Fields **Associates**
Litigation Consultants

Why Your Commercial Clients Need a Forensic Readiness Programme

Over the last three decades, technological advancement has grown at a truly prodigious rate and, with a variety of devices now essential to the everyday business of the vast majority of organisations worldwide, it is no way surprising that most companies have practicable disaster recovery/contingency plans in place. Whilst such policies are well suited to addressing matters that may arise as a result of events which, whilst unlikely, are potentially catastrophic, little consideration is given to polices designed to address events which, whilst not necessarily disastrous, can be disruptive and occur far more regularly.

Common examples of such incidents include, but are in no way limited to, disputed payments, employee misconduct and the need to assist law-enforcement agencies with their investigations. In each of these – and many other – instances, it will almost certainly be necessary to provide and/or utilise some form of digital evidence; hence the need for companies to have an actionable Forensic Readiness Programme in place.

Digital evidence is notoriously volatile and can easily become worthless if handled incorrectly. In spite of this, few organisations have plans in place to allow them to preserve, identify and collect digital evidence in such a way as to ensure that it would be able to stand up to the vigorous tests to which it would be subjected in legal proceedings. This, of course, could prove costly should a company find themselves involved in various types of civil proceedings.

The need for organisations to provide various bodies with admissible digital evidence will not only apply when they are directly involved in procedures either. Should a crime take place at a business, for example, then they will almost certainly be required to provide law enforcement agencies with video recordings or files that may relate to matters. Furthermore, institutions operating within the public sector are required to retain a variety of documents in order to adhere to stipulations set out within the Freedom of Information Act 2000. Financial and other institutions must also hold documentation on clients for set periods of time, also – something which, due to convenience, they are now likely to do through digital rather than physical means.

In order to form a workable Forensic Readiness Programme, organisations will need to utilise the skills and knowledge of their senior managements, legal advisers such as solicitors or digital forensics experts and their own systems administrators. The plan should focus on risk assessment whereby it will be identified what legal threats the organisation is most likely to encounter, the type of data that they are most likely to need to disclose as a result of these and cost-effective ways of backing up and securing this data so as to ensure that, should these records need to be accessed, this does not affect the organisation's day-to-day activities.