# Kestrel TSCM ® Professional Software

# Technical Surveillance Countermeasures (TSCM)

**September 2017** **Technical Research and Standards Group (TRSG)**

**Paul D Turner, TSS TSI**

Understanding the findings and observations during an inspection, is a critical element in providing professional TSCM services. Every member of the team must bring a wide range of very specific skills to the mission, for the benefit of the end-user. Permitting, untrained, and unsupervised warm bodies to assist, often in order to justify unrealistic professional service rates, not only fails to accomplish the core task of identifying the threats, but also the significance of the threats, understanding the implications and significance of the findings and observations is a critical task.

As noted in the August 2017 newsletter.

*"There are many aspects of conducting organized high-risk assignments that significantly benefit, from actionable RF intelligence. Professional Development TSCM Group Inc., is perhaps one of the few technical security organizations that has cultivated years of field experience in providing, operational counter-intelligence support, and defensive RF based counter-surveillance, for international venues, aircraft, marine vessels, residences, hotels, meeting, conference facilities, and special events. Protective operations often bring all of the unknowns together in one place, and raise the threat profile in every respect during out of country operations".*

There are very few technically qualified operators in Canada, actually (or should be) working at high threat levels, and the vast majority of those assigned to assist during technical sweeps, are simply not qualified to understand, or undertake high threat level assignments.

An experienced technical operator can not only identify potential compromises, but they can also understand the implications and significance of the findings and observations, on a non-technical level (investigative).

This takes years of real experience, and does not involve simply climbing a ladder and shining a flashlight around for the benefit of the client. The ladder and flashlight must be in the hands of an experienced technical security specialist, in order to be, in any way effective.

Every member of the inspection team, must have the required skill sets and experience, to accomplish the task at hand, and be able to direct and advise the end-user client, well beyond the technical findings. During a recent assignment, it was determined that the client was utilizing an analog Hearing Assist system which interfaced directly with meeting room and boardroom table top microphones, to accommodate visitors and employees that might require Hearing Assist technology. The findings, revealed two powerful VHF analog audio devices transmitted room audio from the meeting room, and boardroom, up to 50 feet away from the rooms in question, to include the lobby, reception areas. Located in a typical commercial building with excellent high floor line-of-sight, allowed all room audio on a 24 / 7 basis to be transmitted, and potentially intercepted by persons, and entities unknown. The boardroom microphones were always on, providing real-time, crystal clear room audio for anyone interested in monitoring meetings, events, secret level briefings, and the words of anyone having a private conversation behind the closed doors of the affected meeting rooms, contrary to sections of the Criminal Code of Canada.

A previous inspection, apparently noted the device as analog, and notified the client, but failed to understand the significance, or delineate the significance of the finding. The resulting decision of the client to maintain the current practice, based on a failure to understand the implications of the practice, with certainty, has resulted in a serious compromise of sensitive or classified strategic business information. Since one of the transmitters was openly visible within a meeting space, it is reasonable that anyone using the room, with an interest in conducting economic-espionage, would have taken note of the system, as a compromise. On an entirely different level, we found the Hearing Assist receivers located in several different areas, meaning anyone at anytime could activate the devices and listen to sensitive, or classified briefings from the most critical meeting spaces, without any risk of detection.

# Kestrel TSCM ® Professional Software

# Understanding the Findings and Observations is a Powerful Lesson for the Private and Public Sector

**Professional Development TSCM Group Inc.** **Technical Security Branch (TSB)**

Lets look at a possible scenario, where an individual makes a presentation, and is then asked to wait outside while the proposal is discussed, or a decision is made. Once outside the meeting space the individual either utilizes a small VHF receiver, or simply utilizes one of the provided dedicated Hearing Assist receivers to monitor the events. There was not obvious accounting of the system receivers. Now, consider the optics of perhaps an employee, potentially utilizing the same receiver to monitor guests, visitors, or others entering the space, or engaged in a private discussion in the lobby, or reception areas.

There are a number of factors at play in this scenario that need to be understood. First, the Hearing Assist system is required for guests and company personnel that might need it. Second, the system is analog in nature, which is a serious breach of security and privacy in a modern digital age. Next, the system is active 24 / 7 and does not discriminate as to who, and what information it transmits, as the AV system appears to be turned off. There is no indication that all of the table microphones are actively sending room audio to the Hearing Assist system transmitter 24 / 7 even if the system is off. All room audio is being send to the AV controller.

Unfortunately, this is not the first time we have found these types of systems, installed in such a way that the client is compromised. So who is to blame, the AV company, who clearly failed to understand the legal implications, and threat to national security? Is it the client, for not recognizing the potential compromise, given the significance of the business entity? Is it the competitive sweep team, who failed to ensure that the client fully understood the active threat posed by the system, the significant civil and criminal liability, and the violation of various sections of the Criminal Code of Canada?

In the end, all assume some level of responsibility, through errors and omissions.

The obvious is the obvious and failing to understand the implications of a client installed technical compromise is what every state-sponsored player involved in economic-espionage tradecraft, can only dream of, when the target makes it so easy, to compromise extremely sensitive information, including secret level material.

To learn more about developing an effective Technical Security (TSEC) program, or seek information about training and certification opportunities, please contact Paul D Turner, TSS TSI

| www.pdtg.ca | www.kestreltscm.com | www.ctsc-canada.com |

***Kestrel TSCM ® Professional Software is innovative industry leading, disruptive technology, now sold in 29 countries worldwide.***