TSCM - Technical Surveillance Counter Measures

Corporate eavesdropping poses a significant risk to any organization. Global statistics shows that the threat of internal eavesdropping is real and imminent. The statistics also shows that the majority of eavesdropping devices found during "Bug Sweeps" were planted either by current employees, recently terminated employees or associates.

Intellectual Property and Information Assets are critical to any business remaining functional and competitive, yet this data is routinely exposed to the risk of theft and overlooked in cybersecurity risk management.

Organizations are increasingly ineffective at safeguarding data for example current company dealings and negotiations, trade secrets, product design, development or pricing, and other sensitive information.

For many businesses, intellectual property protects more than just an idea or a concept – it protects genuine business assets that may be integral to the core services of the business and overall long-term viability.

Intellectual Property consists of many different areas, ranging from corporate identity through to products, services and processes that differentiate your business offering.
It's when these ideas are used without permission that an organisation can suffer.

Almost all businesses have undoubtedly benefited from the internet, where products, services and marketing communications can reach vast audiences at relatively low costs - but this has also increased the chances of Intellectual Property theft.

Companies of all sizes are at risk of having their current cutting-edge ideas, products or services infringed upon, making Intellectual Property protection more important than ever.

Advanced Corporate Solutions (ACS) are experienced practitioners in the field of Technical Surveillance Counter Measures (TSCM), Electronic Countermeasures Investigation (ECMI) "Debugging" and carry out searches for a broad based clientele worldwide.

TSCM - Technical Surveillance Counter Measures

All members of ACS's Assessment and Inspection Team are highly qualified in the field of TSCM/ECMI.

Awareness and training is key to our success. We also offer awareness and training in the field of TSCM/ECMI to our clients and their personnel.

In most cases, there are limited numbers of security professionals in an organization and therefore the need to train and create awareness to the company's employees is very important so as to have a joint effort when dealing with matters of security and TSCM/ECMI services.

Security awareness and training also ensures that employees are fully awake to the consequences of failing to protect the organisation from outside attackers. Such consequences span from criminal penalties to large scale economic damage to the company and the loss of employment.

Your security awareness and training program should highlight the key entry in which attackers can gain access to your operational and executive environment, and the necessary steps to curtail these risks. It is imperative that all companies have systems and processes in place to protect and safeguard their Intelectual Property as per the King IV report

At ACS we pride ourselves in accreditation and association with the following local and international authorities and bodies:

South African Police Service
Reg. No.: 4000271

Private Security Industry Regulatory Authority
Reg. No.: 0058804

Safety and Security Sector Education and Training Authority
Reg. No.: 051901409857

Association of Certified Fraud Examiners
SA Chapter

REI USA

SHEARWATER

Blake Technical SARL

Advanced Corporate Solutions
"Debugging" Specialists

22 Years of Service Excellence (1995 - 2017)

Office: +27 (0) 12 349-1779
Riaan Bellingan: +27 (0) 82-491-5086
André Oosthuizen: +27 (0) 83-260-6125

TSCM - Technical Surveillance Counter Measures

Our physical search covers the areas most commonly used to conceal eavesdropping devices and includes an inspection of ceiling and floor voids, power, telephone and data sockets. We pride ourselves on using state of the art equipment during our TSCM/ECMI Assessment and Inspections.

Our equipment is manufactured by leading manufacturers based in the United Kingdom and the Unites States of America. Our equipment follows stringent maintenance schedules, ensuring that they operate at the highest level of accuracy.

Below is an overview of equipment that we use during our TSCM/ECMI assessment and Inspections.

RAPTOR RXI

The Raptor RXi is an ultra-fast-scanning counter-surveillance receiver for quickly detecting surveillance transmitters. The Raptor scans from 10kHz to 26GHz in under 4s, detecting even the briefest pulsed transmissions. Featuring a fast Core 2 Duo processor, its multiple software tools and demodulators detect frequency hopping, burst mode and spread spectrum devices as well as analogue audio and video signals.

ANDRE

The ANDRE Advanced Near-field Detection Receiver is a broadband receiver that detects nearby ambient RF energy. The ANDRE is an economical tool for detecting known, unknown, illegal or disruptive, or interfering RF transmissions across a 10 kHz to 6 GHz frequency range.

CPM-700

The CPM-700 is a broadband receiver designed to detect and locate all major types of electronic surveillance devices including room, phone, body bugs, video transmitters, and tape recorders. Broadband receivers such as the CPM-700 provide a very important costeffective tool for professional sweep teams, government security personnel, and private citizens with important security needs.

TALAN 3.0

Voice-over Internet Protocol (VoIP) phone systems present a new form of security risk to communications. With new enhancements built into the TALAN software interface, users can now test internet protocol (IP) packet traffic on VoIP phones and systems. VoIP data collected by the TALAN software includes Source and Destination Mac Addresses; header type; statistics - total packets; packet rate; peak rate and run time. Users can also define advanced filtering options. Data can be stored and exported to USB or Flash as data files for further analysis, sharing and reporting. The NEW TALAN 3.0 Telephone and Line Analyzer represents advanced. capability to detect and locate illicit tampering and security vulnerabilities on digital, analog, and VoIP telephone systems. New hardware provides the ability to test twisted pairs against modern telecommunication threats including shield and ground

Advanced Corporate Solutions

"Debugging" Specialists

22 Years of Service Excellence (1995 - 2017)

Office: +27 (0) 12 349-1779
Riaan Bellingan: +27 (0) 82-491-5086
André Oosthuizen: +27 (0) 83-260-6125

TSCM - Technical Surveillance Counter Measures

HAWK XTS

The HAWK XTS-2500 is a portable, simple to use advanced Electronic Device Detector, also known as a Non-Linear Junction Detector (NLJD). The HAWK XTS-2500 is capable of locating and confirming the presence of electronic components found in devices, regardless whether they are switched on or off.

BLOODHOUND

Bloodhound is an ASMD, Acoustically Stimulated Microphone Detector which is an electronic system for use by Technical Security Inspection Teams for detecting audio eaves-dropping. The system works by detecting the radiated field created whenever a microphone detects sound. The Bloodhound operator can either listen to the detected audio or establish acoustic feedback.

VIDEO POLE CAMERA

White LED illumination for colour inspection in dark areas, i.e. drop ceilings, behind immovable objects, around corners, other difficult to reach areas and in dark situations..

CAT FLIR CAMERA & FLIR ONE

Powered by FLIR's Lepton® camera and using FLIR's exclusive MSX® technology. This rugged device uses FLIR (Forward Looking Infrared) to capture clear thermal imagery, video and even timelapse footage. The thermal imaging technology is used in the field of TSCM/ ECMI to determine if there are any hidden or rogue electronic devices in the vicinity. Electronic devices have multiple ways of accessing power sources on order to function, which indivertibly leads to the emission of heat. The device is also used to identify and locate rogue WI-FI access point in the target area.

CELLEBRITE

Cellebrite is a world leader in the development of advance mobile forensic hardware and softwareproducts. The Universal Forensic Extraction Device (UFED) Touch Ultimate from Cellebrite is an example of hardware used by mobile device investigators to gather information. Mobile devices, which include smart phones and tablet computers, provide increased functionality and ease of use to people, anywhere and anytime. With it comes the potential for mobile device malware (malicious code).

Our assessment / investigations reports include the following key focus areas:

- Findings of the investigation.

- Identified and potential eavesdropping threats and scenarios.

- Shortcomings in the client's physical security measures that can facilitate eavesdropping attempts.

TSCM - Technical Surveillance Counter Measures

Our all encompassing and holistic approach to security guarantees the safeguarding of all our clients Intellectual Property. We have a proven track record that spans over 22 years in the industry, and formal references can be supplied on request. Contact us today for a detailed discussion and overview of our services, and how we can assist your company with the safeguarding of its Intellectual Property. Your security is our number one priority.

"We must inspire a commitment to security rather than merely describing it"

First Floor, Building 16, CSIR, 627 Meiring Naudé Road
Brummeria, Pretoria, Gauteng, South Africa
Gate 3, S25 44.874, E028 16.523

Office Tel: +27 (0) 12 349-1779 / 83

Riaan Bellingan
+27 (0) 82-491-5086
riaan@acsolutions.co.za

www.acsolutions.co.za