AIRMIC ENTERPRISE RISK MANAGEMENT FORUM

Date 10 November 2016

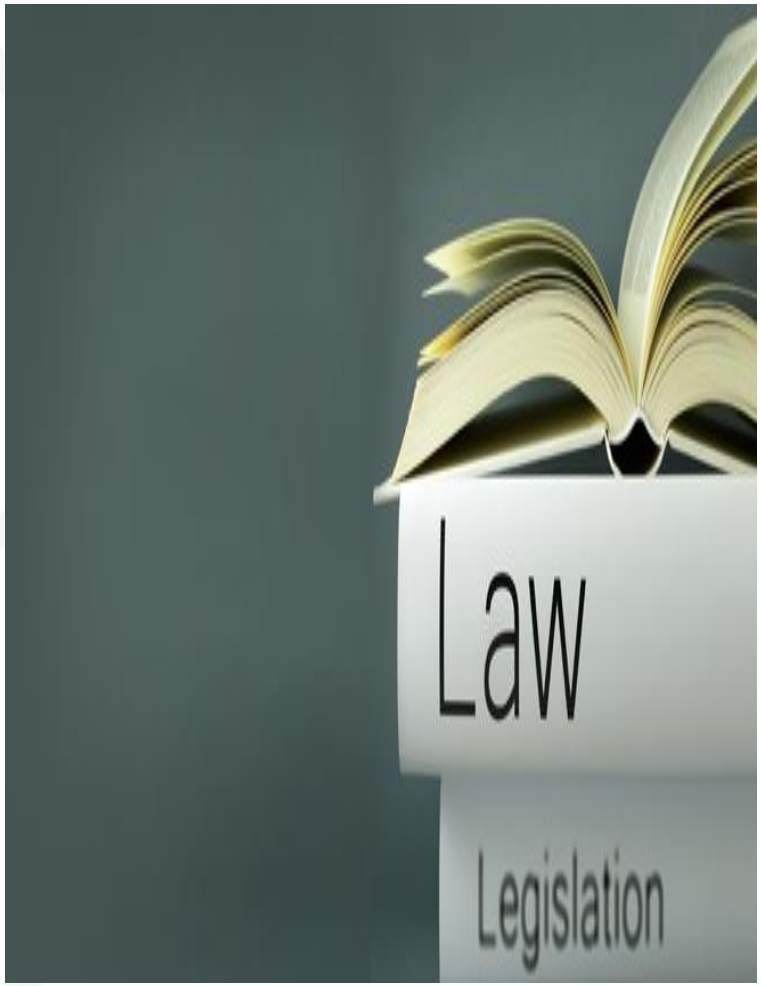
Name Nick Gibbons
Position, PARTNER BLM
T: 0207 457 3567
E: Nick.Gibbons@blmlaw.com

SUMMARY

- Cyber crime is now a daily reality
- Every business has its own genuine and significant cyber exposures
- Although many businesses have addressed internal/technical security, staff procedures and perimeter risk remain serious problems
- GDPR will make significant and complex changes to data protection law
- The EU Cyber Directive may have an even greater impact.
- The new law is very unlikely to be materially affected by Brexit
- Cyber risk is not effectively covered by conventional insurance

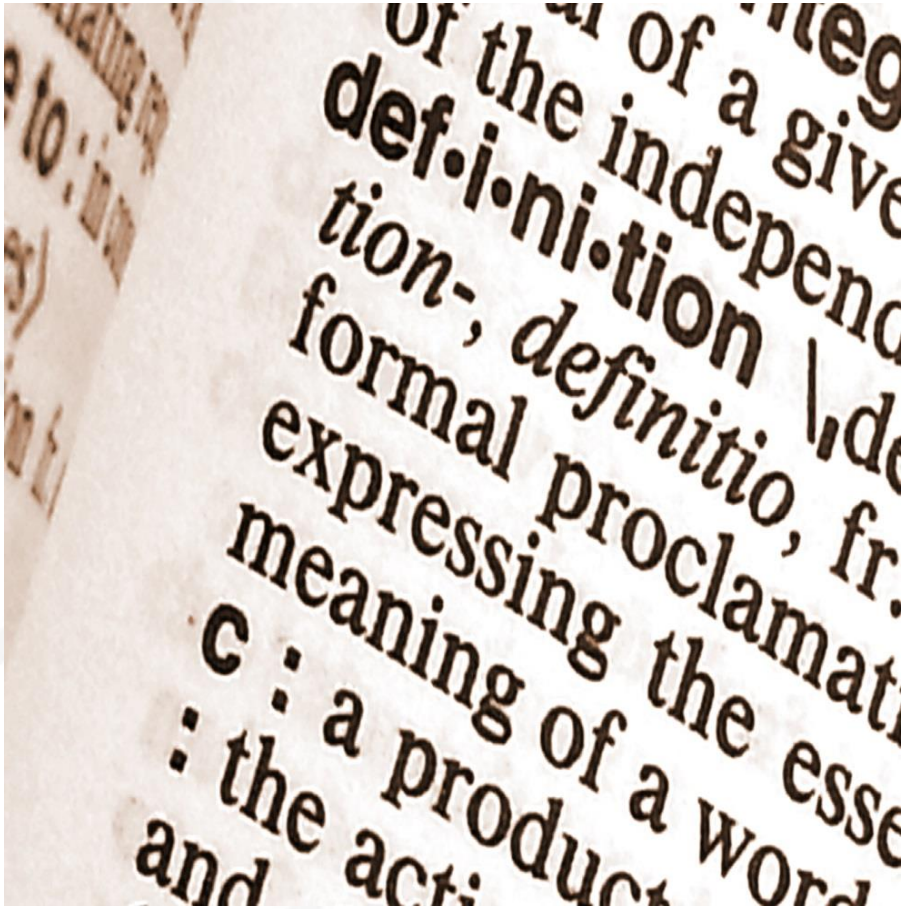
DATA PROTECTION : LEGAL FRAMEWORK

- Data Protection Directive 1995
- Data Protection Act 1998
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- Law of Confidence
- Contract
- Tort
- Payment Card Industry Security Standards
- General Data Protection Regulations 2016
- Cyber Security Directive 2016



DATA PROTECTION BASICS : KEY DEFINITIONS

- Data
- Personal Data
- Sensitive Data
- Processing
- Data Controller
- Data Subject



DATA PROTECTION BASICS – EIGHT PRINCIPLES

1. Personal data shall be processed fairly and lawfully.

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.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

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 is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects.

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.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

CYBER CRIME IS NOW A DAILY REALITY

- Cyber security now at the top of the agenda in many business
- Cyber attacks are now a virtual constant for large companies.
- Symantec estimates more than half a billion personal records were lost or stolen in 2015.
- Off-the-shelf criminal software is now widely available on the dark web.

THE PEOPLE PROBLEM: CYBER RISK MANAGEMENT IS NOT JUST A TECHNICAL ISSUE

Have you…… ?

- Implemented organisational and physical cyber security measures in addition to technical cyber security measures
- Made partners and staff aware of your firm's cyber exposures
- Identified the types of information that you hold on your computers and where
- Appointed a cyber risk manager and allocated management responsibility for digital risks within the firm
- Checked the cyber security of the firm's suppliers, service providers and business partners
- Implemented a written cyber security policy that has the proactive backing of partnership and is enforced through regular staff training and monitoring
- Implemented intellectual property guidelines
- Created a cyber incident risk management plan for each type of incident, which includes access to external incident response services
- Drawn up an accurate prediction of what the impact would be on the firm of each type of cyber incident to which it is exposed

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;

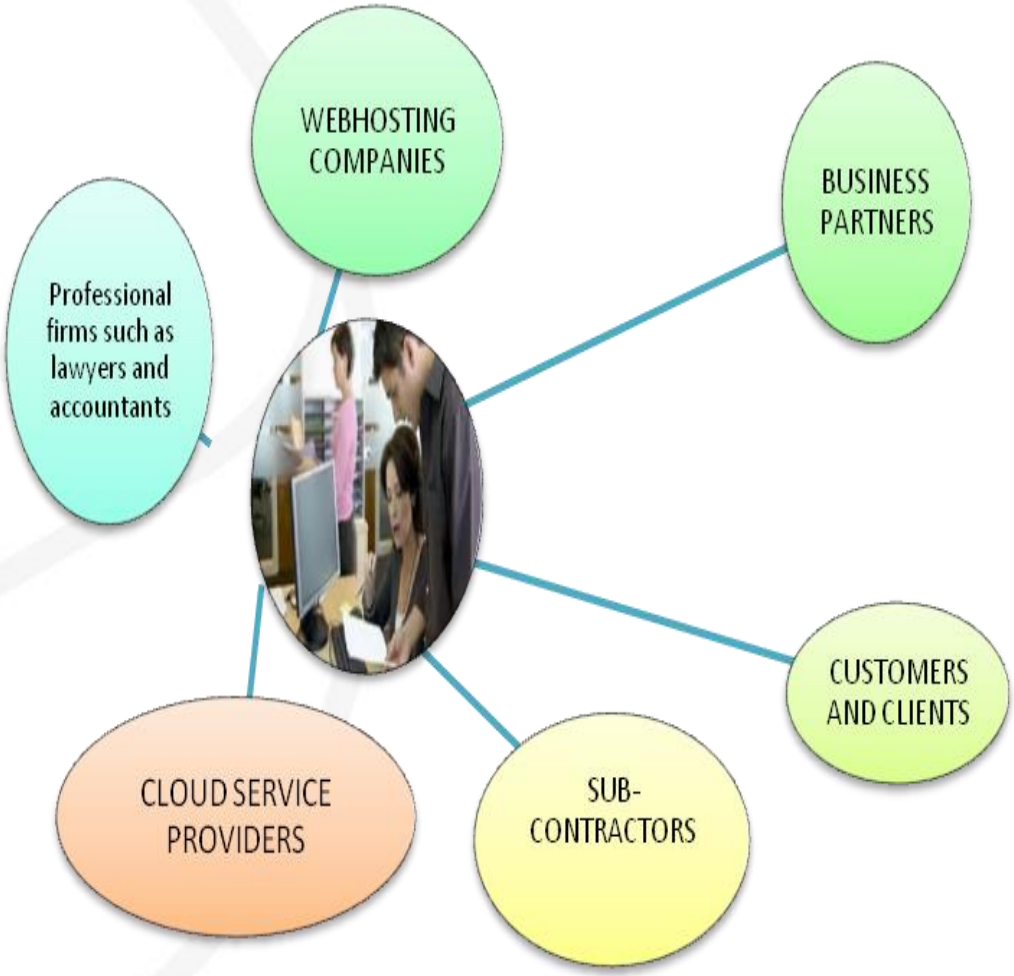
Suppliers;

Employees.

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

PERMETER RISKS:SHARING INFORMATION ALSO CREATES RISK:

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



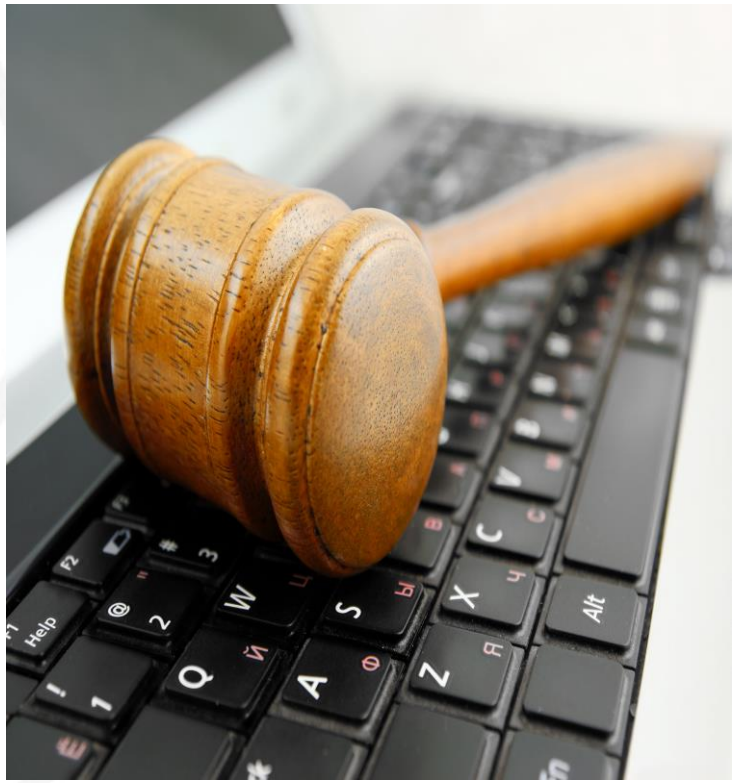
SHARING DATA WITH OTHER ORGANISATIONS: LEGAL ISSUES

- ICO GUIDANCE:

  "make sure that it will continue to be protected with adequate security by any other organisations that will have access to it.....

  ...take reasonable steps to ensure that those security measures are in place, particularly by ensuring that an agreed set of security standards has been signed up to by all the parties involved in a data sharing agreement.....

  ...the organisations the data is disclosed to will take on their own legal responsibilities in respect of the data, including its security.



CLOUD SERVICE PROVIDERS/WEBHOSTING – LEGAL ISSUES

- DPA Schedule 1 Part II :

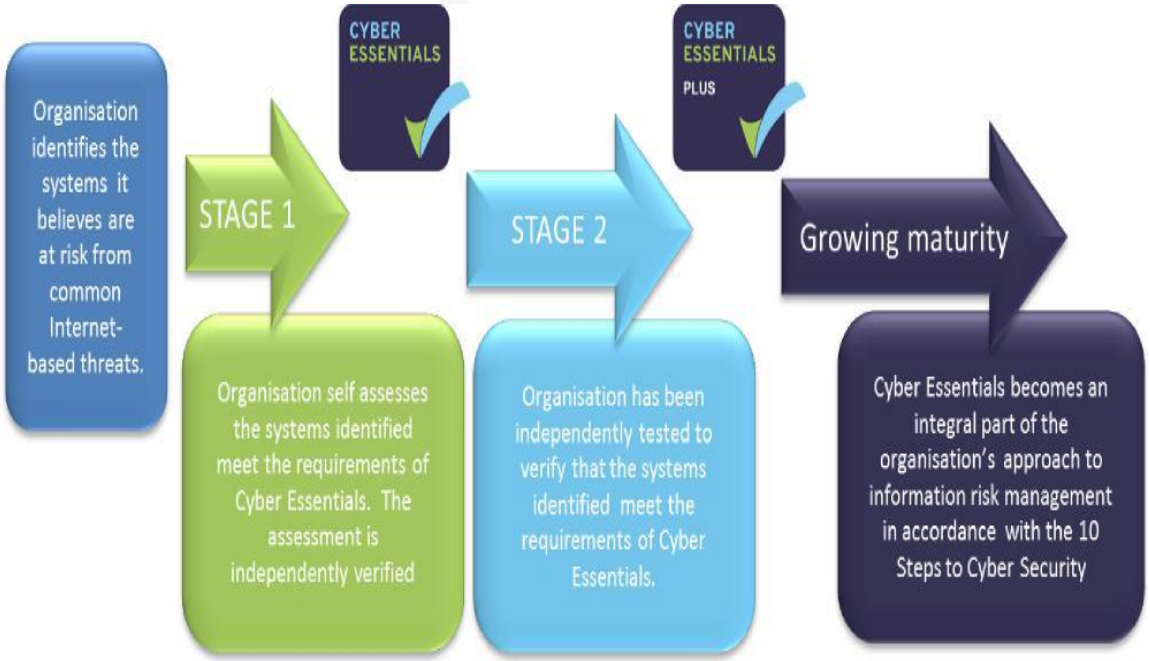
  "the data processor will comply with security obligations equivalent to those imposed on the data controller itself."

- ICO Guidance:

  "When processing is undertaken by a data processor, the data controller must choose a processor providing sufficient guarantees about the technical and organisational security measures governing the processing to be carried out, and must take reasonable steps to ensure compliance with those measures."

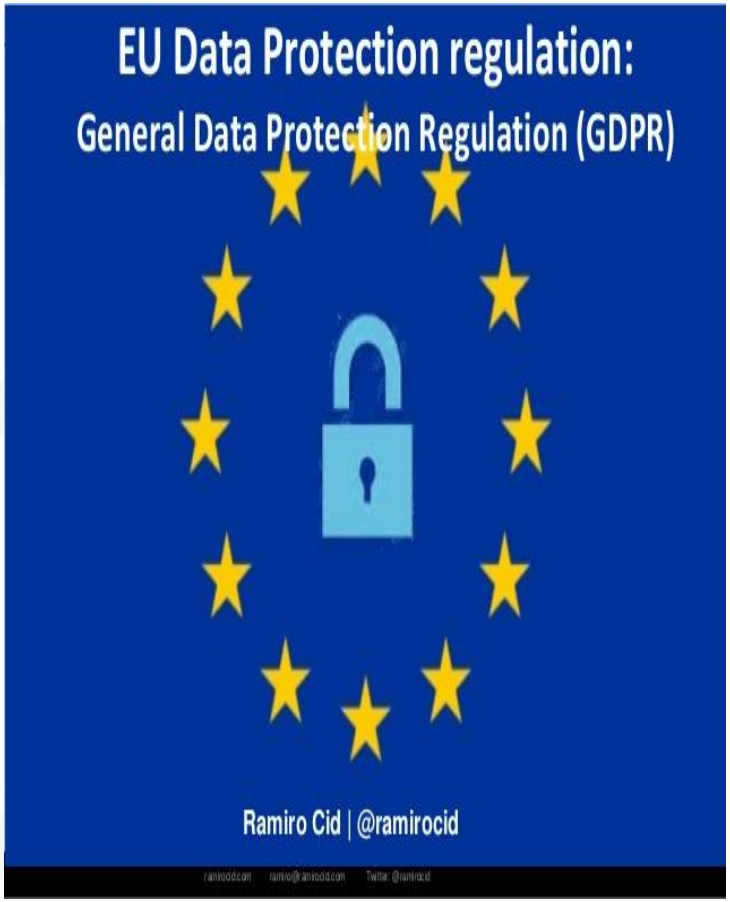
THE PROBLEM WITH CYBER ESSENTIALS…

- **Boundary firewalls and internet gateways**
- **Secure configuration**
- **Access control**
- **Malware protection**
- **Patch management**



GENERAL DATA PROTECTION REGULATIONS 2016 KEY CHANGES

- Requirement to notify breaches
- Much tougher fines
- Extra-territorial applicability
- Application to both processors and controllers
- One Stop Shop – lead supervisory authorities
- Abolition of requirement to register as a data controller
- Processing children's data
- European Data Protection Board
- Right to be forgotten
- Easier access to one's own data
- Right of data portability



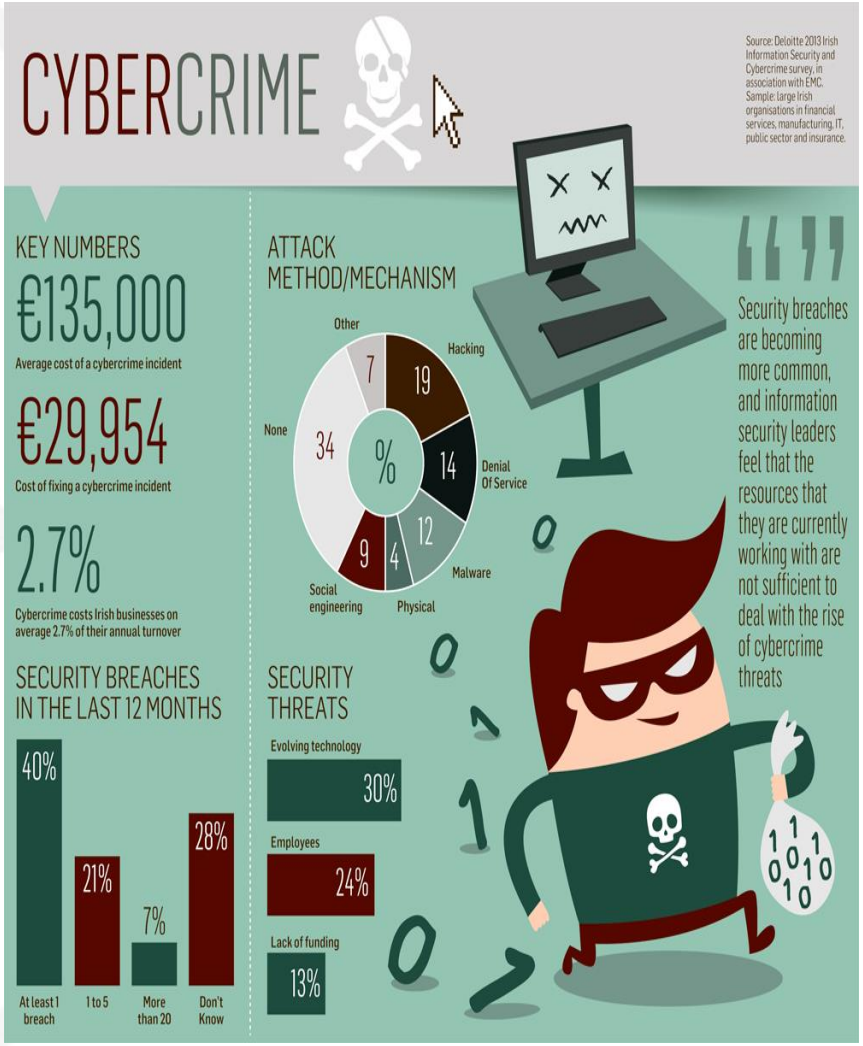
TO WHAT EXTENT WILL THE BREXIT VOTE AFFECT DATA PROTECTION LAW?

- Article 50 of Lisbon Treaty
- Timing
- GDPR's "long arm"
- UK Post Brexit options and adequacy
- EFTA and the Swiss model
- Going it alone
- Impact of Brexit on 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.



CONVENTONAL INSURANCE DOESN'T 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…."


CLEAR ▸ CONCISE ▸ CONNECTED