

Digital Forensics

Despite precautions, it is possible that security incidents or system compromises will occur. Security incidents can originate from a number of threat agents including trusted internal employees, third parties or motivated external attackers. An immediate response is necessary when dealing with any security breach. A methodical approach and controlled reaction to an incident can mean the difference between complete recovery and major disaster. IRM's Incident Response services can help ensure incidents are effectively managed and contained.

As part of an incident response, a digital forensics investigation is often required to determine the source of a compromise, the extent of the compromise or simply to gain evidence that could be used during legal proceedings or employment tribunals.

IRM's digital forensic experts routinely access IT systems and networks to recover residual evidential data and determine whether it has been tampered with, deleted or damaged. The process is performed following specific guidelines in line with Association of Chief Police Officers (ACPO) regulations. Once seized, the data is imaged and examined.

At all stages evidential integrity remains and can be utilised in the event of legal action. Fundamental to the correct handling of an incident is the creation of an incident response strategy, which should be a strictly documented process. Such processes require management and implementation by specific individuals.

IRM forensic examiners have experience in managing various scenarios and dealing with diverse types of systems digital evidence. Evidence relating to an incident can be retrieved from many devices which include:

- Servers / Desktops / Laptops
- Backup Media
- Portable Storage Media (USB devices, Zip drives)
- PDAs / Mobile Phones
- Digital Cameras
- Network Traffic & E-Mail Communications

IRM's forensic services can be used to provide expert assistance with external and internal incidents:

- Data recovery
- Fraud investigations
- Violation of corporate policy (e.g. data theft, internet usage, discrimination)
- Employment tribunals and legal proceedings
- Child pornography

IRM will provide a full report containing details of the investigation and evidence retrieved, as well as an executive summary.

About IRM

Information Risk Management Plc (IRM) is a vendor-independent information security consultancy. Founded in 1998 to work alongside global enterprises in understanding the security risks inherent in an increasingly interconnected business environment, IRM has become a leader in penetration testing, risk assessment and security auditing.