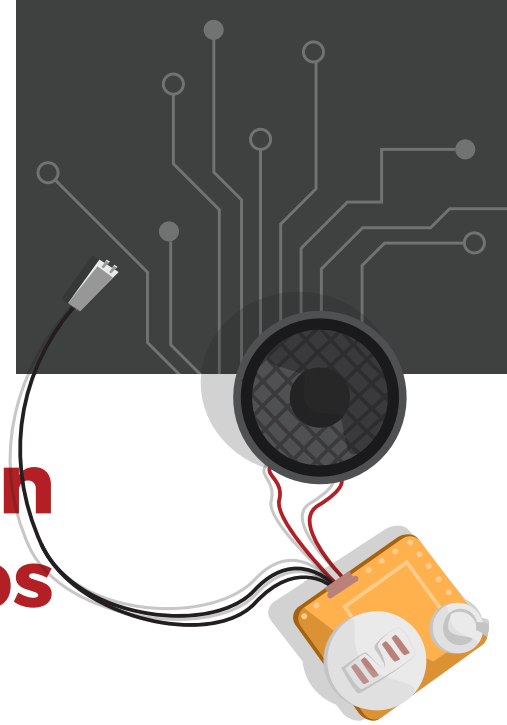
TSCM NZ



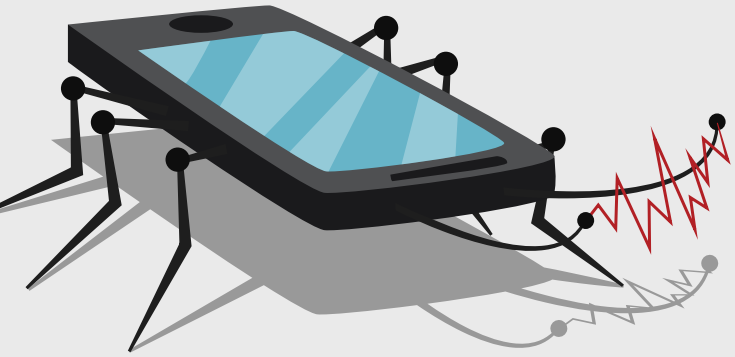
An Explanation of TSCM Sweeps

TSCM sweeps are known by many different names: bug sweeping, TSCM inspections, electronic counter-surveillance etc. They are all one in the same thing; an electronic and physical check or inspection of a room, building, area or vehicle. These services are known as a TSCM sweep.

Ideally, companies should look at TSCM sweeps as part of their security housekeeping policy; they should have a security and risk policy that includes the budgeting for TSCM. The frequency and the requirements are down to the individual company and how they perceive the level of threat against them at that particular time. For instance, a company might be involved in a hostile take-over or substantial litigation and may wish to increase the level of service at that particular time.

If a company feels that it may have an issue of loss of sensitive information then a TSCM sweep is not the only thing that it should be thinking about. This is very much a common mistake and one that is often regretted in hindsight.

Should a company find that it is in the position where it feels it is losing information or data, then really that company should launch a full internal investigation and, where required, call in external counter espionage experts..

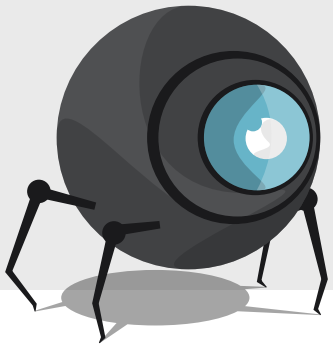


In many cases the loss of sensitive company information can be down to a failing in internal policy, such as office refuge or key staff leaving. It is not always about targeted acts of espionage, but if this is the case, it's often worthwhile managing the issue correctly, leaving open options of legal action. Should this be mismanaged at an early stage then it is difficult to regain the situation and opportunities to gather key evidence may be lost.

Most people's understanding of bugging or eavesdropping devices comes from watching television, films or popular fiction books. Most of the capabilities of bugging devices that are depicted in popular film and television are not technically possible.

It would be very foolish to think that one could just buy a device, plant it and place it within an office; there is much more to it than that. There are many more things to think about; not to say of course that a person with no prior knowledge or training could not pose a threat.

Small eavesdropping devices are great for quick, short-term tasks, such as those built into pens, computer mice or stuck under desks or chairs etc. However, these devices have their drawbacks and devices that are going to be required to be in position long-term require more sustainable power supplies and are normally “hard wired” or built in to powered devices, for example plug sockets, extension leads, phones or computer monitors etc.



Sometimes it really is as simple as placing a Dictaphone on voice activation for later retrieval.

There has been a large increase in “off the shelf” eavesdropping devices, ranging from complex GSM devices to the lower end of the scale FM, UHF devices.

An individual or organisation carrying out acts of espionage is going to look at the easy options for intelligence gathering first, i.e. those with the least risk and that are most cost effective. Eavesdropping and monitoring of devices is expensive and full of risks, with huge damage to profits and reputations if caught, not forgetting prison sentences. That said, very few corporate espionage cases are ever brought to court, victims instead prefer to settle such matters outside of court to save bad PR and reputational damage.

Exactly how a TSCM Sweep takes place is very much dependant on the topography of the building and how it is laid out; how many floors, how much open office space etc.

Ideally, the team would enter the target building at night when there are no workers in the building. Normally, the TSCM Team would set up in a central location on each individual floor that requires sweeping (in the case of a rural residence, one location will suffice).

A TSCM team should employ different TSCM equipment, with each piece of equipment carrying out a specific role. The team should also be looking for redundant hardwired devices, covertly placed recording devices (such as Dictaphones) or devices that are piggybacking on or off the back of genuine electronic devices (such as telephone lines or computers). To look for these devices both a physical and technical inspection is required, often employing equipment such as a Non-Linear Junction Detector. This looks for, and detects, circuitry used within circuit boards or microphones that are or are not powered at that time, i.e. “passive devices”.

There are many, many other types of equipment that can and should be deployed on a TSCM sweep, from thermal imaging cameras to look for devices buried within walls or soft furnishings.

Meeting rooms and offices of directors or senior partners should be at the very top of the list, not forgetting offices of related personal assistants. Open areas are in many ways harder to sweep, as they have a number of sockets and work stations. These areas take time; particular attention should be paid to allocating the correct amount of time to this task.

Computers are not normally covered on TSCM sweeps but can also easily be turned into eavesdropping devices with just the edition of spyware. This is not a real worry for large companies with IT security managers and teams, but can be totally forgotten and overlooked when it comes to company directors working remotely from home.

A TSCM sweep should be part of your ongoing security and counter espionage policy; employed alone in isolation they are a token gesture.

There are a variety of motives or personal situations that may increase the likelihood someone will spy against their employer:

Greed or Financial Need:
A belief that money can fix anything. Excessive debt or overwhelming expenses.

Anger/Revenge:
Disgruntlement to the point of wanting to retaliate against the organization.

Problems at work:
A lack of recognition, disagreements with co-workers or managers, dissatisfaction with the job, a pending layoff.

Ideology/Identification:
A desire to help the "underdog" or a particular cause.

Divided Loyalty:
Allegiance to another person or company, or to a country besides the United States.

Adventure/Thrill:
Want to add excitement to their life, intrigued by the clandestine activity, "James Bond Wannabe."

Vulnerability to blackmail:
Extra-marital affairs, gambling, fraud.

Ego/Self-image:
An "above the rules" attitude, or desire to repair wounds to their self-esteem.

Vulnerability to flattery or the promise of a better job.
Often coupled with Anger/Revenge or Adventure/ Thrill.

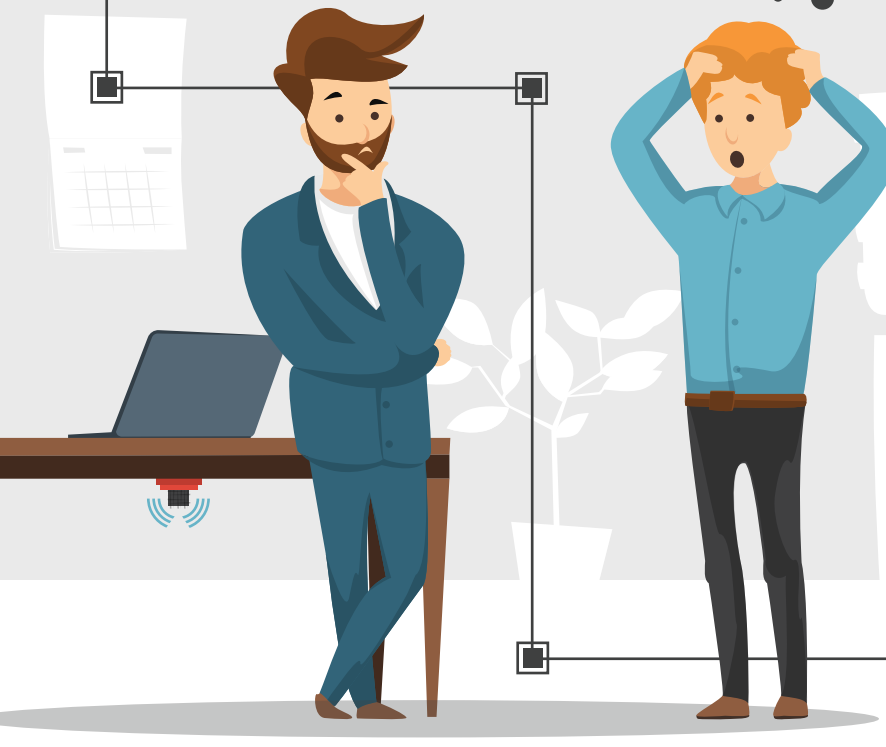
Ingratiation:
A desire to please or win the approval of someone who could benefit from insider information with the expectation of returned favors.

Compulsive and destructive behavior:
Drug or alcohol abuse, or other addictive behaviors.

Family problems:
Marital conflicts or separation from loved ones.

Some behaviours may be a clue that an employee is spying and/ or methodically stealing from the organization

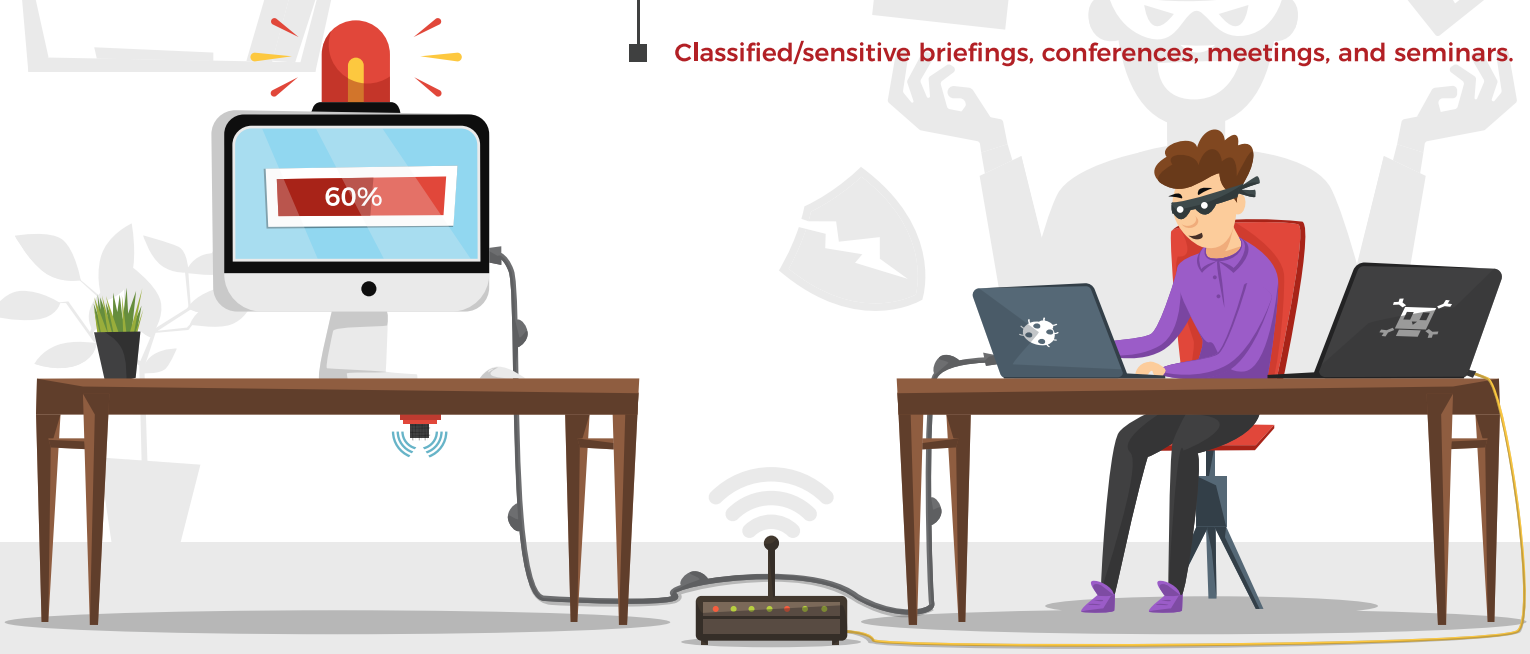
- Without need or authorization, takes proprietary or other material home via documents, thumb drives, computer disks, or e-mail.
- Inappropriately seeks or obtains proprietary or classified information on subjects not related to their work duties.
- Interest in matters outside the scope of their duties, particularly those of interest to foreign entities or business competitors.
- Unnecessarily copies material, especially if it is proprietary or classified.
- Remotely accesses the computer network while on vacation, sick leave,or at other odd times.
- Disregards company computer policies on installing personal software or hardware, accessing restricted websites, conducting unauthorized searches, or downloading confidential information.
- Works odd hours without authorization; notable enthusiasm for overtime work, weekend work, or unusual schedules when clandestine activities could be more easily conducted.
- Unreported foreign contacts (particularly with foreign government officials or intelligence officials) or unreported overseas travel.
- Short trips to foreign countries for unexplained or strange reasons.
- Unexplained affluence; buys things that they cannot afford on their household income.
- Engages in suspicious personal contacts, such as with competitors, business partners or other unauthorized individuals.
- Overwhelmed by life crises or career disappointments.
- Shows unusual interest in the personal lives of co- workers; asks inappropriate questions regarding finances or relationships.
- Concern that they are being investigated; leaves traps to detect searchesof their work area or home; searches for listening devices or cameras



Many people experience or exhibit some or all of the above to varying degrees; however, most people will not cross the line and commit a crime.

Some of the reasons to request a TSCM service may include, but are not limited to:

- Renovations or modifications to the area.
- Items received from foreign governments as gifts.
- Unrestricted/unescorted access by unauthorized individuals.
- Classified/sensitive briefings, conferences, meetings, and seminars.



- Changes to security operations procedures that could facilitate the compromise of information and material.
- Discovery or suspicion of a technical penetration, an unauthorized device, or a technical security hazard.
- Renovations/upgrades to equipment, furniture, and/or protection systems within the area.

TSCM services are tailored to meet local operating conditions based on the level of threat and potential vulnerabilities. TSCM services are categorized as "recurring" or "special." Recurring TSCM services are conducted on a schedule that provides the highest protection standards for highly sensitive information.

TSCM Survey

A TSCM Survey, which includes anomaly resolution and penetration investigations, is the most comprehensive of the TSCM operational activities. The TSCM Survey includes thorough instrumented, physical and visual examinations by the TSCM Team to identify the presence of technical surveillance devices, technical security hazards and weaknesses, and physical security weaknesses.

TSCM Inspection

A TSCM Inspection is a limited activity addressing specific concerns. An inspection evaluates the changes to the operating environment and ensures that no vulnerabilities were created by modifications. Inspections also are required to assess the technical integrity of furnishings, electronic equipment, proposed or completed construction, gifts or installation of items not previously examined by the TSCM Team.

TSCM In-Conference Inspection

A TSCM In-Conference Inspection is a limited service, normally provided in conjunction with classified/sensitive briefings, conferences, meetings, and seminars, in an area that is not normally secured but must be employed due to the size of the specific activity or the unavailability of suitable space in secure areas. This is primarily a limited inspection of the technical attributes of the facility before, during, and (as necessary) after the activity.

TSCM Advice and Assistance

TSCM Advice and Assistance is a service conducted before and or during construction or renovation of a new or existing area to ensure that appropriate physical and technical security standards or vulnerabilities are addressed prior to procurement to avoid costly modifications. This service is also appropriate prior to the purchase, replacement, installation, and going “live” with electronic systems, such as video teleconferencing systems and telephone systems.

About BugSweeps.co.nz - Technical Surveillance Counter Measures

TSCM NZ are the most experienced, trained, professional and capable Technical Surveillance Countermeasures sweep organisation in New Zealand.

Our staff are highly skilled investigators with years of experience in the field of covert investigations. We are committed to maintaining an in depth knowledge of devices, methods and tactics used by persons attempting to obtain information and intelligence that can be used for monetary gain, blackmail or personal knowledge.

Our working knowledge in the use of electronic & digital eavesdropping devices is second to none, and we pride ourselves in keeping abreastin the ever-changing world of sophisticated covert spying equipment.

We have carried out hundreds of technical sweeps across New Zealandfor some of the country's largest private organisations and government agencies.

Are you concerned about the security of your information?

TSCM NZ

Give us a call, we are happy to discuss your concerns in confidence on 0800BUGSWEEPS (08002847933) or email us at info@bugsweeps.co.nz.