

# IT Law for IT Managers

## Aim

The aim of this Course is to help delegates develop an understanding of the nature of electronic data as it relates to the management and litigation readiness of a computer network.

## Audience

The target audience for this course is anyone whose job function it is to manage and prepare any business concern for litigation readiness.



## Introduction

- Who is the IT Manager - Job function not necessarily Job title
- The unique role of the IT Manager
- The myth about restrictive role to technical issues on the Network
- The ideal - prominent member of the board in the design and implementation of corporate policy
- Traditional Role of the IT Manager debunked

## Tangential laws affecting liability in the running of a Computer Network

- Rule of law
- Human Rights protection for the User
- Privacy laws
- Freedom of information Act
- Data protection Act
- Safe harbour principle
- Criminal law
- Espionage
- Hacking - No hack back
- Compliance regulations e.g Sox

## Resolution

Use of log on Banners  
Employment contracts properly drafted- liaise with HR  
Regular IT audit

## Why it is important to understand the role of law in a computer network environment?

- Paradigm shift from paper documents to digital documents - statistics
- Emails
- Internet
- File sharing
- Security and corporate espionage
- Human resource
- Health and safety
- Document custodians
- IT Budgets
- Tendering for business - 3rd party requirements about the network

## Criminal Law Provisions – UK

- Computer misuse Act
- Terrorism Act
- Telecommunications Act
- Data protection Act
- RIPA
- WEEE
- PACE

## Criminal law Provisions – USA

- CFMA
- ECPA
- Other Title 18 offences

## Civil law provisions

- Human Rights Act
- Copy rights design and Patents
- Distant selling directives
- Contract and Commercial law

## Electronic document discovery

- Electronic document recovery
- Statutory compliance – emails see Sox
- Document archiving
- Online repository

## Examine the OSI model – Potential problems at each layer

Layer	Responsibility
7	This layer represents the end user application - http, ftp, smtp or telnet - what can possibly go wrong -
6	Handles formatting, compression, encryption and presentation of data to the application e.g. SSL and TLS
5	Deals with management and setup of sessions between computer applications
4	Deals with data transport and error control
3	Routing packets between networks - routers
2	Data layer from one host to another
1	Physical link, cabling and binary transmission of data.

## Reporting a Computer crime

- Why report
- Before you report
- Impedements
- Police agent
- Board concerns

## **Working with law enforcement**

- Preliminaries - Questions to ask
- What reports to provide to the police
- What you cannot do

## **Investigating computer misuse**

- Working with the victims
- Legal pitfalls
- Technical pitfalls
- Best practice

## **Auditing Network Devices**

- Switches
- Routers
- firewalls
- IDS

## **Auditing Stand alone computers**

- What are you looking for?
- Where to look
- Know your limitations

## **Auditing relevant servers**

- Domain controller
- File server
- Print server
- Database server
- AV server
- Honey pot or sandbox
- Know your limitations

## **The incident response Team**

- What is an incident response team
- Role of the incident response team
- Setting up an incident response team
- Responding to an incident
- Designing an incident response protocol
- Implementing an incident response protocol

## **The Litigation ready Network**

- What does this mean?
- Proactive protocol for litigation readiness
- Who is a document custodian?
- Expectations of a document custodian
- What document to protect and in what format
- What is a litigation hold
- What is spoliation
- Conducting a document search
- Producing responsive data
- Privileged documents
- Redaction

## **Expert relationships**

- Assisting the corporate board
- Working with external consultants
- Working with in house counsel
- Assisting the police

## **Life circle of computer evidence- overview**

- Evidence identification
- Evidence collection
- The digital evidence scene – Locards principle
- Evidence analysis / filtering
- Evidence preservation – chain of custody
- Evidence presentation.

## **Testifying as a witness in court**

- Do's
- Don'ts

## **Intended Learning Outcomes**

On successful completion of this course a delegate will be able to:

### **Knowledge**

- Recognise the need to design and implement a digital evidence protocol within and IT environment
- Understand the need to design and implement an incidence response team
- Recognise the legal implications of conducting a computer investigation
- Understand the full life circle of digital evidence within a computer network
- Recognise the risk involved in hasty investigations

### **Skills**

- Conduct a gap analysis of corporate requirements in digital data security
- Design and implement an incidence response protocol with appropriate team members.
- Liaise with in-house counsel , external consultants and the police
- Testify as an expert witness or document custodian in court.