

Introduction to Computer Forensics

Today, being prepared to handle a computer security incident has become a top priority for most system administrators. As businesses increase their online presence and their dependency on information systems' assets, the number of computer incidents also rises.

Organisations must develop and implement security plans and controls in a proactive effort. Second, they must work to ensure that their plans and controls are effective by continually reviewing and modifying them to guarantee that appropriate security is always in place. Finally, when controls are bypassed, either intentionally or unintentionally, organisations must be prepared to act quickly and effectively to minimise the impact of these lapses.

The prime objective of these security measures is to prevent an operational security problem from becoming a business problem that impacts revenue and services. Administrators can plan a response to incidents and minimise any negative impact to a business. Waiting until an incident has occurred is naturally too late to begin planning how to address such an event. Incident response planning requires maintaining both administrative and technical roles. Each party must be familiar with the other's role, responsibilities, and capabilities.

The Incident Response course lasts for one day and is designed to train both IT and non IT staff in the procedures required for Incident Response.

Delegates will be shown how to handle potentially criminal or damaging digital evidence in accordance with the current UK legislation and the ACPO guidelines thereby preserving the continuity of evidence and avoiding contamination of that evidence.

Incident Response and Computer Forensics course contents:

Types of computer crimes

- The current threat
- What constitutes computer crimes
- Why you should be concerned about computer crime
- Reasons for Forensics
- Civil, criminal and internal investigations

Incident procedures

- Types of evidence
- Processing the Incident
- Legal evidence acquisition
- Shutdown vs. pulling the plug
- Why it is important for a controlled boot when required
- Evidence handling procedures and issues
- Chain of custody
- Removal transportation and storage

Incident response

- Planning before the incident occurs
- What you will need
- Who should be on your response team
- Step by step computer incident response procedure

Working with the Law

- ACPO guidelines
- Civil Vs criminal investigation
- UK Laws and rules of evidence
- Civil litigation and restitution
- Legal Issues

Presenting the evidence

- The status of the expert witness
- The role of the expert witness
- Expert witness testimony

Head office:

IntaForensics Ltd

1 The Courtyard, Eliot Business Park,
Nuneaton, Warwickshire, CV10 7RJ
DX 16453 NUNEATON
Tel: 0845 0092600 Fax: 0845 0092601