Cyber Insurance

CAS Seminar on Reinsurance
Southampton Princess
June 6th, 2013

Andrew Lea
Senior Vice President & Commercial E&O PLM
AIG Cat Excess Liability

Agenda

- Coverage
- Types of Insureds
- Losses

AIG

Coverage

AIG

Third Party Liability (and E&O)

- Network Security Liability
  - Liability arising out of an insured's failure of computer security.
    - Transmission of virus, denial of service, unauthorized access
    - Release of confidential information
- Privacy Liability
  - Loss of PII (personally identifiable information) or confidential information such not related to a security failure, such as lost backup tapes or missing hard drives.
- Regulatory Proceedings (usually a sublimit)
  - Coverage for defense of any resulting liability, including insurable fines and penalties arising out of regulatory actions.
- Media Liability
  - Liable, slander, defamation, copyright or trademark infringement.
- Professional Liability/Errors & Omissions
  - Cyber Coverage is often included within a professional liability. Common with Tech & Software.

AIG

First Party Coverage

- Breach Event Expenses
  - Notification Costs – 46 states have cyber breach notification laws on the books.
  - Forensic Costs
  - Credit Monitoring
- Network Business Interruption
  - Lost income and extra expense when a network is down as a result of network security failure.
- Digital Asset Protection
  - Costs related to restoring or recreating lost data resulting from a security failure.
- Cyber Extortion
  - Costs related to responding to an extortion event.

AIG

Security & Privacy

- Security & Privacy Insurance responds to important third party liability for claims arising from:
  - A failure of the insured's network security
  - A failure to protect personally identifiable information including disclosures as a result of social engineering attacks (e.g., phishing)
  - Violation of any federal, state or local privacy statute alleged in connection with failure to protect confidential information
- Duty-to-Defend coverage
- Broad definition of "confidential information" and "computer system"
- Coverage extends to information held by "Information Holders"
- Endorsement available for regulatory fines/penalties and PCI assessments

AIG

Cyber Extortion & Network Interruption

- Cyber Extortion Insurance pays to settle network security related extortion demands made against the insured.
  - Triggers when there is a threat to commit a computer attack against the insured and a demand for money to terminate the threat
  - Includes the costs of investigations to determine the cause of the security threat and to settle the extortion demand
- Network Business Interruption Insurance responds to an insured's loss of income and operating expenses when business operations are interrupted or suspended due to a failure of network security
  - Broad definition of loss includes lost business income, normal operation expenses (including — payroll) and those costs that would not have been incurred but for the interruption
  - System Failure can be added by endorsement
  - Limited coverage for outsource provider - $100,000
  - Waiting hour period applies

AIG

Event Management

- Responds to the costs to retain services to assist in managing and mitigating a covered privacy or network security incident
  - Includes costs to notify consumers of a release of private information
  - Costs of credit-monitoring or other remediation services to help minimize damages. Credit monitoring not limited to 12 months
  - Forensic Investigation Coverage
  - Public Relations/Legal Assistance Expense Coverage
  - Call Center Services
- Goodwill notification – not limited to state notification or legal requirements
- Can be offered on a Monetary (Insured uses own vendors) or Number of Affected Persons (Insurer handles) basis
- Includes costs associated with losses to information assets such as customer databases

AIG

Reputational Risk

- Whether accidental or malicious, data breaches can spell disaster for an organization's reputation
- Diverse state notification requirements may require an organization to disclose detailed information about a data breach, no matter the size or scope
- In today's digital age, both traditional and social media spread negative publicity swiftly
- If not handled efficiently and correctly, a data breach could ruin an organization:
  - Disrupt operations
  - Decrease customer loyalty
  - Damage brand image
  - Create negative perception in marketplace

AIG

Reputational Risk

- Coverage for confidential information protected under foreign privacy laws and breach notification laws;
- Expansion of the definition of a privacy event to include the failure to comply with an organization's privacy policy or the wrongful collection of confidential information;
- Inclusion of a "goodwill option" providing an adaptable response to event management giving a policyholder the option to offer a credit, coupon or rebate for future purchases in lieu of credit/identity monitoring in the event of a data breach;
- An updated definition of computer system to include coverage for an organization's use of cloud computing resources.

AIG

Type of Insured

Who’s Buying?

- Started with Tech companies as an E&O add-on.
- Retailers/e-tailers are big purchasers.
- Financial Institutions
- Healthcare
- Hospitality
- Manufacturers are starting to buy for business income protection
- Education

AIG

Security/Privacy Concerns by Industry

- Manufacturing – Corporate confidential information; Concerned about network interruption/cyber extortion
- Retailer/Hospitality – Rogue employees with card skimmers; Malware on point-of-sale (POS) terminals; franchise issues
- Education – IT issues: weaker controls; decentralized; student turnover; budgets/attracting IT talent
- Healthcare – Higher than average employee turnover; shrinking operational budgets; Accountable Care Organizations (ACOs); Health Information Exchanges (HIE)

AIG

Losses

Breaches

Date Made Public	Incident
January 17, 2007	**TJX** Hacker theft due to an outdated wireless security encryption system resulted in breach of 45M card numbers. $40.9M settlement Visa; $24M settlement with Mastercard and a $9.75M settlement agreement with 41 State AGs. Fraction of total $275M+ cost of breach. $40M recovered from GL policy in defense.
March 24, 2008	**Hannaford** Malware attack that resulted in 4.2M credit card numbers stolen from magnetic strip of credit/debit cards swiped at checkout. Large forensic, defense costs and damages to financial institutions (no cognizable damage to consumers). Lengthy litigation with appeals.
January, 2009	**Heartland** Computer forensics determined that the company network was infected with several instances of malicious software, connected to a global fraud operation. $134M records breached leading to 16 separate class action lawsuits filed. Large settlements with credit card companies (i.e. Mastercard $41.4M and Visa $60M). Estimated cost of breach $140M+.
April 2, 2011	**Epsilon** Email marketing services provider whose customers included Walgreens, Best Buy, Citigroup and other major U.S. companies were affected by a breach of email addresses (not considered PII).
April 26, 2011	**Sony** Network breach exposed over 77M user accounts (cloud system). Many lawsuits filed, voluntary take down of network, litigation with Zurich (GL carrier, not Cyber). Millions of dollars in forensic costs; 55 class action complaints filed. Significant reputational risk.

AIG

Breaches

Date Made Public	Incident
June 7, 2011	**Citibank** Initial reports that hackers stole 21.2Mof its U.S. credit card customer's numbers; it was later determined only 1% was compromised (210,000). Alleged slow and reluctant announcement of breach and lead to spear phishing attacks.
January 6, 2012	**Zappos** Various PII compromised of 24M customers via hacking attacks against servers. Customers advised to change passwords and phishing attacks were a concern. Multiple class action suits against it and parent company, Amazon.
March 31, 2012	**Global Payments** Breach in its data processing system. The company was one of the biggest processors for Visa, Mastercard, Discover Financial and American Express. 1.5M card numbers affected. Questionable handling of incident from public relations perspective. Global Payments removed from approval list from some of the credit card companies.
June 6, 2012	**LinkedIn** 6.5 million encrypted passwords compromised and showed up on a Russian website that could allow criminals to break in to subscriber accounts. $5M Class action lawsuit filed alleging the social network failed to protect users' data and didn't use industry standard protocols and technology.

AIG


AIG