Murray Associates | Security Report

TSCM - During Construction Projects

by Kevin D. Murray, CPP, CISM, CFE, CDPSE

In the world of business espionage there is a golden time to install bugs, taps, and other electronic surveillance items.

It is a time when nobody is checking.
It is a time when these devices become completely hidden from future detection.
It is construction time.

The Bugged Embassy Case: What Went Wrong, is a well-documented story of eavesdropping devices so deeply planted the building had to be abandoned.

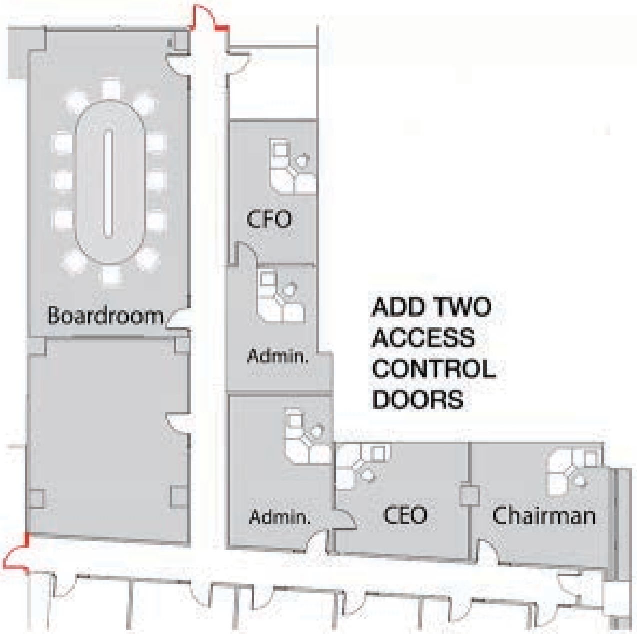
The Attack on Axnan Headquarters: An Espionage Operation, is a true story (sanitized) of exactly how corporate construction penetrations are accomplished.

Both accounts are a fascinating read, and are true cautionary tales for our times.

Design Information Security into Construction Projects

Electronic eavesdropping and information attacks can be stopped, but there is a catch; timing. Technical Surveillance Countermeasures (TSCM) needs to be included in the planning and construction phases of your project.

TSCM is neither complicated, expensive, nor disruptive. Or, put another way, including TSCM as a privacy precaution at the outset of a project is cost-effective due diligence, and it is cheap insurance. No, this is better than insurance. Insurance cannot prevent the problem.



Before You Begin

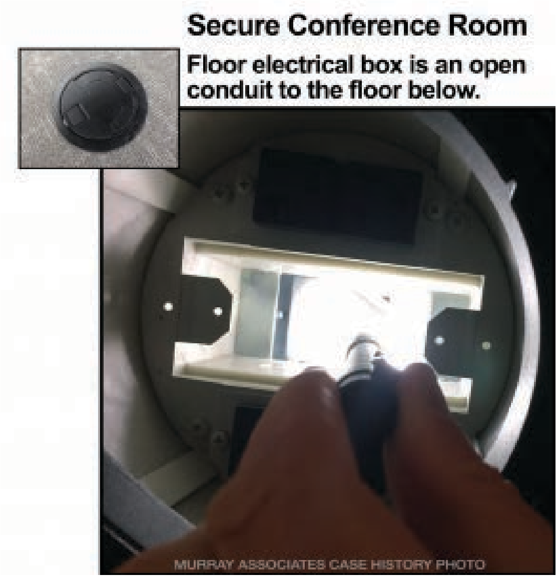
Engage the services of a knowledgeable Technical Information Security Consultant as early in the process as possible. Ideally, this will be at the concept stage, when security considerations can be easily introduced.

At this point, your advisor will be thinking in Crime Prevention Through Environmental Design (CPTED) terms. In a Boardroom renovation, for example, access control and placement of visual displays might be suggested for the architect's consideration. In a C-suite environment with large windows, suggestions might include visual surveillance deterrence tips.

> *"You really don't want electronic surveillance to become the latest tech innovation in your new Boardroom, C-suite, or other sensitive area."*

TSCM - Step One

This is when planning hardens into blueprints, new construction areas are established, and renovation areas are gutted. At this stage your consultant will briefly visit to photographically document the basic structure. This creates a clean baseline for future comparisons. It also aids in spotting acoustical leaks to contiguous areas, or floors, of the building.


Secure Conference Room
Floor electrical box is an open conduit to the floor below.
MURRAY ASSOCIATES CASE HISTORY PHOTO

As shown in the photo, acoustical leakage is often caused by small construction oversights, which later become big information security vulnerabilities.

TSCM - Step Two

This inspection occurs when all the wiring is in, and just before the walls and ceilings are enclosed. The area will be photographed again to document what and where everything is. Wiring can now be visually inspected.

Placement of other items, such as fire sensors, Wi-Fi Access Points, cell service extenders, etc. are also located and documented at this time.

Once **Step Two** is complete the walls and ceiling are cleared for enclosure. Any unauthorized electronics placed in the interim will become readily apparent during the Step Three inspection.

TSCM - Step Three

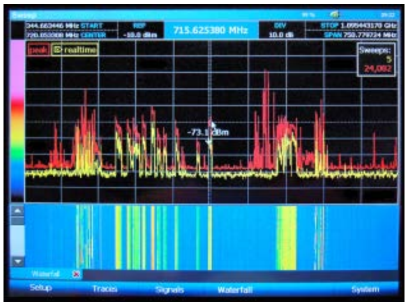
Once construction is finished, and all of the furniture and fixtures have been moved in, it is time for a complete TSCM inspection. Try to do this just before the space becomes an active workplace.

The basic elements of a TSCM inspection include…

Visual Examination

A thorough physical examination is conducted to discover electronic surveillance devices currently in place, and any evidence of prior eavesdropping attempts. This phase of the inspection includes a detailed examination of: furniture; fixtures; wiring; ductwork; computers, and small items within the area.

TSCM physical inspections are enhanced using the latest technology: hi-res CCTV, laboratory



grade thermal imaging, advanced Non Linear Junction Detection (NLJD), and more.

Non-transmitting attacks such as:

- miniature voice recorders,
- sound extraction via wiring,
- carrier current,
- infrared,
- ultrasonic or laser microphones,
- covert video (spycams),
- and keystroke loggers,

are just some of the things which this phase of the inspection covers.

Surveillance devices may be secreted in hollow walls, behind false ceilings, in or on furniture, fixtures and other common items which have a legitimate place in the room, such as: computers, power strips, radios and clocks.

Inspection is conducted with the aid of Non-Linear Junction detection, Thermal Emissions Spectrum Analysis, additional tools, and manual inspection techniques.

Technical Inspection

Detection of non-radiating devices.

Dormant, non-radiating, dead or broken surveillance devices are discovered by detecting the transistors, diodes — semi-conductor materials used in their circuitry.

Surveillance devices do not have to be on and operating to be discovered with a Non-linear Junction Detector (above). This technology is similar to shoplifting detectors used at retail store exits. Just the fact that the electronic components are there is enough sound the alarm.

Radio Reconnaissance Spectrum Analysis® (RRSA)

Detection and demodulation of wireless surveillance (audio, video & data) is accomplished with the aid of computerized spectrum analyzers.

RRSA® detection is very sensitive. Even though only certain areas may be designated for inspection, surrounding areas also benefit from this particular test.

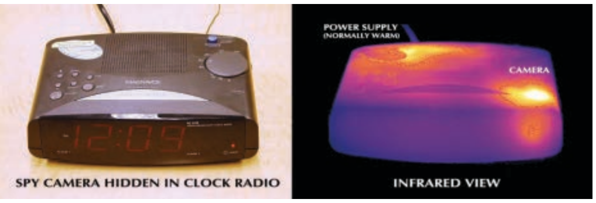
Optical Emissions Spectrum Analysis® (OESA)

Some electronic eavesdropping devices transmit intelligence by converting sound into infrared or laser light. This invisible light can be picked up optically from a distance and converted back into sound. (The average television remote control operates using the same principle.) TSCM instrumentation can detect this.

Thermal Emissions Spectrum Analysis® (TESA)

Minute amounts of heat are generated as electricity moves through a surveillance device's circuitry.

Thermal camera instrumentation detects these active items. The technique can also see bugs hidden in antique furniture and other delicate items – without damaging them.


SPY CAMERA HIDDEN IN CLOCK RADIO
POWER SUPPLY (NORMALLY WARM)
CAMERA
INFRARED VIEW

Concealed Space Examination

Spaces which cannot be directly viewed are optically examined using a flexible videoscope.

Hard-wired Communications Examination

- Visual inspection of the individual system components and connecting pathways.
- Frequency Domain Reflectometery (FDR) Analysis of the wiring paths.
- Carrier Current Analysis of the wiring paths.
- Audio Leakage Analysis.
- Electrical Characteristics Analysis.

Wireless Communications Examination

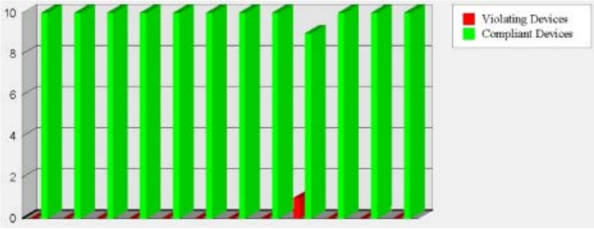
- Cordless telephones.
- Wireless headsets, keyboard and mice.
- Wireless presenter's microphones.
- Other wireless communications (Bluetooth, FM Analog, etc.)

Wireless LAN (WLAN) - Security and Compliance Inspection

A Wi-Fi security and compliance audit is an essential element of the TSCM inspection process. It detects WiFi-reliant audio and video covert surveillance, rogue network intrusion devices, in addition to compliance issues. This test helps guard against eavesdropping, data syphoning and government penalties due to compliance lapses.

Although a Wi-Fi inspection is part of a TSCM service, it can be conducted separately when compliance is the sole concern.

Just one loophole...

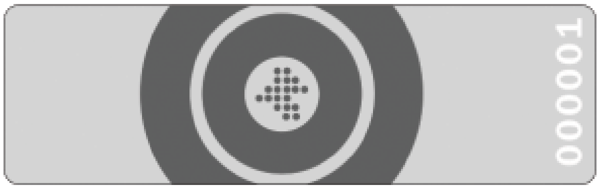


Hackers are in.
Data is out.
&
"You are out of compliance."

Some of the privacy laws and directives which may impact your Wi-Fi usage include…

- Sarbanes-Oxley Act – U.S. Public Companies
- HIPAA – Health Insurance Portability and Accountability Act
- GLBA – Gramm-Leach-Bliley Financial Services Modernization Act
- PCI-DSS – Payment Card Industry Data Security Standard
- FISMA – Federal Information Security Management Act
- DoD 8100.2 – Use of Commercial Wireless Devices, Services and Technologies in the Department of Defense Global Information Grid
- ISO 27001 – Information Security Management
- Basel II Accord – Banking
- EU - CRD (Cad 3) – EU - Capital Requirements Directive - Banking

Tamper Detection



Security seals are used to seal phones, tag non-malicious USB cables and other objects after inspection. Items previously inspected and sealed may be re-examined at any time to verify seal integrity. The seal numbers are recorded in the written report.

Keep the following in mind when examining these seals. A damaged or missing seal may indicate tampering. A missing seal may also indicate the object being sealed was replaced with a pre-bugged, identical-looking item. Either condition is a suspicious incident which should be investigated further.

Acoustical Ducting Evaluation

This phase of the inspection evaluates the possibility of sound migration — a common cause of information loss. Ductwork, open ceiling plenums, common walls / ceilings / floors can conduct sound in unexpected ways.

Information Security Survey

As part of the inspection process general security efforts already employed are observed to assess appropriateness and current effectiveness. Items observed may include:

- CCTV, locks, alarms.
- Employee compliance with good information security practices.
- Access control.

- Security officer efficiency.
- Potential for abusing in-place technologies.
- Security policies (in place, or needed).
- General security and safety observations.
- Cost-effective recommendations for improvements, repairs, upgrades, and additions are made as necessary.

Note: Your technical consultant should not sell, or profit in any way, from the products and services recommend. Your best interests must come first.

In addition to the above procedures, some other specialized tests may be employed based on unique needs.

Debriefing

As appropriate, an immediate on-site debriefing should be conducted to convey the results of the inspection and to discuss future strategy. Recommendations which need to be implemented quickly are also discussed at this time.

Written Report

A written counterespionage report will document the inspection details. It may also contain recommendations requiring your immediate attention.

General Advice

Maintain a cautious attitude and safeguard your report. It discusses security strategies which are not for general dissemination. It also documents your proactive stance and due diligence on information security – a legal prerequisite for protection in court.

###

Thank you for considering our services. If you have any questions, or would like to schedule our services, just let me know.[1]

Kevin

Kevin D. Murray CPP, CISM, CFE, CDPSE is a business counterespionage consultant and TSCM specialist with over four decades of experience.

Murray Associates[2] is an independent security consulting firm, providing eavesdropping detection and counterespionage services to business, government and at-risk individuals.

Headquartered in the New York metropolitan area, a Murray Associates team can assist you quickly, anywhere in the United States, and internationally.

[1] https://counterespionage.com/contact-murray-associates-tscm/

[2] https://counterespionage.com/about-murray-associates/electronic-eavesdropping-detection/