

# CYBER – THE LEGAL OBLIGATIONS ON CUSTOMERS AND HOW CYBER POLICIES CAN ADDRESS THEM

Tim Smith  
Partner, BLM  
T: 020 7865 3313  
E: [tim.smith@blmlaw.com](mailto:tim.smith@blmlaw.com)

# KEY CYBER EXPOSURES



- ▶ Almost complete dependency on computer systems
- ▶ All key business and customer/client data stored in one place
- ▶ Vulnerable to system malfunction or denial of service attack
- ▶ A hacker with access to the data could wreak havoc operationally, through the physical destruction of data, servers and infrastructure and by threatening the safety of people.
- ▶ Hackers who are not interested in one company's data may still capitalise on weaknesses in its system to reach other IT networks.



# WHAT ARE 'CYBER' RISKS?

---



- ▶ Data (loss or theft)
- ▶ Intellectual property
- ▶ Confidential information
- ▶ Private information
- ▶ Defamation
- ▶ System failure (hardware/software)

- ▶ Loss of own data/trade secrets
- ▶ Business interruption (e.g. through system failure, denial of service attack, cyber extortion)

## PERIMETER RISK: RESPONSIBILITIES FOR DATA BELONGING TO THIRD PARTIES



Nearly all businesses will have not only their own data on their computer network but that of:

customers;

business partners;

suppliers;

employees.

They have legal obligations to all of them to protect that data.

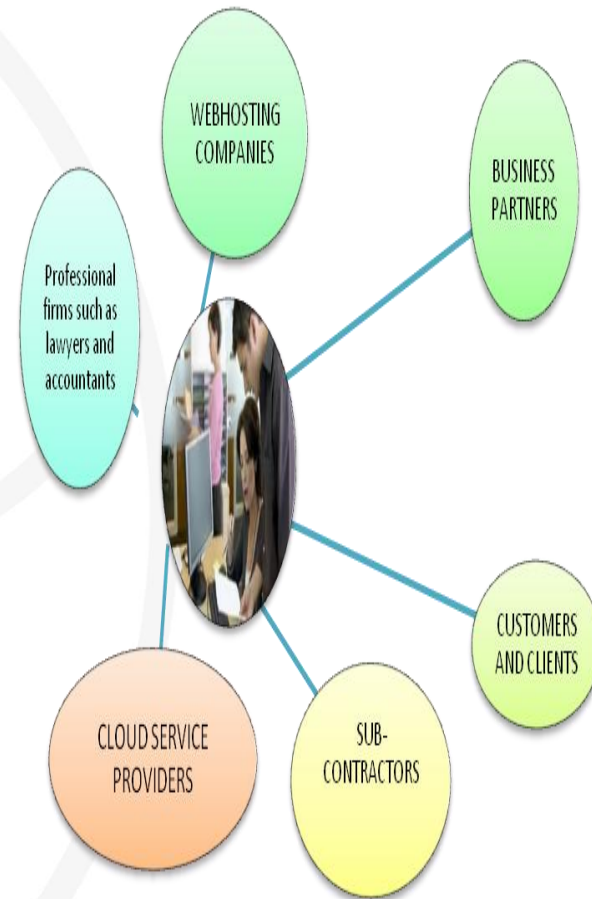


## PERIMETER RISK: SHARING INFORMATION ALSO CREATES RISK:

---



- Cloud service providers
- Webhosting companies
- Professional advisers
- Business partners
- Customers and clients



# WHAT ARE THE OBLIGATIONS ON INSUREDS AND WHAT ARE THE CONSEQUENCES OF BREACHES?

---



- ▶ Damages, fines, regulatory action, reputational harm
- ▶ Data protection
- ▶ Breach of confidence
- ▶ Privacy
- ▶ IP/Defamation
- ▶ Negligence
- ▶ Payment Card Industry Security Standards

- ▶ Section 4(4)

*"...It shall be the duty of a data controller to comply with the Data Protection Principles in relation to all personal data with respect to which he is the data controller".*



# THE DATA PROTECTION PRINCIPLES

---



*“(1) Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless (a) at least one of the conditions in Schedule 2 is met, and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.*

*(2) Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes...*

*(4) Personal data shall be accurate and, where necessary, kept up to date.*

*(5) Personal data processed for any purpose or purposes shall not be kept for longer than it is necessary for that purpose or those purposes...*

*(7) Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.”*

## ▶ Section 13

*“(1) An individual who suffers damage by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller for that damage.*

*(2) An individual who suffers distress by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller for that distress if (a) the individual also suffers damage by reason of the contravention, or (b) the contravention relates to the processing of personal data for the special purposes.*

*(3) In proceedings brought against a person by virtue of this Section it is a defence to prove that he had taken such care as in all the circumstances was reasonably required to comply with the requirement concerned.”.*

- ▶ Halliday v Creation Consumer Finance
- ▶ AB v Ministry of Defence
- ▶ CR19 v Police Service of Northern Ireland
- ▶ Vidal-Hall v Google
- ▶ TLT and Others v Secretary of State for the Home Department and Others
- ▶ Brown v (1) Commissioner of Police of the Metropolis (2) The Chief Constable of Greater Manchester Police

# THE PEOPLE PROBLEM: QUESTIONS TO CONSIDER WITH YOUR CLIENT

---



Have you:

- ▶ Implemented organisational and physical cyber security measures in addition to technical cyber security?
- ▶ Identified key cyber exposures and the types of information that you hold on computers?
- ▶ Appointed a cyber risk manager/Chief Information Security Office ("CISO") and allocated management responsibility for digital risks within the organisation?
- ▶ Implemented a written cyber security policy that has the backing of the board and senior management and is enforced through regular staff training and monitoring?
- ▶ Developed a cyber incident risk management plan for each type of incident which includes access to external incident response services?
- ▶ Checked the cyber security of your suppliers, service providers, business partners and professional advisers?
- ▶ Accurately predicted what the impact would be on the business of each type of cyber incident?

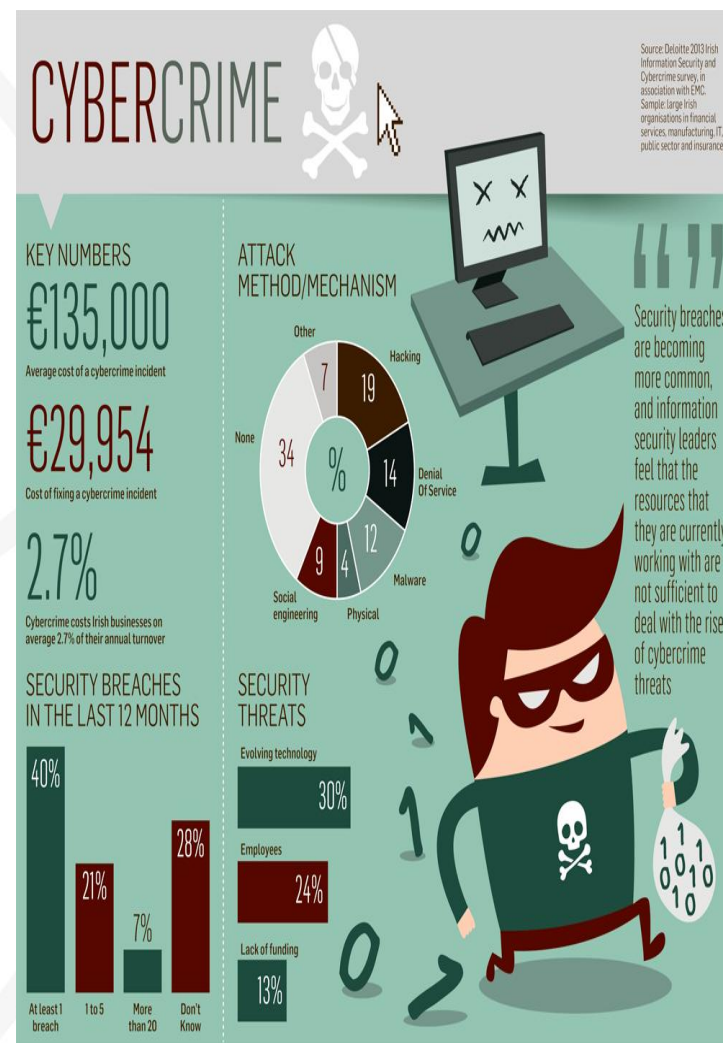
- ▶ Physical security
- ▶ IT security
- ▶ Training
- ▶ Policies/procedures
- ▶ Supply chain management
- ▶ Supporting insureds – claims defensibility, data protection risk, technical vulnerability, incident training
- ▶ Cyber essentials, cyber essentials plus and ISO27001
- ▶ Guidance and support from the Information Commissioner's Office ("ICO")

# THE BUSINESS CASE FOR CYBER INSURANCE



Potential financial consequences of a cyber incident:

- ▶ Financial losses due to theft of own personal and commercial data.
- ▶ Financial losses due to loss of own personal and commercial data.
- ▶ Claims by third parties in respect of theft or loss of personal and commercial data stored on the victim's system.
- ▶ Financial losses due to system downtime.
- ▶ Financial losses due to reputational damage.
- ▶ Claims by third parties as a result of the interruption of computer based services provided by the victim.
- ▶ Regulatory and industry fines.
- ▶ Costs of dealing with incident.



- ▶ Duty of Fair presentation:
  - ▶ *“every material circumstance which the insured knows or ought to know, or*
  - ▶ *failing that, disclosure which gives the insurer sufficient information to put a prudent insurer on notice that it needs to make further enquiries for the purpose of revealing those material circumstances.”*

- ▶ Deliberate or reckless non-disclosure, the insurer:
  - ▶ may avoid the contract and refuse all claims, and
  - ▶ need not return any of the premiums paid.
- ▶ Non-deliberate or non-reckless breach or innocent mistake:
  - ▶ Proportionate remedies will apply which are all based on what the insured would have done had it known the true facts.



- ▶ Basis of contract clauses abolished
- ▶ Condition precedent that does not apply to the whole risk will only provide an insurer with a complete defence to a claim where the insured cannot demonstrate that its breach could not have increased the risk of loss sustained.
- ▶ Insurers no longer be able to rely on warranties that are irrelevant to the risk.
- ▶ Warranties suspensory

- ▶ Cyber Proposal forms generally specific and detailed.
- ▶ The Insurance Act has “levelled the playing field”.
- ▶ Ironically, therefore, the Courts are likely to be unsympathetic to insured’s not providing a genuinely fair presentation.
- ▶ Conditions precedent will apply to requirements to report cyber incident – care needs to be taken to distinguish between notification of an “incident” and a “claim”.

- ▶ Third party – data loss, data theft, IP infringement, defamation, privacy, breach of confidence.
- ▶ First party – business interruption due to cyber event (such as a denial of service attack or ransomware), data loss, data theft, system restoration.
- ▶ Response team

# CONVENTIONAL INSURANCE MAY NOT COVER CYBER RISK



Insurance Product	Core Loss Coverage	Consideration
Property	Physical Loss or Damage to Assets	Exclusionary Language Physical Loss Trigger Events
Business Interruption	Loss of Revenue Plus Additional Costs	Commonly Triggered in Conjunction with the Property Policy
General Liabilities	Third Party Liability for Physical Property Damage and Bodily Injury	Exclusionary Language Physical Loss (To Property)
Errors and Omissions (Professional Indemnity)	Third Party Liability arising from Performance of a Professional Service	Breach of Professional Service Trigger Events
Crime Insurance	Loss of money, securities and other property arising from the fraud or dishonesty of employees or a third party	Loss of Money and Securities "Other Property" Definition

## CYBER RISK IS OFTEN SPECIFICALLY EXCLUDED

---



“.....subject only to clause ...., in no case shall this insurance cover loss, damage, liability or expense directly or indirectly caused by or contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system....”

- ▶ The General Data Protection Regulation
  - ▶ Mandatory reporting of incidents to those whose data has been lost/stolen and to Regulators
  - ▶ Fines of up to 4% of turnover
  - ▶ Increased territorial scope
  - ▶ More people/information caught
  - ▶ Stricter rules on consent
  - ▶ More focus on data security
- ▶ Brexit
- ▶ Types of claim
- ▶ Numbers of claim
- ▶ Policy developments - (e.g. new policies may cover physical damage)



CLEAR ► CONCISE ► CONNECTED