C4: ARE YOU READY FOR 2018?
WHAT LIES AHEAD FOR DATA PROTECTION, CYBER-HACKS AND DIRECTORS' LIABILITIES
A LEGAL UPDATE IN THE LAND OF BREXIT

June 2017

Helen Grimberg
Partner
BLM

Terry Renouf
Consultant
BLM

Tim Smith
Partner
BLM

Alexander Traill
Partner
BLM

Alexander Traill
Global Head of Underwriting
Generali

WHAT LIES AHEAD FOR DATA PROTECTION AND CYBER

WHAT ARE 'CYBER' RISKS?

- Data (loss or theft)
- System failure (hardware/software)
- Intellectual property
- Confidential information
- Private information
- Defamation/multimedia risk
- Payment Card Industry Security Standards
- Consequences - damages, fines, regulatory action, reputational harm

KEY CYBER EXPOSURES

- Almost complete dependency on computer systems
- Vulnerability to system malfunction or denial of service attack
- All key business and customer/client data stored in one place
- Someone (a 'hacker' or insider) with access to the data could wreak havoc operationally, through the physical destruction of data, servers and infrastructure or by stealing data
- Supply chains - hackers who are not interested in one organisation's data may still capitalise on weaknesses in its system to reach other IT networks

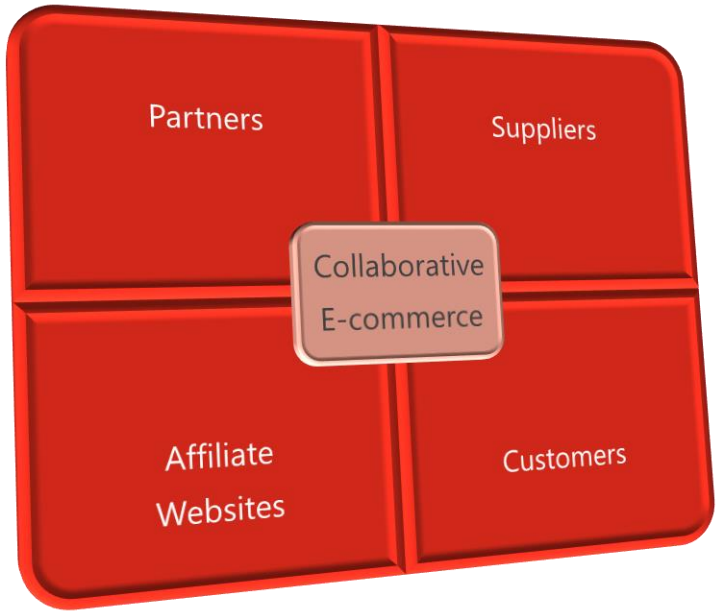
FIRST PARTY RISKS

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

THIRD PARTY RISK

Nearly all businesses will not only have 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

- 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."

DATA PROTECTION ACT 1998

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.".

THE RECENT CASES – PATTERNS AND TRENDS

- *Halliday v Creation Consumer Finance*
- *AB v Ministry of Justice*
- *CR19 v Police Service of Northern Ireland*
- *Vidal-Hall v Google*
- *Gulati v Mirror Group Newspapers*
- *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*
- *Morrisons*

WHAT NEXT

The General Data Protection Regulation – 25 May 2018

- 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
- Right to be forgotten
- Easier access to your own data
- Right of data portability

WHAT NEXT (…continued)

Technological developments

- Continuing use of (and reliance on) computers and the internet
- Internet of things
- Driverless vehicles

WHAT NEXT

BREXIT

"We will be members of the EU in 2018 and therefore it would be expected and quite normal for us to opt in to the GDPR and then look later at how best we might be able to help British businesses with data protection while maintaining high levels of protection for members of the public".

Karen Bradley, Culture Secretary

"We will be bringing legislation forward in the next [parliamentary] *session to put that* [full implementation of the GDPR] *into practice".*

Matt Hancock, Digital Minister

"We are committed to helping organisations to prepare for the GDPR, which will apply in the United Kingdom from 25 May 2018".

ICO

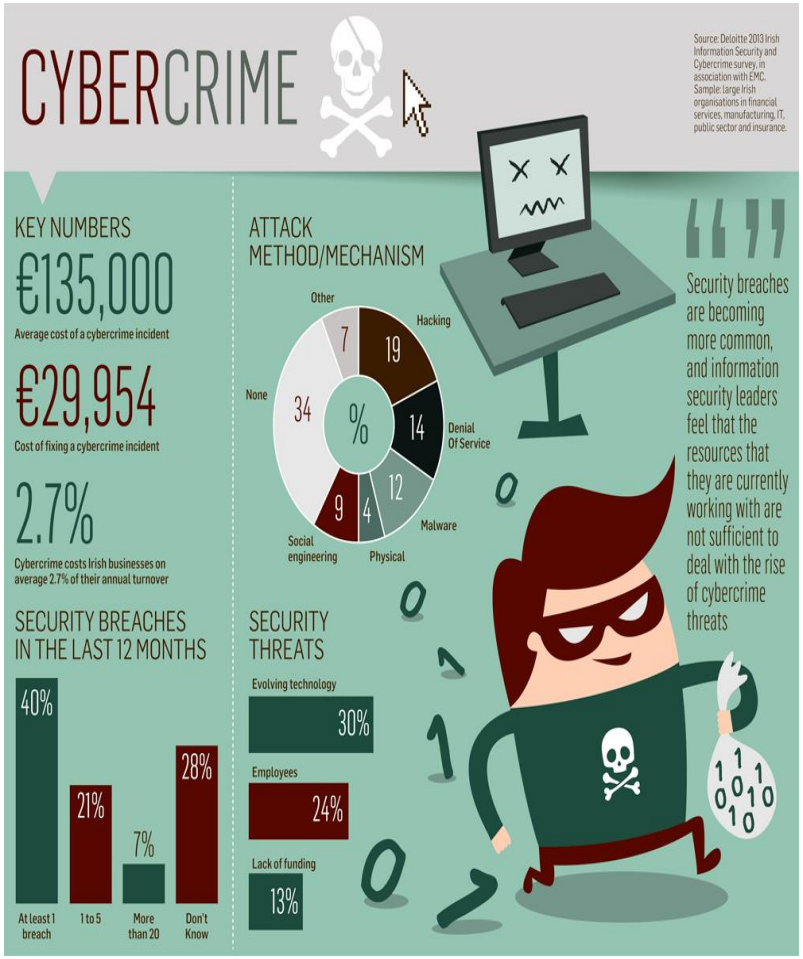
WHAT NEXT

WHAT WILL BE THE INPACT OF THE GDPR, THE DEVELOPMENTS IN CASE LAW AND DEVELOPMENTS IN TECHNOLOGY?

- Types of claim
- Numbers of claim
- Insurance market response – policy developments (e.g. new policies covering specific sectors or physical damage)

RISK MANAGEMENT – 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.



RISK MANAGEMENT – QUESTIONS TO ASK

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?

RISK MANAGEMENT – ISSUES TO CONSIDER

- Physical security
- IT security
- Training
- Policies/procedures
- Supply chain management
- Working with insurers/risk businesses - 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')

COMMON ELEMENTS OF A CYBER POLICY

- 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…."

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."*

INSURANCE ACT PROPORTIONATE REMEDIES FOR MATERIAL NON-DISCLOSURE

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.

INSURANCE ACT: CYBER CONTEXT

- 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 customers not providing a genuinely fair presentation.

WHAT LIES AHEAD FOR DIRECTORS' LIABILITIES IN 2018

OVERVIEW

1. Cultural change in the Regulatory landscape

2. Cyber: the impact of the General Data Protection Regulations ('GDPR')

3. Key considerations for risk managers when engaging at Board level

INCREASED REGULATORY ACTIVITY

1. Catalyst for change: Senior Managers Regime
2. Deferred Prosecution Agreements
3. Persons of Significant Influence'
4. Health and Safety Guidelines

INCREASED REGULATORY ACTIVITY

Insurers' perspective to the changing landscape:

- Costs : adequate protection to emerging exposures?
- Disclosure: Insurance Act obligations

Impact of the GDPR on Directors and Officers:

- Basic Principles which D&Os should be aware of
- How does personal liability arise?
  - Regulatory exposure
  - Civil exposure

Insurers' perspective:

- How companies might evolve, e.g. committees
- How D&O policies might adapt, e.g. fines/penalties

ENGAGEMENT AT BOARD LEVEL

- Considerations for risk managers :

- Coverage for investigations
  - Pre-investigation costs
  - Identity of the insured and depletion of aggregate limits
  - Adequate protection for Health and Safety risks

- Cyber risk management

ENGAGEMENT AT BOARD LEVEL

Insurers' perspective:

- Read and know your policy
  - Scope of coverage
  - Notification requirements
- Get to know your claims department
  - Early establishment of relationship with your insurer

CONCLUSIONS

1. Increased **personal accountability** for executives

2. Beware of **dual exposure** potential: ‘the double whammy'

3. **Know your policy** before you need to rely on it


CLEAR ▸ CONCISE ▸ CONNECTED