Spies at the water cooler

Spooks cash in as companies snoop on each other like never before

GRAEME HOSKEN

INDUSTRIAL espionage is at an all-time high in South Africa, with an increase in requests for debugging services coming from gaming firms, research and development companies and those tendering for multimillion-rand contracts.

Driving fear in the world of Spy vs Spy are tough economic times and the ease with which South Africans can buy listening devices online.

The unregulated eavesdropping industry had led to an apparent surge in spying by businessmen on one another, according to Justicia Investigations, a company specialising in surveillance.

Its operations director, Alan Carey, said the number of inquiries about debugging services had increased rapidly since November, indicating a spike in South Africans spying on each other.

"In the past we received maybe two inquiries every fortnight. Now we are receiving at least three a week.

"The majority are from the gaming industry, research and development firms, cellular communication companies and businesses bidding for tenders," he said.

Eavesdropping in the gaming industry was being fuelled by the suspicion of hacking of computer

● Continued on Page 2

Industrial espionage helps win tenders

● From Page 1

systems to manipulate online betting, he said.

"As you can imagine, the losses would be astronomical."

The motive for industrial espionage was competition for tenders, Carey said.

"Fears are over hacking; the protection of information and communication technology and intellectual property is high. CEOs, company presidents, managers and now the government are becoming aware of the cost of this very real threat and are worried."

Carey said though figures released by Ernst and Young suggested industrial espionage was a $67-billion-a-year industry, losses were often difficult to quantify.

"Reasons for the 'loss' of a tender are often unknown. Only when businesses are shut down through continued tender losses to competitors are the true reasons learnt." He said driving the concerns about industrial espionage in South Africa was a lack of regulations over the sale of eavesdropping devices. They could be bought for as little as R300 over the counter, with no questions asked.

A search on online auction site Bid or Buy came up with an array of devices, from ashtrays fitted with listening devices to specialised tracking watches, conventional lamp-fitted bugs and super-sleuth glasses.

Recent spy scandals that have rocked the country include:

- The Al-Jazeera spy cables, which revealed, among other things, the government's concerns about Iran using official and unofficial channels, including front companies in South Africa, to beat sanctions;
- The spy cables' revelation that blueprints for the Rooivalk helicopter had been stolen by a known foreign intelligence agency, and there had been theft of missile systems and intellectual property at several state-owned enterprises;
- The cables said France and the US had been "working frantically" to influence the bidding process for expansion of South Africa's nuclear-energy capacity;
- A breach of the police website in 2013, in which hackers stole the identities of 16 000 whistle-blowers and complainants; and
- Revelations by US whistle-blower Edward Snowden that, during the 2009 London G20 summit, the UK government spied on dignitaries, including South Africans, relaying information in real time to delegates to strengthen their negotiating positions. Danny Myburgh, managing director of Cynare, The Computer Forensic Lab, which supplies forensic services, said the biggest threat to industry was computer spyware, which, unlike listening devices,

> "Eavesdropping devices for as little as R300

went undetected.

"Unlike normal listening devices, which have to be installed through physical access, cyber spyware can be installed from remote locations, monitoring not only computers but cellphones.

"The risks posed are dire, especially in relation to a country's critical infrastructure such as energy, security and crisis response systems. Trade programmes are also at grave risk," he said.

The establishment of a national cyber security framework was long overdue, Myburgh said.

"One of the biggest threats to businesses and the government is the lack of experience in responding to such threats, with no established reaction plans in place." Cyber crimes expert Haroon Meer warned that the government was at as much risk as private business.

"Knowing a country's economic development strategy is priceless. Knowing where mining companies, energy utilities and telecommunication companies are going to operate and plan developments is crucial," he said.