

## Holistic Information Security - Understanding the Threat, UK/EU Law and Practical Steps for Risk Reduction

**SRA approved course – 1.5 hours CPD credit**

Keeping assets, personal, business and financial information private and safe is a major challenge in today's world. Threats include insecure computer systems, covert surveillance devices, corporate espionage, identity theft and many others. These threats are of particular concern for lawyers and law firms, to protect information and assets of both clients and the firm.

*Holistic Information Security* is a new and exclusive course designed to help you understand and mitigate these risks. An informative, interactive and engaging 90 minutes, providing you up-to-date, practical information security advice from both legal and business perspectives. Our instructors are experienced professionals from the security and legal communities.



**“This is a very well-planned and presented course, which covers a range of technical information, yet delivers it in an interesting, but easy to follow, step by step manner.”**

SRA assessor 2009

### Course outline

#### Part I - Evolving Threat Environment

- FB Holistic security approach
- FB Major threats – risks and mitigations
  - FB Human – insiders, predictable behaviour traits
  - FB Computers – access controls, malware
  - FB Mobile devices – mobile phones, PDAs
  - FB Surveillance devices – latest technologies
  - FB Other threats

#### Part II – UK / EU Legal Environment

- FB Data protection
  - FB EU law – Data Protection Directive, Privacy and Electronic Communications Directive
  - FB UK law – Data Protection Act 1998, secondary legislation
  - FB Surveillance – employees, others
  - FB Information security
  - FB Access to data
- FB Illegal access to data – communications, stored data

#### Part II – UK / EU Legal Environment cont.

- FB What is illegal?
- FB UK law – Regulation of Investigatory Powers Act 2000, Computer Misuse Act 1990
- FB EU law – Information Systems Attacks Decision
- FB Data breach reporting
  - FB What to report (or not)
  - FB How to decide

#### Part III - Best Practices and Steps for Risk Reduction

- FB Risk assessment model
- FB Best practice guidelines on:
  - FB Security policy
  - FB Document handling
  - FB Computers
  - FB Passwords
  - FB Software
  - FB Mobile devices
  - FB USB devices
  - FB Surveillance devices

Course includes full notes, *Best Practice*, *Warning Signs*, *Drilling* and *SpyPhone Software* guides.

**How to book** - Check out <http://www.faberbrent.com> for upcoming dates and more information.  
- Contact FaberBrent to arrange either dedicated in-house or external courses.

