
a presentation by
HILL DICKINSON

WINNER

National law firm of the year
Legal Business Awards 2010


HILL DICKINSON

THE ANATOMY OF A CYBER POLICY

Jamie Monck-Mason & Andrew Hill

What's in a name?

Lack of uniformity in policies:

- Cyber
 - Cyber liability
 - Data protection
 - Tech PI
- 

The scope of cyber insurance

First party coverage

- **Breach response costs comprising:**
 - Forensic costs (i.e. identifying there has been a breach, the source of the breach, the extent of the breach and shutting the vulnerability off)
 - Notification to data subjects
 - Notification call centre
 - Credit monitoring
 - Legal costs and PR costs

Claims example: A large data processor lost back up tapes in transit. They contained personal data of army veterans. Their cyber policy met the costs of notification, call centres and credit monitoring

- **Fines and penalties:**

FCA fines not insurable under English law (Chapter 2 of CP191 of the FSA Handbook).

Safeway v Twigger [2010], Claimant could not recover OFT fines from D&O insurers.

Under English law, no express ban on indemnifying against ICO fines; however, ICO fines not likely to be insurable as a matter of public policy. PCI fines are contractual damages and therefore insurable.

Cover fines “where insurable” until there is greater certainty.




- **Cyber business interruption**

- Loss of income due to network security failure
- Additional expenses associated with getting back online

Claims example: Sony PlayStation Network offline for period of time owing to security compromise resulting in loss of income.

- **Data restoration costs**

- Costs associated with restoring or recreating data following network security failure
 - Additional expenses associated with getting back online
- 

- **Cyber extortion**

- Sums paid to criminals who, for example, issue threat of DDoS attack if ransom is not paid
- Alternatively, sums paid to criminals e.g. to withdraw existing DDoS attack or for the return of sensitive information
- Costs associated with instructing investigator

- **Cyber crime**

- Theft via computer systems
- Loss due to unauthorised and fraudulent access to electronic communications

Claims example: Criminals can hack into the computer system and direct telephones to call premium rate numbers (most telephone networks are now linked to computer network via voiceover IP)



Third party coverage

Traditionally comprises three heads of cover:

- 1. Privacy Liability**
- 2. Security Liability**
- 3. Multimedia Liability**



Privacy liability

Cover for:

Losses arising out of actual or suspected disclosure of personal data and/or credit card information via computer systems, laptop, data storage device, paper records.

Claims arising out of:

- invasion of privacy of the individual;
- breach of privacy-related legislation e.g. The Data Protection Act 1998



How these claims may be advanced under English law:

- **Breach of confidence**
- **Misuse of private information**
- **Breach of contract or negligence**
- **Claim for compensation under Section 13 of Data Protection Act 1998**
- If all domestic avenues exhausted, **claim under section 7 of Human Rights Act 1998** for breach of Article 8 of the European Convention on Human Rights (right to respect for private and family life)



Claims examples:

- **Data processor lost back up tapes in its custody. Following notification of the data breach, proceedings commenced by affected individuals. Claimants alleged invasion of privacy by public disclosure of private facts.**
- **Price comparison website referred customers to an IFA, which turned out to be a criminal organisation. The IFA used customers' details to perpetrate various frauds against them. Affected parties issued a claim for invasion of privacy and negligence.**
- **A university doctor's work laptop stolen, which contained the medical records of his patients. Following notification of the breach, proceedings were issued by affected individuals.**

Security liability claims

Cover for:

Losses arising out of virus transmission or hacking attack from the Insured's computer system and failure to facilitate authorised access to computer network.

Claims arising out of :

- Hacker/employee utilising without authorisation computer network to commit fraud, theft or DDoS attack (i.e. via unauthorised access to computer network).
- Transmission of viruses (inadvertently or by employee with vendetta) (i.e. one computer network attacking another).

How these claims may be advanced under English law

- Breach of contract or negligence
- 

Claims examples:


- Online retailer engaged marketing company to distribute promotional emails to its customers. An email contained a link with embedded malware designed to record keystrokes. Affected customers issued claim against online retailer (PL insuring clause), which in turn claimed for an indemnity against marketing company.
- Tech company employee sent an email to client containing a virus, which took down their entire network. Client issued claim against tech company alleging breach of duty.
- Software company working on the development of prototype mobile telephone, on behalf of major tech company, were hacked by organised hacking group in China, which resulted in the theft of sensitive IP. Tech company issued claim against software company.

Multimedia liability


Claims arising out of:

- Defamation e.g. tweets, blogs
- IP infringement


How these claims may be advanced under English law:

- Libel/slander
 - Breach of copyright
 - Trademark infringement
- 

What isn't typically covered under a cyber policy?

- Patent infringement
 - 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
- 

Do other policies cover “cyber” losses?

- **Property & Crime/Bond** (data not tangible property; absence of IPG)
 - **EL/PL** (focus on personal injury)
 - **K&R** (not concerned with data except maybe when for purposes of extortion)
 - **PI/E&O** (typically only covers claims arising out of “professional services”, specific exclusions for data related losses)
- 

UK vs US

- Too much emphasis in domestic market on US law/wordings? US policies have been transferred into domestic market
 - PII/PHI versus personal data
 - Claimant's costs
 - Mandatory notification in UK limited to ISPs and telcos, at present. Draft EU Regulation. Notification should, however, be encouraged. ICO likely to issue significant fines if they suspect a cover up

a presentation by
HILL DICKINSON
