Cyber: The Continuing Evolution of Risk

Jeremy Ong
Divisional Vice President
Great American Insurance Group

Categories of Cyber Attacks: C.H.E.W.

C ybercrime - Financially motivated

- **Theft of money**
- **Ransomware**
- **Distributed denial of service attack (DDoS)**
- **Theft of identity**

H activism- Not money motivated but more ideology driven. Meant to force certain actions or to simply punish the victim organization.

E spionage- Spying to obtain political or financial advantage. Corporate trade secrets /intellectual property, sensitive information, etc.

W ar - Nation states attacking critical infrastructure (utilities) or military /government targets of another nation.

Data Breach Trends:

The 79,790 security incidents studied are attributed to the following:

- Miscellaneous Errors: 29.4%
- Crimeware: 25.1%
- Insider /Misuse: 20.6%
- Physical Theft: 15.3%
- Web App Attacks : 4.1%
- Denial of Service: 3.9%
- Cyber Espionage : 0.8%
- Point of Sale Intrusions: 0.7%
- Payment Card Skimmers: 0.1%

Estimated Cost of a Breach

# of Records	Expected Cost	Average Cost
100	$25,450	$35,730
1,000	$67,480	$87,140
10,000	$178,960	$223,400
100,000	$474,600	$614,600
1,000,000	$1,258,670	$1,775,350
10,000,000	$3,338,020	$5,241,300
100,000,000	$8,852,540	$15,622,700

Cyber Insurance Marketplace

- Estimated US cyber premiums at $2.5 Billion in 2015. (Source: Advisen)
- Increasingly competitive. More educated and motivated buyers.
- More standardization of coverage amongst competitors.
- Cyber Insurance is typically offered on a standalone policy or as an endorsement to a Commercial Package or D&O /E&O policy.
- Constantly changing cyber trends make it challenging for carriers from the standpoint of product development, risk / trends analysis, and pricing.

Cyber Insurance Marketplace

- Rise in contractual requirements for cyber insurance which also resulted in more motivated buyers.
- Breach related services are part of the insurance offering.
- Increasing attempts to treat cyber insurance as a commodity product even though it is still an emerging coverage line.
- Evolving cyber insurance forms. It is really a package policy or a “melting pot” of insurance coverage.

Typical Cyber Policy Offering in the Marketplace

1. **Liability Coverages** (Claims- Made) **:**

- Electronic Media or Full Media Liability (online and offline)
- Security Breach Liability & Expenses

2. **First party Coverages :**

- Damage to Electronic Data
- Business Income/Extra Expense
- Public Relations Expense

3. **Crime :**

- Cyber Extortion
- Computer Fraud /Funds Transfer Fraud
- Social Engineering Fraud

Typical Cyber Policy Offering in the Marketplace

4. Fines / Penalties:

- Fines/Penalties/Defense costs from a regulatory proceeding
- PCI (Payment Card Industry) Fines

5. Breach Remediation Services

- Breach Consultation
- Online portal access
- Risk management tools

Underwriting :

Underwriting:

- Continuous learning. Being current on cyber trends.
- Reviewing contracts and understanding the transfer of risk.
- Understanding the applicable state breach law requirements.
- Coverage analysis. What is included or excluded ?
- Determining aggregation risk.
- Website /Social Media review.
- Evaluating the internal controls of a client based on data security assessment reports.
- Establishing limits and deductible adequacy.

Pricing : Moving Target

Pricing:

- Rating basis is typically based on revenue .
- Pricing will range based on key underwriting information such as:
  - Type of personal Identifiable information / number of records
  - Internal controls (ie. Security)
  - Volume of time sensitive transactions
  - Industry sector
  - Website /social media content.
  - Risk transfers (contractual)
  - Current cyber trends

Questions