

Industrial espionage a big threat

Mercury Reporter

INDUSTRIAL espionage – stealing trade secrets, theft of intellectual property and databases, and leaking confidential information – is not just the stuff of Hollywood movies.

Alan Carey, from South Africa's Justicia Investigations, says that in a highly competitive environment and tough economic times, it is far easier and cheaper to expropriate information than to innovate. Leaked technical specifications could negate a massive investment in being the first to market with a new product. A copied customer database could shrink a market share advantage overnight, he warns.

Carey has noted an upsurge in the number of calls from companies requesting debugging services. "We are getting between three and five calls a week from large corporates," he said.

Leo Nardi, Justicia's technical manager, says these calls are not only coming from South Africa, but throughout Africa from Botswana to Tanzania, as the rush to conquer African markets gathers momentum.

Figures released by Ernst & Young (SA) suggest that industrial espionage is a \$67 billion-a-year (R800bn-a-year) industry.

Nardi says the information and communications technology industry is gearing towards more data storage, but has fallen behind in adopting suitable security protocols or in configuring the equipment correctly to minimise risk.

Companies need to tackle industrial espionage. They should adopt both reactive and proactive measures, such as having their premises swept regularly and adopting an anti-bugging policy.