SWISS BUSINESS PROTECTION

Sweeping / TSCM (Technical Surveillance Counter Measures)
Finding hidden bugging devices / cameras

Leakage of confidential information can have severe consequences for a company. In addition to the loss of reputation, an operational disruption and financial damage, those affected may be confronted with penal issues as well as matters of private or regulatory law.

Opposing parties use illicit aids and methods to obtain information, patents, and technologies, as well as personal data. The use of today's technology allows hidden sound and image recordings, which enables unauthorized persons to acquire secret or confidential data and information. In addition, a GPS tracking device can be well hidden on a vehicle to constantly record and transmit the travelers location.

We recommend to examine the technical infrastructure, premises and vehicles used by key decision makers and interlocutors in order to counteract such threats. TSCM enables suspicious objects to be identified and removed from commercial buildings (from the shell to the finished state), from meeting rooms, lecture halls, offices, private houses and various means of transportation (including aircraft and vessels).

BENEFITS	You will explicitly know: ▪ Whether your competition / third parties are monitoring you technically and/or electronically ▪ Which rooms are safe for confidential meetings and discussions ▪ What kind of information could have been leaked ▪ Whether a selective or continuous information leak is existing ▪ Whether your vehicle is being monitored (tracking device) or conversations tapped ▪ What kind of countermeasures are necessary and suitable
PROTECTION CLASSES	With the 3 protection classes, the security needs can be covered individually. ▪ **Basic protection class** Use primarily for private individuals who feel threatened by eavesdropping devices in their personal environment. Detection of simple eavesdropping devices. ▪ **Medium protection class** Includes eavesdropping defense measures that have proven effective in the private and/or business premises of private individuals and business people as well as in companies. The potential attackers here are in the environment of employees and detective agencies. ▪ **Upper protection class** The upper protection class is optimized for potential attack scenarios in the areas of industrial and competitive espionage.
CONTENT	▪ Detailed physical search of the building infrastructure and furniture, (e.g. opening of fixtures) ▪ X-ray of portable objects and equipment to detect permanently or temporarily installed listening devices or cameras ▪ Creation of thermal images to identify hidden electrical devices through their heat emission ▪ Use the Non-Linear Junction Detector (NLJD) to search for inactive, switched-off or only temporarily operating eavesdropping devices. ▪ Sonic measurements to detect external eavesdropping ▪ Frequency measurements using highly sensitive instruments ▪ Documentation / reporting ▪ Recommendation of suitable countermeasures for future defence
METHODOLOGY	Preliminary discussion and information gathering, analysis, sweeping on site, reporting.
TARGET GROUP	▪ Companies and their decision makers or discussion partners ▪ Law firms, trust offices, asset managers, family offices and private persons ▪ Security authorities, data protection-relevant administrative departments, government agencies
DURATION / PLACE	As required for inspection; depending on premises, equipment, data carriers and vehicles, etc.
COSTS	According to expenditure. After an initial consultation and an inspection of the premises we'll be pleased to present you an offer.
DIRECTION	Chris Eckert, Thomas Winkler