Liberty Mutual Insurance Europe Limited (LMIE)

Strategic Assets
ACORD
27th June 2013
Liberty Mutual Insurance Europe Limited (LMIE)

Practicing what we preach: cyber risk management and insurance for the Insurance Industry
Liberty Mutual Insurance Europe Limited (LMIE)

Data Breach Statistics
Data Breach Statistics

- According to Ponemon’s *2013 Cost of Data Breach Study*, the average number of records compromised in a UK data breach was 23,833.
- The average per capita cost of a UK data breach was found to be £86, a 7.5% increase from the previous year (Ponemon 2013)
- The average organisational cost of a UK data breach was over £2 (equivalent US figure £3.5m)
- In 2011 36% of data breaches involved negligent contractors or employees, making it the most common cause of a data breach. (Ponemon)
- Malicious or criminal attacks accounted for around 31% of data breaches in 2011. (Ponemon 2012)
- Detection and escalation costs averaged out at £455,000 last year. (Ponemon 2013)
- Average notification costs were £244,699
- The 3 most important factors identified as reducing the financial impact of a data breach were: CISO leadership, external consulting services and a quick response. (Ponemon 2012)
- In the 2011/2012 period, 136 data breaches were reported to the ICO by the private sector, an increase of 58% when compared to the 86 breaches reported in the same period the year before. (ICO official statistics)
- In a study of SMBs carried out by the National Small Business Study 85% reported they were secure from cyber threats though 77% didn’t have a formal written internet security policy and 40% had no data recovery plan. (Symantec: Small Business Study, USA)
- 40% of targeted cyber attacks are aimed at companies with fewer than 500 employees. (Symantec: Small Business Study, USA)
- This year alone (2013) the ICO has issued fines totalling £1,090,000
- Detica’s report on the cost of cyber-crime to the UK estimated that the UK economy lost £27bn per annum to cyber crime. (The Cost of Cyber Crime 2011)
- The theft of intellectual property was estimated as being the most costly form of cyber crime
- ID theft and other consumer targeted forms of Cyber Crime are estimated to have cost UK citizens £3.1bn in 2011
Liberty Mutual Insurance Europe Limited (LMIE)

Claims Examples in Financial Sector
Recognising Exposures: Data

• **Norwich Union**: Fraudsters were able to gain access to the data of hundreds of customers by using publicly available data to impersonate them.
  - The FSA said that although the other policyholders had not had their money stolen, Norwich Union’s call centre staff had disclosed confidential information about the customers, in some cases divulging their full bank account details. The fraud led to £3.3m being stolen from customers.
  - The FSA fined Norwich £1.7m for failing to adequately protect their customers' data.

• **Zurich** UK outsourced their data processing to Zurich South Africa. An unencrypted back up tape containing the personal information of 46,000 customers was subsequently lost.
  - The FSA found that Zurich had not made adequate provisions for the safety of their customers data and fined the company £2.275m.

• **A4E** A laptop containing full names, dates birth, postcodes of 24,000 people was stolen from the London home of an A4e worker. The Information Commissioner’s Office (ICO) ordered the Government's biggest private contractor to pay £60,000 for breach of the Data Protection Act.

• **Skipton** A printing error led a UK building society to expose the details of over 3000 customers. The building society sent letters to some of its customers containing the account number, balance, interest paid and surname and initial of other customers.
Recognising Exposures: Network Integrity

• **Bank of America**: For six consecutive days, the site delivered a series of slowdowns and outages, which the bank attributed to a combination of technical issues and higher than anticipated website traffic. The problem was noted as the result of a "multi-year project" to upgrade its online banking platform.

• **RBS, Natwest and Ulster Bank** In March this year the group’s computer systems were severely disrupted, leaving customers unable to access or manage their accounts. The bank had undergone a similar downtime the previous year caused by a problem with a software update. The downtime is estimated to have cost the group over £200m.
Liberty Mutual Insurance Europe Limited (LMIE)

Exposures in the Insurance Industry
Exposures in the Insurance Industry

Data exposures

- Insurers are “data aggregators”.
- There are around 40m motorists in the UK, each requiring insurance.
- Sometimes this data may by necessity relate to personal or financial characteristics which are highly sensitive.
- The following types of data are classed as sensitive under the Data Protection Act:
  - the racial or ethnic origin of the data subject,
  - his political opinions,
  - his religious beliefs or other beliefs of a similar nature,
  - whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
  - his physical or mental health or condition,
  - his sexual life,
  - the commission or alleged commission by him of any offence, or
  - any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.
Network Exposures

• According to a 2010 survey by Accenture, 70% of consumers expected to purchase or renew an insurance policy online in the coming 12 months.
  – The UK’s insurance market has seen the most penetration from online services internationally.

• Celent estimates global IT spending by insurance companies will reach $40.6 billion in 2012, an increase of 6.3 percent over 2011. This figure is substantially higher than the 1.1 percent IT spending growth increase experienced in 2011.
Liberty Mutual Insurance Europe Limited (LMIE)

What are Cyber Exposures?
General Exposures

• Property Damage (tangible)
  – Consider a virus on a PC
    • Multiple re-writing of hardware to create bad cluster
    • Controlling functions, e.g. slowing down cooling-fan, whilst making the processor work hard
    • Erasing firmware of devices (although arguably a software risk?)
    • “Turkey” virus, focused the photon beam in CRT monitors to cause burn-damage
    • In a world run by computing power, imagine consequences in commercial properties
      » Control of buildings, factories, utilities, data-centres
      » Consequential damage to 3rd parties
  – Consider all business interruption
  – Digital Assets
General Exposures

• Personal Injury Damage?
  – Uncontrollable machinery
  – Utilities, controlled environments
  – Mental anguish/emotional distress?
  – Proximate cause issues
General Exposures

• **Privacy Liability**
  – Violation of privacy laws or regulations that permit individuals to control the collection, access, transmission, use, and accuracy of their personally identifiable information

• **Confidential Information**

• **Data Damage & Network BI**
  - Of first & Third party
  - Malicious Code
  - DDOS

• **Regulatory Fines & Penalties**
General Exposures

European Regulatory Issues

- European Convention of Human Rights
- EU Data Protection Directive – Civil Liability
- National Interpretations
- “Data controller” responsibilities
- Strict rules on sharing non-public personal information
- E-Privacy Directive: ISP & Telecoms - notifications
- Country specific notifications
  - Austria, Germany and Norway legislation
  - Cyprus, Czech Republic, Estonia, Sweden and Hungary - Interpretation of duty to notify
- Regulatory Fines and Penalties (not always insurable)
  - Information Commissioners Office (ICO) can issue fines of up to £500,000
- PCI – Credit Card Fines
General Exposures

United States

• State Breach Disclosure Statutes (46 states)
• Trend toward state data security regulations:
  – Massachusetts 201 CMR 17 (WISP)
  – Nevada Rev. Stat. 603A (compliance with PCI DSS)
  – Minnesota (Plastics Card Security Act)
• Aggressive regulatory scheme at state and federal level:
  – Attorneys General
  – Federal Trade Commission
  – Health & Human Services
• National Laws
  – Gramm-Leach-Bliley Act
  – FCRA/FACTA
  – Health Insurance Portability & Accountability Act
  – Health Information Technology Act (HITECH)
• Class Actions & Multi-District Litigation
General Exposures

• **Security Liability & Contractual Liability**
  - Unauthorised access or computer attacks from a network to another's
  - Liquidated damages & Civil damages
  - Extortion
  - Fraud and theft using network

• **Reputation**
  - Loss of confidence by customers leading to a drop in revenues over an extended period of time

• **Media Liabilities**
  - Liability for content on websites
    - Defamation
    - Breach of copyright and trademark
Liberty Mutual Insurance Europe Limited (LMIE)

Can traditional coverage help?
Can Traditional Coverage Help?

• **Property**
  - Data not “tangible” property at law
  - Physical-damage business interruption only
    • Requirement of property damage
    • Fire, wind and other named perils etc
  - *Furthermore the following exclusions are often contained in property policies:*
    • Virus exclusions
    • Failure of a system or microchip exclusion
    • Intangible property & electronic data exclusions
    • Costs to recreate data excluded even where physical damage. (This can sometimes be added by endorsement where caused by named peril, but it will cost extra and the cover will be narrower than that in cyber policy)
    • Value of the data excluded
Can Traditional Coverage Help?

• **General Liability**
  – Only covers damages to a third party.
  – Typically limited to bodily injury or property damage of tangible assets.
  – May be geographically limiting.
  – Some policies will have a specific cyber exclusion (e.g., might apply be applied to a bank, trading platform, telecom company), this exclusion is often included in addition to “loss or damage to data” exclusions on many policies.

• **Crime insurance**
  – Usually limited coverage for money, securities, or “tangible assets.”
  – Must be a “loss” and a “gain” to trigger coverage.
  – Identification of perpetrator sometimes required.
  – Does not address the business income loss.
Can Traditional Coverage Help?

- **Professional Indemnity/E&O**
  - Not all businesses buy such coverage
  - Some Tech/Media coverage gives partial cover
  - Liability only
  - Occurring in the “ordinary course of business”- the definition of professional services may be narrow and not include, for example, administrative changes.
  - Employee liabilities excluded
  - Notification costs/Asset damage/BI typically excluded
Liberty Mutual Insurance Europe Limited (LMIE)

“Cyber” Market Coverage
“Cyber” Market Coverage

• Triggers?
  – Computer crime & malicious attacks
  – Accidental damage or destruction of hardware which damages software/data
  – Accidental modifications/maintenance/entry of data
  – Failure to safeguard/destroy data

• Typical Exclusions
  – Power supply issues
  – Electrostatic build-up
  – “Backbone” of internet – outside control
  – Property Damage & Bodily Injury
  – Contractual liabilities (except where liability naturally at law)
  – War & Terrorism (carve-back available)
Insurance Driving Standards

• Developing a risk-based framework of *recommended* information security practices and policies

• Encouraging a risk-based culture, *adequate* business continuity plans and corporate information security policies within the industry

• Raising *awareness* through events and briefings to the industry highlighting the risks of Cyber loss

• Providing risk management and insurance professionals with *tools* to approach Cyber risks in partnership with their information security colleagues
Growth of Cyber Insurance

- Cyber Insurance is the fastest-growing specialty line in the commercial market. (2013 Experian Report)
- According to the 2013 Betterley report, the estimated total annual premium for Cyber Insurance is $1.3bn
- The number of Marsh's FINPRO practice clients that purchased cyber insurance grew by 33.3% in 2012 from 2011
- Limits purchased in 2012 averaged $16.8 million across all industries, an increase of almost 20% (Benchmarking Trends: More Companies Purchasing Cyber Insurance)
- 11.8% buy cyber insurance (Zurich 2013)
  - in 2012, this figure was 7.9%
  - by way of contrast, 43.9% of organizations in the US buy cyber insurance
Contacts

• Matthew R. Hogg, LL.B.(Hons), LL.M., ACII
  • Vice President, Strategic Assets
  • Liberty International Underwriters
  • Phone: +44 (0)20 7860 6208
  • Mobile: +44 (0)7825 953 918
  • Email: matthew.hogg@libertyiu.com

• Michael Shen ACII
  • Senior Underwriter, Strategic Assets
  • Liberty International Underwriters
  • Phone: +44 (0)20 7082 8520
  • Mobile: +44 (0)7879 445 139
  • Email: michael.shen@libertyiu.com

• Matthew Muggeridge (BA Hons)
  • Underwriting Assistant, Strategic Assets
  • Liberty International Underwriters
  • Phone: +44 (0) 207 8608 543
  • Email: Matthew.muggeridge@libertyiu.com