

IT SECURITY & INCIDENT RESPONSE

24-25 January 2008
12-13 November 2008

Location: Thames Valley, UK

This intensive two-day programme provides delegates with a thorough understanding of the value of effective response measures in handling incidents of IT-facilitated crime and misuse. Combining theory-based lectures and discussions with a unique one-day investigative simulation, the course is designed to give participants greater confidence in their decision-making and also in their approach to developing incident response strategies. Suitable for general security managers, consultants, investigators, line managers and IT staff.

CONTENT

IT Threats to the Organisation
Approaching an Allegation of IT Misuse
Legal Issues Relating to IT Crime and Misuse
Analysing the IT Scene of Crime
Utilising the Power of the Courts
in Cases of IT Misuse
Investigative Resources
Managing IT Evidence
Reaching Investigative Resolution
Investigative Simulation: IT Misuse in the Organisation

IT Threats to the Organisation: Overview of potential IT-based threats to your company (internal and external); how threats are made manifest; how to identify and read the warning signs; threat origins

Approaching an Allegation of IT Misuse: How to correctly manage an allegation of IT misuse; the chain of command and coordination; operational security; the roles of group legal and HR; how to liaise with external agencies; how to establish secure exit procedures when employees are suspended or dismissed

Legal Issues Relating to IT Crime and Misuse: How the Law and legislation should be considered, and their application; the Computer Misuse Act 1990 and relevant criminal statutes/civil redress; overview of employment law (including: RIPA; the Human Rights Act; Data Protection Act)

Analysing the IT Scene of Crime: How to devise and carry out an investigation; who to involve; building a response team; securing the situation; containment measures; overview of analytical methods

Utilising the Power of the Courts in Cases of IT Misuse: How the Law can assist (and sometimes challenge) your investigation; overview of legal process; search warrants; how to avoid mistakes that can trap the unwary

Investigative Resources: How to request and deploy technical and human resources; overview of tools and techniques to recover and restore data; review of the software used to recover evidence from storage media; how to present data for review; how to handle, collate and store admissible computer evidence (thus maintaining evidential continuity and relevance)

Reaching Investigative Resolution: Bringing the investigation to a close; how to determine the “end game”; the role of the expert witness; an overview of methods used to present IT-based evidence at tribunals/court (with a view to negating contested cases)

Investigative Simulation: IT Misuse in the Organisation: A real-life simulation that asks delegates to manage and resolve a work-place computer-based crime. This friendly but competitive exercise requires that teams filter and apply all learning from the course to guarantee successful resolution.

- **£1400 (plus Value Added Tax @ 17.5%)**

Includes 2 nights full board accommodation

For more information, or to make a booking, please contact us on:

Telephone: +44 (0) 118 984 1040

Fax: +44 (0) 118 984 5060

Mobile: +44 (0) 779 911 2197

E-mail: janetward@arc-tc.com

www.arc-tc.com