

Incident Response

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.

If an incident has occurred or is detected, the incident response procedures and any subsequent forensic investigation processes used are crucial. Correct procedures ensure integrity is maintained when evidence is being located and extracted from applicable devices and media. Even the most hidden, deleted or encrypted information can be traced by experienced Digital Forensics investigators.

IRM's services include direct Incident Response and pre-incident preparation. Whilst it might be infeasible to predict an incident, strategic planning based on an organisation's business operations could be achieved to minimise the impact.

Incident Response Planning

The scope of an Incident Response Plan could be limited to critical systems within the IT estate or cover the entire organisation to construct a full Business Continuity Plan. Having a plan prepared in advance, which is activated when necessary is essential.

IRM can assist in:

- Incident management; the setup and organisation of internal Incident Response teams
- Outlining guidelines and procedures for responsive actions based on common scenarios related to the business
- Providing user training for best practice and containment measures (e.g. computer virus outbreak, internal or external intrusion, and preserving digital evidence)
- Ensuring adequate levels of monitoring are available within the organisation, including logs and backup storage management

Incident Response

Internal incident response teams are not always available, specialist skills are limited, or there might be a requirement to have an independent third party opinion on actions taken by staff members during an incident either for legal or compliance reasons. This may establish the need to:

- Review the precautionary actions taken by the company staff and identify whether any additional procedures were required (e.g. dismissal of a disgruntled system administrator)
- Detect and identify intrusions and affected systems. For instance, examine critical servers for the presence of any malicious software
- Devise appropriate containment measures
- Analyse any malicious software
- Thorough review of network traffic, system logs, monitoring solutions reports, and system backups
- Conduct an impact assessment
- Perform forensic analysis (refer to IRM's Digital Forensics service)

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.