

Other TSCM Services

In-Place Monitoring

Designed to provide protection during sensitive meetings held in non-secure locations such as hotel suites, conference rooms or convention facilities. In-place monitoring consists of an electronic and physical inspection of the facility and adjacent areas prior to the meeting, and electronic monitoring while the meeting is in progress.

Pre-Construction Survey

Designed to detect and correct technical and physical security vulnerabilities in areas undergoing construction or remodeling. Our service includes meeting with the building contractors, blueprint studies and on-site visits to monitor work in progress.

Pre-Occupation Survey

Prior to moving into your new offices let us conduct a comprehensive sweep of your key areas to confirm that no devices have been installed in the build out phase, we will establish a baseline that can be invaluable when used as a reference for future.

VIP Support

Incorporating many aspects of the TSCM survey, this service provides protection for traveling executives and dignitaries. We help ensure that personal and proprietary information remains secure during travel away from home or regular place of business.

RISK3

TSCM
Computer Forensics
Incident Response
Data Recovery
Audio Forensics
Litigations Support

Technical Surveillance Countermeasures (TSCM)

Protecting the Spoken Word in Asia Since 1992

RISK3 CONSULTING LIMITED



RISK3 CONSULTING LIMITED

21/F., The Strand
49 Bonham Strand East
Sheung Wan, HKSAR

Tel.: (852) 2815 2025
Fax: (852) 2815 2024
E-mail: info@risk3.com

24 Hr Crisis Response:
Alan Jeffries: (852) 9103 1852
Fred Chan: (852) 9452 9676

DISCLAIMER:

The information on this leaflet is provided with the understanding that the authors and publishers of this information are not intending to render legal or other professional advice and services. No client relationship is established from making general information available on this material. None of the information on this material should be used as a substitute for consultation with competent advisors that are able to consider the application of any general information to your specific situation.

All Rights Reserved ©

Safeguard Your Critical Information

INFORMATION, it as been said, is one of the most important assets of any business, and the need to **prevent** the unauthorized disclosure or interception of confidential information or intellectual property cannot be overstated. The techniques used to obtain such information can be many and varied, senior executives need to be aware of the real and potential dangers of allowing important information to fall into the hands of unauthorized persons.

Industrial espionage and illegal information gathering is big business. Global companies that are eager to gain an edge against their competitors are going to great lengths to seize information that could give them a competitive advantage; our experience has shown that the Asia business sector is highly exposed to such illicit practices. Industrial and commercial spies, competitors, disgruntled employees, activists and many others with a wide range of purpose have a large diversity of easily obtainable devices and techniques at their disposal.



The Threats

At Risk3 we define eavesdropping as the unlawful interception of data in any form be it audio, visual and/or written information.

Most technical methods of information gathering are virtually impossible to identify without the use of advanced electronic detection equipment and the employment of highly trained personnel.

The Risk3 TSCM Survey

Electronic eavesdropping is devastating to any business; proactive countermeasures not only mitigates the risk, **it satisfies due diligence and management fiduciary responsibilities and, if conducted regularly, can aid in the attainment of business secret status within a court of law.**

The Risk3 TSCM Survey addresses espionage threats involving both specialized surveillance devices as well as standard equipments modified to act as listening devices. The Risk3 TSCM team reviews your specific circumstances and formulates a strategy to "sweep" the areas that are most susceptible to an eavesdropping attack.

Our Commitment

In addition to real expertise, The Risk3 TSCM team is fully equipped with state-of-the-art countermeasures equipment, which ensures the efficiency and effectiveness of our electronic inspection. Upgrades to our software and equipment are continually implemented in order for us to maintain the edge in technology advancements of today's eavesdropping devices and equipment.

In order to keep up to date with current trends and techniques, Risk3 invests both time and capital in new and updated equipment as well as technical training in the latest eavesdropping techniques and the necessary countermeasures to isolate and nullify these threats.

The Process

The Risk3 TSCM Survey generally includes at least the following:

- **Threat assessment** results will be discussed off-site with the client.
- **Radio frequency (RF) spectrum analysis** from 10 KHz to 40 GHz; including identification of digital, spread-spectrum, and frequency-hopping transmitters in addition to the standard analogue devices.
- **Telephone system analysis** including instruments, in-house cabling, and peripheral switching equipment for intercept devices.
- **Infra-red (IR) and optical search** of all appropriate access areas
- **Carrier current analysis** of mains power cables & outlets, telephone and computer cabling, and other wiring as appropriate, to detect devices capable of transmitting communications
- **Physical and electronic search** of the area with a Non-linear Junction Detector to detect and locate dormant or remotely activated devices hidden microphones, transmitters, audio recorders, video transmissions and any other interception devices
- **Other analysis as required** depending on the threat assessment results and specific area analysis.

RISK3 CONSULTING LIMITED

Tel.: (852) 2815 2025
Fax: (852) 2815 2024
E-mail: info@risk3.com

24 Hr Crisis Response:
Alan Jeffries: (852) 9103 1852
Fred Chan: (852) 9452 9676