

## War Dialling

If your organisation relies on modems and PABX interfaces to provide telephony services and remote access to your employees and customers, these could provide backdoors into your network for remote attackers.

IRM's War Dialling Assessment evaluates the security of all the telephony components making up that environment using proven methodologies to assess the security of the architecture. The result is a clearer view of the vulnerabilities that may be present.

IRM will identify all potential modems, fax machines, PABX interfaces and rogue devices across a range of telephone numbers, and will highlight possible risks and exposures related to the presence and misconfiguration of these telephony devices that would allow an attacker to gain access to sensitive information such as customer data.

A complete War Dialling exercise includes the following phases:

- **Environment Mapping**

IRM will gather information about all devices located across the range of telephone numbers related to the organisation. This information is gathered through manual and automated telephony based scans, using specialist war dialling software.

- **Component Analysis**

Each of the identified devices will be examined with a view to understanding the correct operation of each element. The elements will also be considered in detail within the wider context of the environment as a whole, assessing its legitimate or rogue nature.

- **Vulnerability Identification and Analysis**

The security requirements of the telephony presence are assessed and potential gaps between the requirements and the implementation are identified. The following are considered core components of this analysis yet other areas of interest may be considered as appropriate to the environment in question:

- Authentication assessment
- Security of access to data
- Administration interfaces
- Distinction between rogue and legitimate devices.

- **Deliverables**

IRM will deliver a formal report including an executive summary, a risks and recommendations table detailing the high level results of the assessment and a detailed description of each issue discovered including remediation advice.

## 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.