Barbican
Group

Meet the Market Event - Warsaw

24th October 2013

Introduction

- Barbican Insurance Group are a Lloyds syndicate formed in 2007. This year we have stamp capacity of £227m

- The Cyber / Technology / Media book started in 2009 and has grown to £7.5m this year

- I joined at the start of this year as Underwriting Manager

- We have a wide range of customers from start ups to large global companies

- Our book is heavily dominated by US clients, however 30% of our customers are based outside of the USA

- We have handled over 120 circumstances since the book was formed

What is cyber?

- As a market we have not helped ourselves by labelling the product “Cyber”

- Typically consists of the following:-
  - Technology Professional Services (3rd Party)
  - Multimedia Liability (3rd Party)
  - Security and Privacy Liability (3rd Party)
  - Crisis Management Costs (1st Party)
  - Data Recovery and Business Interruption (1st Party)
  - Regulatory Defence Costs (1st Party)
  - Cyber Extortion (1st Party)

Who is the enemy?

Understanding the exposure

- The average cost per individual for a data breach in 2011 was:-
  - UK = £79
  - USA = $194
  - Mainland Europe = €120-150
  - Australia = A$138
- The average cost per data breach in 2011 was:-
  - UK = £1.75m
  - USA = $5.5m
  - Mainland Europe = €2.5-3.5m
  - Australia = A$2.16m

Source - Ponemon Institute

Understanding the exposure

- Of the 47,000 incidents in 2012:-
  - 37% affected financial organisations
  - 23% affected retail firms and restaurants
  - 20% affected manufacturing, transportation and utilities
  - 20% affected information and professional services firms
- Other breach characteristics:-
  - 52% used some form of hacking
  - 76% exploited weak or stolen credentials
  - 35% included physical attacks
  - 29% leveraged social attacks
  - 13% resulted from employee privilege misuse or abuse

Source – Verizon Data Breach Investigations 2013

Vendors

- Vendors are key to handling Cyber claims
- Pre Loss is essential and would include:-
  - Risk management (may include surveys, penetration testing etc)
  - Education and training
  - Workshops
  - Assistance with DRP / BCP
  - Provision of applications or software
- Post Loss you need the following vendors or in house capability:-
  - Defence Breach Counsel
  - Monitoring / Coverage Counsel
  - Loss Adjuster
  - Forensics
  - Public Relations Firm
  - Customer Notification
  - Customer Support
  - Credit Monitoring (or similar)
  - IT Firm

Some claims scenarios

Technology Professional Services

- Typically claims will emanate from:-
  - Breach of contract
  - Avoidance of counter claim
  - Intellectual property rights
  - Efficacy
  - Defamation, libel or slander

- Possibly the most famous incident in recent years is the BSkyB vs EDS which settled at £318m in 2010. This relates to an EDS salesperson agreeing to build a system for BSkyB for £48m in 2000. Relations broke down between the companies in 2002, and BSkyB built the system themselves at a cost of £265m

Some claims scenarios

Multimedia Liability

- Typically claims will emanate from:-
  - Breach of copyright
  - Defamation, libel or slander
- A current case relates to an insured who started a blog to convey information to customers and the public
- This contained a logo / image that was similar to a logo that had been copyrighted by another entity
- They sent a cease and desist letter to our insured, however discussions failed and the third party filed suit
- Damages are estimated at $5m, and current legal costs are $1.23m
- This has not yet gone to trial

Some claims scenarios

Security and Privacy Liability

- Typically claims will emanate from:-
  - Theft or altering of data
  - Virus or malware attack
  - Denial of service attack
  - Other loss of data from systems
- The US has historically caused more concern due to their class action culture and legislation in place
- Europe may start to catch up as legislation is passed in either 2015/6, and companies target this area in the same way as PPI / ambulance chasing
- We have suffered a number of claims in this area, and this part of the policy responds to legal costs and damages awarded

Some claims scenarios

Crisis Management Costs

- This can include:-
  - Notification costs
  - Credit monitoring or similar
  - PR costs
  - Setting up call centres
  - Forensic analysis
- A recent claim involved an unidentified third party loading files up to our customers servers allowing them to corrupt existing files. This included PII including credit card information, and fraudulent charges were made on accounts worldwide
- We incurred costs under all of the above totalling $129,000. In addition we paid $150,000 in legal fees and $250,000 for the business interruption loss

Some claims scenarios

Data Recovery and Business Interruption

- This operates in the same way as traditional property cover, but typically covers the restoration of data following a breach, or lost revenue as a result of the breach
- Often indemnity periods provided are short (ie. less than 6 months) due to the immediate nature of the claim
- A recent claim we had involved a leading provider of managed services including IT platform hosting and infrastructure
- The hacker implanted malicious software tools and used “masking techniques” on the insured’s mainframe to take down part of the system
- It cost over £1m to resolve the issue, of which £600,000 relates to this part of the policy

Some claims scenarios

Regulatory Defence Costs

- This will cover legal costs to comply with any regulatory action taken against the customer following a data breach
- In some territories this can also extend to include fines levied
- A recent claim in the US involved a healthcare provider misplacing multiple drives containing PHI for over one million patients. It was not known if these were stolen, lost or destroyed
- They were required to notify all individuals as well as the HHS
- The HHS fined them for failure to protect the information
- The fine was $75,000, and legal costs were over $1m (including both HHS and affected parties)
- Overall costs were over $5m

Some claims scenarios

Cyber Extortion

- This covers costs incurred in the event a hacker steals data and then demands a ransom
- Losses under this area are not widely publicised
- A recent claim involves a small healthcare clinic who found that an unauthorised third party had gained remote access to their systems
- The third party posted a message on the server stating that they had encrypted the server, and they could only access their information if they paid a ransom
- The clinic contacted the local law enforcement and it was agreed payment should be made

The future

- Legislation is ramping up on a worldwide basis
- Vendors are expanding their reach from the USA to take advantage of these opportunities
- An increasing proportion of European customers are looking to explore costs of Cyber cover
- The mainstream media regularly reports cyber attacks raising public awareness
- This is an area that continually evolves as technology advances at such a rapid pace

Questions?