EXECUTIVE BRIEFING — 2026 EDITION

The Executive's Guide to Counter-Surveillance

Confidential information has a buyer. Boardrooms, negotiations and executive travel are routinely targeted by financially motivated actors and, in some cases, state-sponsored adversaries seeking strategic advantage. This guide sets out how devices get into a space, the warning signs to watch for, and what to do — and not do — if you suspect a room is compromised.

It is written for executives, board members and the people who manage their calendars and travel — not for technicians. Use it to recognize risk early and to act correctly in the first few minutes after you suspect it, which is often the difference between catching a device and losing the evidence entirely.

What this guide covers:

- The threat landscape — who is targeted, and why
- How devices get into a supposedly secure space
- 12 warning signs you may be under surveillance
- Travel and off-site meeting security
- Vehicle security — the most overlooked attack surface
- When, and how, to call in professional TSCM support

1. The threat landscape

Illegal eavesdropping is a business model. The threat ranges from financially motivated criminal actors to state-sponsored adversaries seeking strategic advantage, and both plant the same kind of device for the same reason: a room that talks freely is worth more to them silent than closed.

Who gets targeted

- Boardrooms & executives — Strategy, pricing and personnel decisions are worth more to a competitor before they are announced than after.
- Legal & deal teams — Privileged strategy, negotiating positions and settlement figures are high-value targets in any contested matter.
- Government & agencies — Classified material, operational planning and diplomatic communications draw state-sponsored as well as opportunistic interest.
- High-net-worth families — Personal security, travel patterns and financial affairs make private residences and family offices a standing target.
- Journalists & activists — Sources, unpublished reporting and internal communications are exposed the moment a device is planted nearby.
- Anyone in litigation or divorce — Legal and divorce proceedings routinely motivate a spouse, business partner or opposing party to plant a device.

What an adversary gains from an unmitigated device

- Conduct reconnaissance and intelligence-gathering against the organization.
- Collect and disclose classified or commercially sensitive information.
- Hijack critical communications, causing loss of finances, assets or worse.
- Obtain money and financial data.
- Compromise law enforcement and intelligence agency operations.

2. How devices get into a secure space

Installing a device requires physical access, and access is usually obtained through the moments an organization least expects — not through a dramatic break-in. Recognizing these vectors is the first step in closing them.

- Maintenance and IT visits: A repair, "IT maintenance" call or renovation that nobody quite scheduled is one of the most common covers for planting a device, because unsupervised access is granted without question.
- Contractors, cleaners and caterers: Anyone with extended, unescorted time in a sensitive room — a cleaner staying longer than the job requires, a caterer setting up alone — has an opportunity most organizations never audit.
- Gifts and everyday objects: Bugs are routinely concealed inside smoke detectors, power strips, clocks and promotional gifts, precisely because nobody questions items that look like they belong.
- Hotel and off-site venues: The moment a meeting moves off-site, you surrender control of the room to venue staff, prior occupants and anyone who booked the space before you.
- Vehicles left unattended: Cars sit in car parks, are handed to valets and service technicians, and are often shared across a pool — every one of those moments is an opportunity to plant a tracker or transmitter in seconds.
- Departing employees or partners: A departing employee, contractor or estranged partner who had unsupervised access before is a common source of both physical planting and inside knowledge of the space.

3. 12 warning signs you may be under surveillance

No single sign is proof. Two or three together, in a space that matters, are reason enough to call for a professional sweep.

01 Confidential information surfaces outside the room it was discussed in.

02 Competitors anticipate pricing, bids or strategy they had no legitimate way to know.

03 Calls carry static, clicking, or faint feedback that was not there before.

04 A negotiating counterpart or opposing party seems to know your position in advance.

05 Furniture, ceiling tiles or wall fixtures show signs of having been moved or reset.

06 An unexplained gift, promotional item or piece of electronics appears in a sensitive space.

07 A phone, radio or Wi-Fi device drains its battery unusually fast or runs warm when idle.

08 Vehicles or individuals seem to reappear across unrelated locations and times.

09 A recent renovation, repair visit or "IT maintenance" call was not one your organization scheduled.

10 Deal terms, legal strategy or HR matters leak before they are formally disclosed.

11 AM/FM radio or baby-monitor interference appears near a specific wall, desk or fixture.

12 A departing employee, contractor or estranged partner had unsupervised access before the leaks began.

4. Travel and off-site meeting security

Off-site meetings exist precisely because the subject matter is sensitive, yet moving to a hotel or hired venue surrenders control of the room. Sweep the venue before principals arrive — the room and adjoining spaces should be RF-mapped and physically inspected, since a neighbouring suite or shared wall can carry a conversation as effectively as a device inside the room itself. For high-stakes sessions, live monitoring during the meeting catches a device introduced mid-session, which a one-time sweep cannot. Threat does not pause between the airport and the boardroom: clearing hotel suites and temporary workspaces along an itinerary before arrival removes the one variable a travelling executive cannot otherwise control.

5. Vehicle security

A vehicle is the single most predictable thing about a target — it reveals home, office, routine, meetings and associations from one small device, and it is the easiest asset to reach. GPS trackers turn up in wheel wells, bumpers and under the chassis, or draw power from the OBD-II diagnostic port, plugged in within seconds and easily mistaken for a legitimate accessory. Audio transmitters conceal in wiring harnesses, power lines and interior trim. Any vehicle that has been outside trusted control — valet, service, long-term parking or shared fleet use — should be treated as a fresh risk and swept accordingly.

6. When to call in professional TSCM support

If you recognize several of the warning signs above, the instinct to act immediately is understandable — but two common reactions will destroy the evidence and tip off whoever is listening.

Do not sweep it yourself

Consumer "bug detectors" miss dormant, burst-transmission and passive devices — the ones that matter most — and hand you false confidence. Poking around also alerts an eavesdropper that you are onto them.

Do not announce it in the room

The moment you say "I think we're bugged" inside the suspect space, you have told whoever is listening to remove or disable the device before anyone can find it. A bug that has been pulled leaves no finding, and you lose the one chance to catch it in place.

What to do instead

- Leave the room and speak from a personal phone or a neutral location.
- Contact a licensed TSCM specialist and let the methodology work quietly.
- Keep the circle of people who know as small as possible.
- If a device is found: do not touch it, document it in place, preserve it as evidence, and act on the agreed mitigation plan.

Boards and executives carry a fiduciary responsibility to protect employees and shareholders from security breaches, including unauthorized access to verbal communications. A comprehensive TSCM program — swept on a regular cadence, typically quarterly, rather than only after a suspicion arises — is what discharges that obligation.

If any of this mirrors your own environment, the correct next step is a discreet, confidential conversation. Call +233 20 778 9103 or email info@forensictscm.com — every enquiry is handled in strict confidence, with no obligation.