Transpire Event | Risk Issues as a NED - Cyber Security

7 June 2017

What we will cover

- The General Data Protection Regulation 2016/679 (GDPR)
- Understanding the cyber threat and reputational risks
- Cyber security insurance
- What this means for you…!

The General Data Protection Regulation 2016

- The Data Protection Act (1998) is nearly 20 years old…
- Technology has advanced greatly and is still changing every day and data protection and privacy cannot keep up
- The GDPR is in force and **all** organisations that process personal data have until 25 May 2018 to comply
- The UK will have the GDPR post Brexit (or a variation thereof perhaps)…

Key GDPR changes

- Scope and applicability
- Accountability principle
- Data protection officer
- Lawfulness and consent
- Privacy notice requirements
- Enhanced and new data subject rights
- Data processor clauses
- Data protection impact assessments
- Personal data breach management and notification

Personal data breach management and notification

- Notify Information Commissioner's Office (**ICO**) of a data breach without undue delay and in any event within 72 hours of becoming aware of a data breach
- Notify individuals without undue delay of a data breach where data breach is likely to result in a high risk to the rights and freedoms of individuals
- Data processors – notify data controllers without undue delay of any data breach
- Log of **ALL** data breaches (irrespective of notification) maintained comprising the facts relating to the data breach, its effects and the remedial action taken to enable the ICO to verify compliance with Article 33

Understanding the cyber threat and reputational risks

- Individual's awareness of data protection is rising
- Data breach consequences could be significant
- New obligations on data processors to help data controllers with breach notification to regulators and individuals
- Information security is a specialist area – seek assistance!
- It is important to act quickly
- On-line activity is increasing and so is cyber crime …

When things go wrong…

- **Tesco**: The bank revealed that the “unprecedented” attack on its online accounts resulted in the loss of £2.5m : 8 November 2016
- **TalkTalk**: has issued with a record £400,000 fine by the ICO for security failings that allowed a cyber attacker to access customer data “with ease” : 5 October 2016
- **Royal & Sun Alliance Insurance Plc**: fined £150,000 by the ICO following the loss of the personal information of nearly 60,000 customers : 10 January 2017

Cyber security insurance

- Not all insurance will include provision for cyber crime
- Review current coverage – what is included and where are the gaps:
  - Regulatory investigations and audits?
  - Forensic examinations?
  - Notification requirements?
  - Remediation costs?
  - On-going support?
  - Directors liability?
- Increased liability caps and requirements in contracts
- Carve outs for indemnities

What this means for you…!

- Who is responsible for data protection compliance?
- What contractual provisions are in place with third party data processors?
- Are you acting as a data controller or data processor?
- What policies and procedures are in place to protect personal data?
- Do you have a data breach notification and management procedure?

Consequences of non-compliance

- The level of fines has increased
- Breach of the GDPR could lead to a fine of up to the greater of €20,000,000 or 4% of worldwide annual turnover
- An individual can bring a claim for damage and distress too

Data protection compliance is serious business!