developing accurate actuarial data.

- Fundamentally, insurers look for a strong security culture within the company as a first step in risk triage. Additional factors such as industry, revenue size, geography, and actual assets at risk contribute to how risk is priced.
Technology and Insurance Converge

- A number of technology product and service companies are joining the market to try to support the risk assessment process for cyber insurance.

- Insurers and brokers are starting to invest in predictive analytics capability based on both internal and external data.

- Ability to price risk more accurately will accelerate the growth in market capacity.
The Future of Cyber Insurance?

- Will continuous monitoring and risk scoring will be the new norm? This is the process of maintaining real time awareness of security threats and vulnerabilities that support organizational risk management decisions?

- Will premium and rates vary on a monthly, weekly, daily, or even hourly basis predicated on dynamic threat and vulnerability environment?

- Underwriters will continue to establish new relationships with security product vendors.
The Public Policy Debate – The Driver

Market Incentives versus Regulation

- Legislators are giving greater prominence to the role of cyber insurance. The failure to drive stronger enterprise security has demonstrated the challenges in trying to enforce minimum standards. There is growing support for market-based incentives such as insurance that can reward strong Cybersecurity through discounted premium or broader coverage.
What Does Cyber Insurance Cover?

Insurers do not address all enterprise assets at risk. The majority of premium spent by buyers was intended to address increasing liability from handling personally identifiable information (PII) or protected health information (PHI) and the costs from either unauthorized disclosure (a data breach) or a violation of the data subject’s privacy. Insurable costs range from data breach response expenses such as notification, forensics, and credit monitoring to defense costs, civil fines, and damages from a privacy regulatory action or civil litigation. Insurers also continue to address certain first party risks, including the impact on revenue from attacks on corporate networks, extortion demands, and the costs to restore compromised data.
What Does Cyber Insurance Cover?

- Insurable assets:
  - Personally identifiable information and/or protected health information of employees or consumers
  - Corporate Confidential Information

- Data breach response costs to include the following:
  - Notification
  - Credit monitoring
  - IT forensics
  - Public relations

- Defense costs and civil fines from a privacy regulatory action
- Defense costs and damages from civil litigation
What Does Cyber Insurance Cover?

- Corporate information technology network:

Addresses the loss of income as a consequence of network downtime. Certain insurers will also extend coverage to downtime of vendors on whom a policyholder is reliant. This is commonly known as “contingent business interruption.”

Costs to restore compromised data

Reimbursement for costs associated with an extortion threat
What Does Cyber Insurance Cover?

- Reputation and Brand

Insuring reputational risk from some form of cyber event remains out of the scope of the majority of insurers. At the time of writing, the London market has begun to innovate to address the financial loss after adverse media publicity. However, capacity remains constrained at $100,000,000 at best.
What Does Cyber Insurance Cover?

- Physical Assets

Cybersecurity is no longer just about risks to information assets. A cyber attack can now cause property damage that also could lead to financial loss from business interruption as well as liability from bodily injury or pollution, for example. Understanding where coverage lies in a corporate insurance policy portfolio is challenging and, at times, ambiguous. An assumption that coverage should rest within a property or terrorism policy may not be accurate. Exclusionary language has begun to emerge and is expected to accelerate across the marketplace as losses occur. Dedicated products also have started to appear.
## Comprehensive Insurance Solution

### Network Security Liability
- Claim expenses and damages arising from network and non-network security breaches

### Multi-Media Liability
- Claim expenses and damages arising from personal injury torts and intellectual property infringement (except patent infringement)
- Claim expenses and damages arising from electronic publishing (website) and other dissemination of matter

### Privacy Liability
- Claim expenses and damages emanating from a violation of a privacy law or regulation
- Common law invasion of privacy or infringement of privacy rights

### Privacy Regulatory Proceedings + Fines
- Claim expenses in connection with a regulatory inquiry, investigation or proceeding
- Privacy regulation civil fines and consumer redress fund
- PCI DSS fines and assessments

### Technology E&O/Miscellaneous E&O
- Claim expenses and damages emanating from a wrongful act in the performance of or failure to perform technology services or other professional services.
- Claim expenses and damages emanating from your technology products’ failure to perform or serve the purpose intended

### Data Breach Expense Reimbursement
- Expense reimbursement for third-party reasonable and necessary costs including:
  - Public relations costs
  - Legal and forensics expenses
  - Credit protection, mailing and tracking, call center, etc.
- Address 3 scenarios – mandatory, contractual and voluntary

### Cyber Extortion
- Reasonable and necessary expenses and any funds paid in connection with an extortion attempt

### Network Business Interruption + Data Restoration and Reputation Harm
- Loss of net income and Extra Expense
What Does Cyber Insurance Not Cover?

- Intellectual property assets

- Theft of one’s own corporate intellectual property (IP) still remains uninsurable today as insurers struggle to understand its intrinsic loss value once compromised. The increasing difficulty in simply detecting an attack and, unlike a breach of PII or PHI, the frequent lack of a legal obligation to disclose, suggest that a solution is not in the immediate future.
What Does Cyber Insurance Not Cover?

- **INSTITUTE CYBER ATTACK EXCLUSION CLAUSE - CL380**

  1.1 Subject only to clause 1.2 below, in no case shall this insurance 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 program, 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 program or any other electronic system in the launch and/or guidance system and/or firing mechanism of any weapon or missile.
Our Mission

To be the worldwide value and service leader in insurance brokerage, employee benefits, and risk management

Our Goal

To be the best place to do business and to work

www.lockton.com