



# TSCM vs INSIDER THREAT

An Insider Threat is a malicious threat to an organisation that emanates from people within the organisation, such as PAs, CPOs, Security Personnel, IT Managers, Employees, Contractors or Business Associates. The mentioned individuals typically have access to inside information relating to the organisation's Intellectual Property and Information Security Practices or Information Assets and have 24/7 access to Executives. This could pose a significant risk and security exposure, as these individuals could be compromised to potentially assist in planting of eavesdropping ("bugging") devices within the Business environment.

In South Africa, Corporate Espionage is rife. Rival companies and insider threats are using malicious tactics to gain access to and obtain Intellectual Property, that in most instances are key to the success of the organisation. It is, therefore, of the utmost importance to understand that proactive TSCM measures are key in countering Corporate Espionage. This was substantiated when ACS visited and met with all the key TSCM delegates and industry leaders at the Milipol Exhibition, held in Paris in November 2019 (<https://en.milipol.com/>).

The threat posed by Corporate Espionage is real and imminent. TSCM is an extremely important step towards proactively protecting Intellectual Property and Information Assets owned by organisations.



Kind Regards  
 Riaan Bellingan  
**ADVANCED CORPORATE  
 SOLUTIONS cc**  
 1995/051218/23

Tel: +27 12 349 1779  
 Fax: +27 12 349 1789  
 Cell: +27 82 491 5086  
 E-mail: [riaan@acsolutions.co.za](mailto:riaan@acsolutions.co.za)  
 Website: [www.acsolutions.co.za](http://www.acsolutions.co.za)

TSCM | "Debugging" Specialists | 25 Years of Service Excellence (1995 - 2020)

