Demystifying Cyber Insurance

Jamie Monck-Mason & Andrew Hill

Introduction

• What is cyber?

• Nomenclature
What specific risks does cyber insurance cover?

- **First party risks** - losses arising from a data breach
  
  **Breach response**
  
  - Forensic costs,
  - Notification of data subjects
  - Credit monitoring/call centre
  - Legal costs and PR costs

- **First party risks** - losses arising from a failure of network

  **Business Interruption (add-on)**

- **Third party risks**

  1. **Security liability**
     - Claims arising out of unauthorised access to/use of an organisation’s computer network e.g.:
       
       - TPLs arising from loss of personal data, for example, credit obtained under stolen identities
       - TPLs arising out of Point of Sale terminal, for example, the skimming of credit cards
       - Network security TPLs, for example, employee vendettas
2. **Privacy liability** (breach of data protection legislation, e.g. Data Protection Act 1998, Privacy and Electronic Communications Regulations 2003) e.g. claims arising out of:

- Invasion of privacy
- Damages arising out of identity theft
- Actions from connected third parties e.g. banks, retailers
- Regulatory actions brought by the ICO resulting in fines and penalties (not presently insurable under domestic law)

---

**What are the threats? Understanding the exposures**

- Theft or loss of physical records
- Theft or loss of laptops/memory sticks
- Hacking for financial gain/activism/state sponsored
- Planting of malware in order to access network
Denial of Service attacks
Third party suppliers responsible for organisation’s data e.g. cloud service providers
Employees (with or without vendettas) including insider-assisted data loss

The Data Protection insuring clause in focus
Forensics – identifying and closing the vulnerability (where necessary); identifying the data subjects affected by data breach
Legal – specialist lawyers to advise on the response required by relevant law and to draft appropriate notification correspondence
Notification – the cost involved in notifying all affected data subjects
• Credit monitoring/call centre – may be offered to affected individuals as part of PR exercise and to mitigate against any potential claims

• PR – perhaps the most serious threat to business following a breach

---

**Quantifying the loss of a data breach/network failure**

• Business interruption – loss of income if computer system down for a period of time following a hack attack

• In the US, the average cost of a data breach is $214 per record

• In the UK, the average cost is £71
What is and isn’t covered under a cyber policy?

• **Third party losses**

  Standard E&O analysis – wrongful acts which gives rise to liability for:
  
  – Breach of duty
  – Infringement of IP rights
  – Defamation

• **First party losses**

  ✓ Forensics
  ✓ Notification
  ✓ Legal fees
  ✓ Credit monitoring/call centre
  ✓ PR
  ✓ Business interruption (add-on)
  ✓ Data loss recovery (add-on)
  ✓ Cyber extortion (add-on)
What is and isn’t covered under a cyber policy? contd

• First party losses under a cyber policy are traditionally triggered by an “event”

• No requirement of a “claim” for “damages” arising out of a “wrongful act” type analysis

- The cost incurred by management dealing with enquiries from affected data subjects (not easily quantifiable)
- Virus software upgrades
- Security consultants
- Replacement or repair of physical item e.g. stolen laptop, failed server
- Data loss recovery (unless purchased as an add-on)
Do other policies cover data breaches?

- Property (data not property)
- EL/PL
- Crime/Bond
- K&R (expect maybe extortion or threat – rarely reported by policyholders in any event due to adverse publicity)

Managing Risk

- Cyber insurance should compliment the risk management program of any business, not be purchased instead of

- Businesses should have procedures implemented in the event of a data breach, and they should be updated on a regular basis
Emerging Risks

• Cybersecurity is a fast evolving area

• Recent attempt by hackers trying to access confidential information in respect of xbox 720 highlights the risk to business – access to such information could take entire company down. Can insurance assist?

EU draft Regulation – why it matters

• Mandatory notification to national regulator
• Requirement to notify affected data subject in the event of a breach
• Imposes requirements that businesses may find costly to comply with
• Increased demand for cyber insurance in the UK?
A presentation by
HILL DICKINSON

WINNER
National law firm of the year
Legal Business Awards 2010