



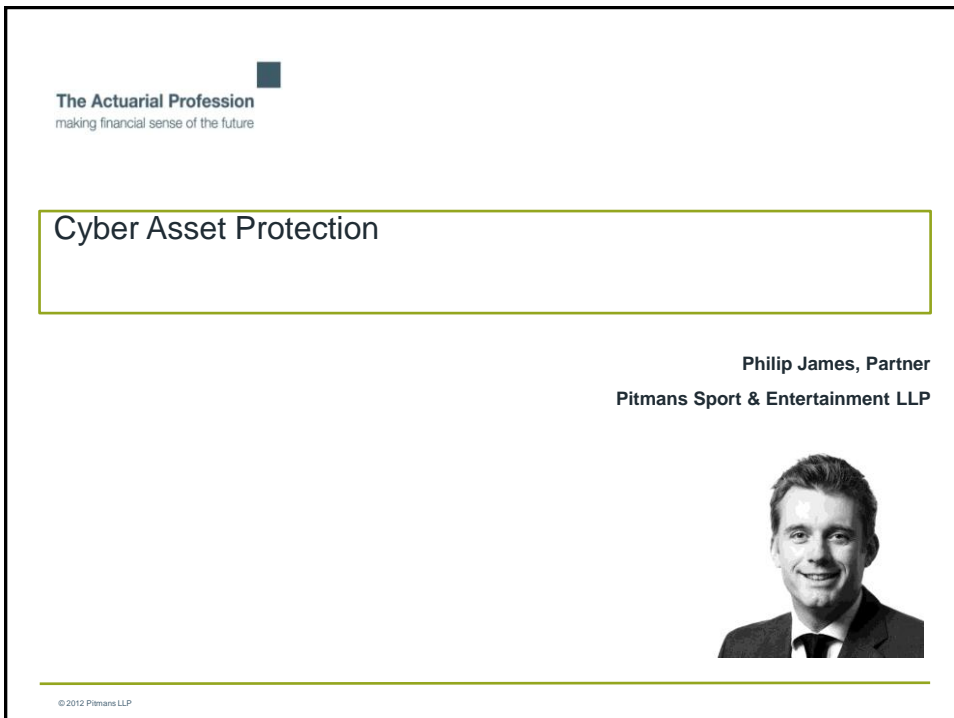
The Actuarial Profession  
making financial sense of the future

**Cyber Asset Protection**

Actuaries and the Law  
2012

13 September


© 2010 The Actuarial Profession • www.actuaries.org.uk



The Actuarial Profession  
making financial sense of the future

**Cyber Asset Protection**

Philip James, Partner  
Pitmans Sport & Entertainment LLP



© 2012 Pitmans LLP

## Why Should Trustees Be Concerned?

- Trustees are data controllers
- Trustees are in the spotlight
- Penalties (and possible class actions)
- Repercussions: cost and reputation
  - Loss of data and reconstitution
  - Notification
  - Re-calculation
  - Fraud and criminal use

© 2010 The Actuarial Profession •  
www.actuaries.org.uk

2

## Common Stumbling Blocks

- Member data: day-to-day handling
- Constant and accurate updating
- Trustee meeting and minutes
- Outsourcing to third parties
- Corporate transactions

---

## **What Powers Does the ICO Have?**

---

- New sanctions
- Criminal liability
- 'Name and shame' undertakings
- Enforcement Notices
- Investigative powers

---

## **What Data Subjects Can Do?**

---

- Civil action
- ICO complaint
- Pensions ombudsman complaint

---

## How to Comply (And Manage Risk)?

---

- Notification with the ICO
- Fair processing notices and consent
- Data processor agreements
- Policies and process
- Security policies and risk assessments
- Data security – 'prepare, protect and deter'

---

## The Fundamentals

---

- Responsibility for compliance
- Can't delegate responsibility!
- Up to date notification in place with ICO
- Complying with the eight DP principles

---

## Data Protection Principles

---

- Fairly and lawfully
- For one or more specified purposes
- Adequate, relevant and not excessive
- Accurate
- Not longer than necessary
- In accordance with the rights of data subjects
- Appropriate measures
- Not transferred outside EEA

---

## Key Issues to Consider

---

### Personal Data

- Sensitive?

### Transfer outside EEA

- Safe Harbour (US)
- Model contract clause

---

## The Pensions Regulator

---

### Record Keeping Guidance

- Where problems – further investigations
- Regular testing

### Data Tests

- Common data
- Conditional data
- Numerical Information

---

## Statutory Record Keeping Requirements

---

- Pensions Act 1994, 2004, 2008
- Occ. Pension Scheme (Scheme Administration) Regulations 1996
- Occ. Pension Scheme (Disclosure Information) Regulations 1996
- Pers. Pension Schemes (disclosure of Information) Regulations 1987
- Occ. Pension Schemes (Internal Controls) Regulations 2005
- Data Protection Act 1998
- The IORP Directive

---

## **Cyber: The Current Theatre**

---

- Davos WEF
- Cyber Attacks – one of the Top 5 Global Risks\*
- No organisation immune
- War 3.0 now fought in cyberspace
- Benefits of improved security

---

## **Cyber: It's Multi-Disciplinary**

---

- Insurance
- IT Security
- Employees
- PR

---

## Cyber: The Issues

---

- Prevention and resilience
- Brand equals trust
- Hope for the best, prepare for the worst
- Information as an asset
- Confidentiality

---

## Cyber: The Solution

---

- Audit and identify risk areas and vulnerabilities
- Incident response
- Have a strategy
- The human element (training, policies and process)
- Protect your IP
- Appoint a DPO (senior or board executive)



---

## **Cyber: Challenges**

---

- Chains of supply
- Due diligence (e.g. The Cloud)
- Accreditations (PCI DSS)
- Data portability and exit management
- Contract framework and insurance
- Prepare a contingency incident response plan

---

## **What's Ahead and Current Trends**

---

- New Draft EU Regulation published in January
- Fines up to 2% of annual worldwide turnover
- DPs and DPOs
- Notification compulsory within 24 hours of breach
- Privacy by Design and Default

---

**Questions or comments?**

---

