Technical & Electronic Surveillance Counter Measures (TESCM) Investigation

Corporate Crime Management (CCM) is pleased to present the following proposal for a professional TSCM Investigation (via our associate company : **Electronic Counter Intelligence Detection Services – ECIDS**), which would include the utilisation of:-

- A range of TESCM Equipment
- Qualified Telephone Technician & TESCM Technicians.
- Report, together with recommendations.

The TESCM investigation would include:

- Offices
- Boardrooms
- PABX, Telephones and Telephone System in the above
- Power cables
- Offices @ residences
- Computers & IT-Network, via IT-Intelligence-methodology (*only performed on request of the client, with additional costs incurred*)

The service proposed is one whereby Corporate Crime Management (CCM) cc, does a Technical & Electronic Surveillance Counter Measures (TESCM) investigation (also known as "debugging") of the above, at a time convenient to all parties.

This is in order to determine if any illegal monitoring has taken place at your premises. CCM can then provide a complete TESCM report advising on Counter Measures, which can be taken to limit the chances of illegal monitoring.

CCM (ECIDS) educates the client on the countermeasure process, by offering explanations in layman's terms, not hiding behind technical jargon.

The TESCM investigation team will consist of Telephone Technician or Technicians and members trained to utilise the TESCM equipment and knowing what to look for (exposed prolonged periods to this activities, creating the expertise needed).

The CCM TESCM Teams have an array of electronic detection equipment at their disposal to detect active, passive and dormant devices.

The **equipment** used is as follows:-

- **SCANLOCK SELECT / OSCOR 5000**
- **SuperBroom Plus -Non-Linear Junction Detector, with Third Harmonic Receiver.**
- **Telephone Toners and Probes**
- **Search Kit**

TESCM PROCEDURES

PREPARATION

The CCM consultant will conduct a background interview with the client to ascertain an overview of the client's security concerns. This discussion will not be held within the facility that is to be inspected. The consultant will require a full understanding of the circumstances that led to the client recognising the need for CCM.

IMPLEMENTATION

Physical Examination

The CCM TESCM Team will conduct a physical search of the areas deemed by the client to be most sensitive and/or vulnerable for all types of current electronic eavesdropping devices and any indications of past attempts.

The team will rely heavily at this stage on their eyes, minds, training and experience. In addition to possibly discovering actual devices during this phase the Team will also be searching for evidence of prior attempts at eavesdropping e.g. fresh paint, putty, disturbed dust, bits of wire.

The SuperBroom Plus/Oscor, which detects and pinpoints bugging devices whether they are on or off, will aid the team. This includes transmitters, tape recorders, microphones, so-called hardwire bugs or any item with diodes in it.

Auxiliary audio input also allows us to listen to telephones or lines for hot mikes, hook switch by-pass and infinity bugs whilst also testing unknown wires or cables for wired microphones.

The Scanlock/Oscor is used to check for any transmitting signals or devices and checks the Mains Power Wiring and any other unidentified cables for so-called Baby-Sitter eavesdroppers

Radio Frequency Spectrum Analysis

Eavesdropping devices which transmit a radio signal, over-the-air or through building's wiring can be detected by an instrument called a **SCANLOCK SELECT / OSCOR 5000. Many Government Intelligence Agencies throughout the world use these systems, for their Security Countermeasures.**

The equipment employed by the CCM TESCM Team will "sniff" your environment for hidden phone, room or body bugs, remote control signals, computer, fax or telex transmitters and wide band frequency hopping or burst bugs.

Telecommunications

Telephones - Direct lines and calls routed through the switchboard. The consultant will examine the main switchboard and associated junction boxes in addition to all telephone instruments within the areas to be inspected.

Associated wiring will be inspected for attachments and damage. Damaged wiring is often the only indication of a previous attempt at eavesdropping.

Junction boxes are where telephone wires connect to each other within the building. These wires form a path between the telephone handset and the in-house switchboard. Junction boxes are an easy and relatively safe place to attach an illegal device. By using the spare wiring, invariably already in place in junction boxes, paths can be constructed to route a call to a remote device or recording unit.

Facsimile Communications

Fax machines are a further prime source of information leaks. They are often the targets of commercial espionage, since they are a concentrated source of important information that must by conveyed quickly. They use ordinary telephone lines and are easily wiretapped. It is a simple matter to tape record fax transmissions or directly connect a fax modem and capture incoming and outgoing faxes on a PC. The CCM TESCM teams will inspect all fax machines and associated cabling.

In addition our consultant will test power sockets, telephone lines and any suspicious wires for very low frequency carrier current signals.

Acoustic Ducting Evaluation

Unexpected sound leakage into adjacent areas has been found to be the cause of many information leaks, especially the in-house type. Air ducts, common heater ducts, walls common with storage/rest/smoking/toilet facilities is an invaluable aid to eavesdroppers.

What if a device is found?

Once the CCM TESCM Team has detected, located and verified the presence of an intrusive device you the client have to decide whether to:

- Have it disabled.
- Use it to provide misinformation or
- Inform the police (& assist in registering a criminal case)

We will be happy to discuss all the options with you, however you should be aware that it is an extremely difficult task to act normally whilst providing misinformation and thereby not alerting the information predator.

REPORTING

Conclusion of Inspection

As the conclusion of the inspection the CCM TESCM Team Leader will provide a full verbal debriefing in which he will highlight in order of priority all problems found, whether existing or potential and will recommend solutions which need to be implemented in order of priority.

If required, the CCM TESCM Team can set up this equipment in stand-by mode for use by you during the course of a Board or other high-level meeting for which you require additional security. In stand-by mode the equipment can warn silently if a device is introduced into the room after it has been swept. The CCM TESCM Team can remain nearby throughout the course of the meeting to respond if required.

Final Report

You will receive a comprehensive written report, which will include a description of all the areas and communications equipment inspected, an explanation of all tests conducted and any necessary recommendations for security improvements. A review of any other espionage loopholes found during the pre-inspection and inspection and any espionage prevention information, which may be of value to your organisation.

Please feel free to visit our web site at **http://www.assesstherisk.com**, to see what other services we have to offer.

If you have any enquiries regarding the contents of this proposal, do not hesitate to call me.

Yours sincerely

Johan Mienie
ccm2@global.co.za
Cell No. 083 601 8171

COUNTER INTELLIGENCE

To organise, implement, co-ordinate and advise the corporate executive on the latest counter intelligence techniques, with the use of sophisticated high technology and strategies. This to ensure maximum protection of company interests in terms of the applicable laws and other statutes pertaining to the companies operations. (in accordance with the company's objectives and policies).

The most critical (viable) area of industrial espionage where information can be extracted from the source, via the utilisation of technical measures (not human), without the knowledge of the subject. This methodology usually applied by competitors, opposition or destructive parties.

Technical counter measures is the utilisation of both advanced and modern, electronic counter-measures equipment and form the bases of the above operational procedure, required to identify, quantify and neutralise, the execution of electronic eavesdropping threats. The latter poses a threat to both the modern executive, as well as the S & M- and R & D- department(s) of a specific institution/client.

Abovementioned threat, originates in the escalation of information-gathering activities by hostile business opposition, which necessitates the creation of an awareness of the posed threat and a vigilant response, towards the application of electronic devices in eavesdropping activities.

Viewed by **CCM (ECIDS)**, as an area of specialisation, specific client requirements will be discussed in confidentiality, at a neutral venue, removed from the possible place of intrusion, in view of the utmost sensitivity, surrounding acts of this nature.

Services:

- Establishing/Implementing a Counter Intelligence policy (& procedures)
- IT-Intelligence applications (*as per separate input at end of proposal*)
- Technical and Electronic Surveillance Counter Measures (TESCM) @ 'Sweeping/De-bugging'

TESCM is an inspection of a physical item or place (office, boardroom, motor vehicle, brief case, etc.). The purpose is to locate possible covert surveillance devices and/or technical weaknesses.

A TESCM inspection will also evaluate for weaknesses on all locks, alarms and other systems of physical and electronic security. TESCM is concerned with all signals leaving a sensitive or secure area, including audio. The TESCM program consists of technical investigations and services (such as surveys, inspections, pre-construction advise and assistance) and technical security threat briefings. TESCM investigations and services are highly specialised and are not to be confused with compliance orientated or administrative services, conducted to determine a facility's implementation of various security directives.

The TESCM program includes four separate functions, each with a direct bearing on the program.

- Detection
- Nullification
- Isolation
- Education (*Counter Intelligence Policy/Procedures*)
- IT-Intelligence (methodology to uncover interception (other destructive activities) on computers/IT-Networks)

Note: *No request for TESCM support will be accepted via non-secure means. Non-secure telephonic discussion of TESCM support is prohibited. If a listening device is installed in the area, such discussion(s) can alert persons who are conducting the surveillance and permit them to remove or de-activate their devices. When de-activated, such devices are extremely difficult to locate and may require implementation of destructive search techniques.*

Offices and conference facilities will be surveyed for future electronic counter surveillance equipment utilisation, including telephone systems (PABX), telephone lines (direct and extensions) and facsimile lines.

This very professional service is delivered through a specialised internal entity @ **ELECTRONIC COUNTER INTELLIGENCE DETECTION SERVICES (ECIDS),** one of South Africa's leading entities for electronic eavesdropping detection (sweeping & de-bugging) and communications security.

Costing here to be pre-determined between *eavesdropping-detection-entity* and the *client*, depending on the nature and extent of the requested service.

Usually rendered @ pre-agreed rates (depending on circumstances & requirements). *Approximate rate = USD35.00/sq. meter* (but depend on request and size of area, additional for PABX & lines inspected!)

In order to facilitate the TESCM Investigation the following information should be available prior to the inspection:

1. *The most important issue is*:-

   "What are we going to do if a listening/interception-device ("bug") is found?"

2. The first item is a detailed description of the area or item to be inspected, which should include the exact physical address, plus directions relative to the local area, and travel directions. (How is the TESCM specialist going to find your facility?).

3. Physical description of the area requiring TESCM services, to include: name of the area, room number, building number, address, and location. Blueprints or floor plans are a real plus.

4. Estimated square metres of the area (with office or room dimensions). This is important, as it will be used to estimate how much time will be involved to inspect the area.

5. Type and number of telephones and computer systems in the area.

6. Identity and telephone numbers of primary and alternate point of contact.

7. Phone number of *secure phone* and fax machine.

8. Security clearance requirements for TESCM specialists and support personnel (if required).

9. Date and serial numbers of the previous TESCM reports and the status of previous recommendations provided.

10. Information that may impact on the scheduling of TESCM services (i.e., date scheduled construction will commence, completion date of construction in progress, etc.).

<u>Ancillary Information</u> (which may be optionally provided)

11. Location of all phone rooms and wiring closets.
12. Diagram of furniture placement inside of area (usually on blueprints)
13. Location of all electrical outlets, and circuit breakers (also on blueprints)
14. Type of ceiling (suspended, open, plaster, etc...)
15. Type of the Phone System (TELKOM, PHILLIPS TELEBOSS, CISCO etc...)
16. List of all known phone numbers on premises.
17. Notes regarding recent repair work, new furniture, or equipment deliveries.

<u>On the day of the TESCM-exercise, the following is important</u>:

- **Access to all Floors & Rooms.**
- **Keys for all rooms, cabinets and storage facilities on the premises.**
- **A Senior Person from your Company is present, throughout the investigation.**

IT-Intelligence Dimension

Threats that can be investigated :-

Software :-

- Adware
- Malware
- Trojans
- Keyloggers
- Spyware Cookies
- Browser Hijackers
- Diallers
- Browser Helper Objects (BHOs)
- Surveillance Software
- Pop-up Generating Programs

Network Security & Intrusion Protection :-

- Wireless LAN / WAN Security implementation and intrusion prevention
- Wired LAN and back-end core Ethernet security implementation and intrusion prevention
- Firewall security

Back- end & Server Security principals :-

- Domain investigation
- Active Directory and security principals
- Organizational unit security
- Software licensing and pirated software detection
- Access control - Physical & Logical