Justicia reports increased calls for debugging services

By Staff Writer 5 May 2015 | Categories: Press Release

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

Alan Carey, Operations Director of Justicia Investigations, South Africa's leading private investigation company, says local companies are vulnerable to losing important data, which will not only impact negatively on their bottom lines and the viability of their businesses, but could also seriously damage their corporate reputations and brands.

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.

Over the past few months Justicia 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 says.

Leo Nardi, Justicia's Technical Manager, adds that these calls are not only coming from South Africa but extending upwards throughout Africa from Botswana to Tanzania, as the rush to conquer African markets gathers momentum.

Finding concrete statistics to back up Justicia's observations is not easy. Both globally and locally, underreporting is rife with companies preferring not to disclose that they have been the targets of industrial espionage for fear of losing customers.

In May last year, Randall C. Coleman, Assistant Director, Counterintelligence Division of the American Federal Bureau of Investigation (FBI) told a Senate Judiciary Committee that estimated losses from economic espionage were thought to run into tens or even hundreds of billions of Dollars annually.

In 2010, the FBI's Counterintelligence Division created a specialised unit called the Economic Espionage Unit to focus on this area. This unit's caseload has sky rocketed with the number of economic espionage and theft of trade secrets cases growing by more than 60 percent between 2009 and 2013.

Another interesting statistic comes from American law firm O'Melveny & Myers - the number of trade secret cases in US federal courts doubled between 1988 and 1995, doubled again from 1995 to 2004 and is expected to double again by 2017.

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

Perhaps the best indicator of the surge in illicit surveillance is a dramatic increase in the sales of bugging devices and equipment. Although, again, there are no South African statistics, but the US State Department estimates that over 700 000 eavesdropping devices are sold each year.

With this comes an inevitable increase in the need for "debugging services" – and, in South Africa, a dramatic rise in the number of fly-by-night operations marketing them.

Carey admits that the security industry has a bad reputation and that there are a number of "one man operations and jack of all trades" offering services that require significant experience and expertise as well as sophisticated equipment.

"Justicia prides itself on 25 years of investigative integrity. We have a team of professionals who are experts in their respective fields and have a combined experience of more than four decades." he says.

In addition to experience, he adds, Justicia is investing extensively in new equipment and training, as bugs are becoming smaller, more sophisticated and increasingly difficult to detect.

In addition to constantly updating equipment, Justicia is moving with the times by extending its range of services and has partnered with an ICT company to ensure a holistic debugging approach

Information and Communications Technology (ICT) infrastructure.

Nardi says that it is evident that the ICT industry is gearing towards more data storage and throughput. Many companies invest in good equipment but then fall behind in adopting suitable security protocols or in configuring the equipment correctly to minimize risk. If you do not take into account your computers, then you are ignoring a large part of your risk profile. Carey adds that companies need to tackle industrial espionage and adopt both reactive and proactive measures. "We encourage clients to introduce debugging policies. In addition to protecting and limiting access to confidential information,

a debugging policy should help managers to recognise the signs – from the irregular conduct of an employee to physical clues of bugging activities having taken place. Companies also need to have their premises swept for bugs regularly."

At the end of the day, he stresses the importance for a company to build a strong relationship with a trustworthy service provider when it comes to something as sensitive as this. "At Justicia, we guard our credibility and professionalism carefully. In the corporate world, we are dealing with decision makers in business and know the value of discretion and building ongoing trust relationships."

Captions: Operations Director of Justicia Investigations, Alan Carey sweeps an office looking for bugs using the latest technology.

Equipment – Some of the sophisticated technology that Justicia Investigations is equipped with to ensure they offer their clients the most comprehensive service.