

# Introduction to Information Security

## Training Course



When we talk about assigning budget to Information Assurance or security within an organisation people often ask, how can I measure the return on my investment? At SBL we ask how can you afford not to invest in training your employees about the importance of securing your data?

Just as you would not contemplate entering a building site without a hard hat, you should never contemplate putting data that has been entrusted to your care at risk.

From 6 April 2010 the Information Commissioner's Office can impose its own penalties (without recourse to the courts) of up to £500,000 where a serious breach of the principles occurs. Before a monetary penalty is imposed, you will be issued with a notice of intent by the ICO. You will then have the opportunity to provide the Commissioner with details of the specific circumstances surrounding the alleged breach, as well as the financial impact of any proposed penalty.

SBL's Introduction to Information Security course is aimed at personnel who are responsible for maintaining the integrity, availability and confidentiality of information within your organisation.

The course will provide you with a clear understanding of the principles behind Information Security, the threats, the risks and the recommendations. The knowledge you acquire will allow you to focus resource on the critical areas in the fight to secure your information.

**For further information or to book a place on this course email [training@softbox.co.uk](mailto:training@softbox.co.uk) or contact your SBL Account Manager on 01347 812100.**

**Duration:** 1 day

**Location:** SBL HQ, York - or we can deliver a course at your site on request

**Content:** This course explores the **Basic Pillars of Security:**

*Technical*  
*Procedural*  
*Personnel*  
*Physical*

SBL's security cleared Information Assurance specialists will deliver a bespoke course, tailored to the needs of your organisation. Please see overleaf for details.



**Simply select the appropriate content and we will tailor the course to your needs.**

## The Need for IT Security?

- IT security as part of overall company security policy
- Confidentiality, integrity and availability
- Losses due to a lack of security
- Computer crime
- The changing IT environment

## Meeting the Need

- Starting point
- Writing a Security Policy
- Roles and responsibilities
- Management and security administration

## IT System Threats

- The types and the sources of threat
- The types of vulnerability - computer and communication

## IT Risk Analysis

- Strategic and tactical risk assessment
- The role of management
- Impact on business
- Cost of IT security vs cost of potential losses

## Legal Framework

- Legal jurisdiction for national/international commerce
- Civil and criminal legal structures
- UK Data Protection Act 1998
- UK Computer Misuse Act 1990
- Freedom of Information Act 2000
- Record keeping requirement
- Human Rights Act 1998

## Principles of Conduct

- Codes of conduct
- Rights and responsibilities of people
- Employment issues
- Ethical considerations

## Security Standards and Procedures

- Security standards - ISO27001
- Evaluation criteria - Orange book, ITSec, Common Criteria, FIPS, CAPS
- Certification - Procedures, Products/services, People, Certification bodies
- Understanding Impact Levels

## Counter Measures

- Technical counter measures
- Procedural counter measures
- Personnel counter measures
- Physical counter measures

## Internet and Intranet Issues

- CIA - NR & A
- Internet and intranet considerations
- Securing internet and intranet connections

## Business Continuity Management

- Business continuity management and process
- Business continuity and impact analysis
- Writing and implementing continuity plans
- Business continuity planning framework
- Testing, maintaining and reassessing the plans

## Analysis and Post Incident Reviews

- Responding to security incidents and malfunctions
- Reporting security incidents and weaknesses
- Reporting software malfunctions
- Learning from incidents
- Disciplinary process