Implementing Electronic TSCM Sweeps

Enhancing Corporate Security and Privacy
with Technical Surveillance Countermeasures and Threat Analysis

by Charles Patterson, President, Exec Security TSCM

What is Technical Surveillance Countermeasures (TSCM) and why are electronic sweeps necessary?

Technical Surveillance Countermeasures, or TSCM, refers to the field of eavesdropping detection and protection from any sort of technical surveillance. It is sometimes referred to as electronic bug sweeps but it is much more than just searching for hidden radio transmitters. A more appropriate description would be **Technical Threat Analysis**. TSCM includes methods of detection and defense against technical, electronic, and cyber surveillance threats that might be used for corporate or industrial espionage and other unlawful or unethical activities. All corporations should understand the importance of protecting the privacy and confidentiality of their business communications, discussions, meetings, and conversations. Protecting this information provides the foundation for the company's stability, profitability, and long term success. Loss or theft of information can cause serious harm to areas such as business development, product research, stock prices, brand reputation, and corporate litigation. Electronic TSCM inspections are an important part of the corporate security program. When preventative security measures are undertaken many serious and damaging problems can be avoided.

Fortune 500 and other high profile companies successfully implement TSCM as an integral part of their information security strategy. Smaller companies, as well, have found that introducing the proactive security measures of TSCM early on helps prevent major problems later. Understanding the importance of protecting communications and information helps increase security awareness and creates an atmosphere where such inspections are not only accepted but expected.

Corporations should have a culture where protecting information assets as well as protecting privacy through proactive TSCM inspections is an accepted part of security in the workplace. We have developed a simple process that all businesses can follow in order to integrate TSCM inspections into their security programs. For more information regarding what is involved in a TSCM sweep and how they are performed, please find more details on our website https://execsecurity.com/tscm.

The following information was prepared by the team at Exec Security TSCM, www.execsecurity.com. We have been providing professional TSCM services for over thirty years, with experience in many aspects of security and electronic communications.

We can help you understand the risks, threats, and vulnerabilities that affect your business. If you would like our assistance, we can start with simple discussions but we can also present more thorough recommendations after visiting your location for a site survey and assessment. Protection of your business information is our primary concern.

When planning for information security, an important requirement is to establish a relationship with a reliable and professional electronic countermeasures firm such as Exec Security TSCM. As a full-time TSCM provider we are available for our clients at any time, not just for sweeps, but also for consultation when any questions or concerns arise. We can arrange proactive inspections on a regular schedule or on short notice for special events and other concerns. We are also available for immediate response when a security incident may occur, and can help you decide on appropriate actions even when sweeps may not be immediately necessary. Contact us with any questions you may have or if you would like assistance with integrating TSCM and electronic privacy sweeps into your security program.

Charles Patterson, President
Exec Security TSCM
www.execsecurity.com
914-819-5400

Step 1: Risk Assessment

As with all aspects of security, performing a risk assessment is an important first step in order to understand the need for TSCM inspections, as well as how and where they should be applied. It involves reviewing your business operations, locations where information is stored and discussed, and what activities may require additional protection due to their sensitive or confidential nature.

When undertaking this assessment, be sure to consult with a TSCM specialist if any questions arise. It can be important to have a professional, objective perspective included in your planning process.

Every business and corporation operates differently, so there are a variety of aspects to consider when performing a risk assessment. Below are some examples that may help you in establishing which areas need the most protection.

A. Identify the critical areas that may require confidentiality:

- Examples of departments and vulnerabilities that should be given attention
    - Executives and C-Suite offices have regular meetings, discussions, and conversations taking place.
        - Executive offices
        - Conference rooms
        - Board meetings
        - Offsite meetings
    - Human Resources
        - Hiring and firing of staff
        - Salary information
        - Personal information
    - Legal Department
        - Ongoing law suits
        - Litigation strategy
    - Research and Development
        - New plans and products
        - Trade secret discussions
    - Business Development
        - Product launch dates
        - Mergers and Acquisitions
    - Financial
        - Competitive bids
        - Other financial information
    - Supply Chain Management
        - Interception of product data
        - Sabotage
- Event Planning
    - Locations and schedules of meetings
    - Attendees or guest speakers
- Executive Scheduling / Travel
    - Travel information could lead to kidnapping or personal attacks
    - Activists or protestors planning harassment, intimidation, or embarrassment
- Executive Protection Teams and Security Details
    - Compromise of protection plans and procedures
    - Organized attacks
    - Most serious attacks on principals are preceded by covert surveillance.

B. Identify locations where confidential information is discussed and communicated:

- C-Suite Offices / Executive Offices
- Executive Dining Rooms
- Conference Rooms
- Teleconference Rooms
- Auditoriums
- Executive Aircraft and Vehicles
- Executive Residence
- Remote Locations
    - Hotel Suites
    - Hotel Meeting Rooms
    - Dining Areas
    - Conference and Convention Spaces

C. Evaluate and prioritize the various aspects of your business:

- Create a list of the areas mentioned above that are most significant.
- Assign a priority level to each area as appropriate.
    - A simple approach would be to set three levels:
    - Basic Security - Medium Priority - Highly Confidential
- Based on the level of confidentiality for each area, consider inspection schedules as presented in the next section.

Step 2: Establish When Sweeps Are Needed

Categories of sweeps

TSCM inspections typically fall into one of three categories:

- Proactive, recurring inspections.
- Special event sweeps.
- Incident response sweeps.

Understanding each type of sweep will help organizations develop the strategies and policies necessary to improve their privacy and security.

Proactive and Recurring

Proactive sweeps are inspections performed on a regular basis throughout the year. They are highly effective not only in finding and eliminating active eavesdropping threats, but they also help to identify security vulnerabilities and monitor potential technical threats. Ongoing inspections are critical to help note any changes in the environment that could indicate vulnerabilities or be an indication of malicious activity or potential eavesdropping concerns. These could include the introduction of new audio-visual or communications equipment, changes in room functions, legacy equipment open to compromise, and other concerns, all of which are examples of issues we have come across that compromised the security of the areas.

There is also a deterrent provided by having proactive inspections performed, as they help employees understand that security procedures and countermeasures have been put in place, and to recognize the importance placed on privacy and confidentiality.

Scheduling proactive sweeps establishes corporate due diligence which is a critical part of conducting duty-of-care for protection of information. Such security measures are also necessary to help establish trade secret status of any information being discussed. If such information is leaked, it may not be considered theft of trade secrets unless it can be demonstrated that security measures were taken to protect that information.

After determining the priority of the locations and areas mentioned above, plan an appropriate schedule for recurring TSCM sweeps. Typical and recommended schedules include:

1. **Quarterly:** A quarterly schedule is considered the standard for highly confidential and high priority spaces. These would include the C-Suite executive offices and meeting areas, but is not necessarily limited to those. Depending on the level of discussions and communications taking place, other locations may also be included and increased frequency may be desired.
   Quarterly inspections also provide the ongoing threat assessment that is needed to be able to identify vulnerabilities and changes that may occur such as in the facility structure, introduction of new signals or communications systems, and other noting any abnormalities that could indicate potential surveillance or espionage.
   Recurring sweeps become even more significant in situations where an incident has occurred and a rapid response is needed. Your TSCM provider will already be familiar with the areas and will have a baseline for comparison from previous signal records and other tests.
2. **Semi-annual:** Semi-annual inspections may be adequate for less critical areas that continue to have confidential meetings and discussions periodically. Providing TSCM inspections twice a year also provides a good beginning step as well as a foundation for your TSCM provider become familiar with your facility.
3. **Annual:** Annual inspections may be appropriate for areas that are perhaps a lower priority or are still sensitive but may be less active. This could apply to auditoriums or conference rooms that are only occasionally used for confidential meetings or for offices that handle sensitive information on a less frequent basis.

Regular inspection during construction or remodeling and other infrastructure changes to your offices is also important for protecting your information and the overall health of your organization's privacy. Each visit establishes a benchmark for which future sweeps and changes can be compared.

The TSCM schedule should also be re-evaluated periodically. Changes may occur over time regarding the functions or activities in various offices or conference rooms in your facilities. That could cause a need to adjust the priority level assigned to the locations.

Special Event Sweeps

Off-site events often involve confidential meetings and conferences that require TSCM inspections. Consideration of information security and the need for TSCM sweeps should be included in the planning process for all important meetings and programs.

Event planners and those organizing corporate programs may not have privacy and information security in the forefront of their minds, so it is important for the security professional to bring it to their attention and see that arrangements are made in advance. Remember that both on-site events as well as off-site programs may need attention. On-site events might be held in less secure spaces and they may bring guests or visitors into your facility that have not been thoroughly vetted, prompting sweeps be performed after the event has concluded.

The importance of electronic sweeps for off-site events also underscores the fact that security and access control at such locations are typically much less than what might be found at your corporate facilities. A conference center or hotel, while they may be concerned about safety and physical security, may not see information security as a priority. They are also dealing with multiple guests and a variety of simultaneous events and will not be able to offer the level of attention needed for ensuring the confidentiality of your event.

Typical events that require TSCM sweeps:

- Board Meetings and Shareholder Meetings
- Senior Management and Partner Meetings
- Mergers and Acquisition Discussions
- Audit Committee Meetings
- HR, Financial, and Legal Team Activities
- Industry Events and Conferences
- Private Meetings

Security considerations may need to include more than just pre-event sweeps:

- Real-time monitoring and live analysis of radio signals can be arranged to ensure no unauthorized transmitting devices and no other compromise or interception occurs during the meetings. Even though a thorough sweep has been performed, other personnel, such as hospitality staff or set up teams as well as attendees, may bring eavesdropping devices into the area. Extra care may be required to ensure the level of security needed.
- The TSCM team can also include a detailed inspection of the audio-video systems to ensure they are not leaking information due to compromised conference lines or unsecured wireless devices. Translation devices or assistance for the hearing impaired often transmit meeting audio over long distances.
- Control of cellular phones or other electronic devices (such as laptops) entering the meeting may be desired. Limiting the use of cell phones in a meeting, although unpopular, is one measure to help secure highly sensitive meetings. This could also require physical inspection of attendee's possessions through the use of magnetometers, X-ray machines, or other procedures. Faraday boxes that can block cellular signals may be deployed so that attendee phones may remain nearby, yet still be protected against transmitting information.

- Plans for such considerations should be made well in advance of any meeting to ensure proper preparations can be made.

Incident Response Sweeps

Security related incidents as well as non-security matters may require that electronic sweeps be performed promptly. Whenever suspicious incidents occur, standard security procedures should include considering if TSCM inspections are needed. Could confidential information have been leaked, surveillance devices installed, or privacy breached in some way during the incident?

Security related incidents that might create a need for TSCM inspections could include:

- **Break-ins or theft** may be more serious than they initially appear. An apparent break-in or theft may have been a cover to hide a more serious threat of the planting of eavesdropping devices.
- Access by **Contractors** or other persons to unauthorized areas may indicate that the security of confidential offices was breached. Contractors may also have legitimate access to secure areas. A sweep should be considered after their work is completed.
- **Sexual harassment incidents** may require inspection for cameras or other surveillance devices.
- **Discovery of an illicit device** such as a camera in one location may necessitate that a full professional inspection be performed of that area and other locations as well.
- **Reports of suspicious activity** by employees may create the need for further investigation. Many eavesdropping incidents are revealed because the perpetrator's actions or comments raised suspicion in fellow employees.
- **Cybersecurity incidents** may also involve electronic devices. Rogue access points and other misuse of technology often go undetected by typical network security measures. A professional TSCM team can arrange to conduct special cyber related tests including wifi and VOIP inspections.
- **All security breaches** should be considered cause for concern if they could have allowed a breach of privacy or access to confidential areas.

Other types of incidents that may be of concern:

- When an **employee or executive is terminated** or quits suddenly, consideration should be made as to whether they had access to confidential information in the course of their responsibilities. Consider if they were involved with data or telecommunications systems, or if there were any suspicious circumstances surrounding their exit. Many breaches of telecom systems have occurred after a disgruntled employee from that department was terminated.
- **Termination of the CEO or company president** regularly necessitates a TSCM inspection as part of due diligence. The same may be required for other C-Suite executives as well.
- Employees who were found to act in a **suspicious manner** or new hires that may be given access to sensitive information will also require consideration.
- **Visitors** from other companies who had access to confidential areas may trigger the need for a sweep, especially if they were from competitors or from other countries.
- **Moving** to a new facility, or executives relocating to new offices, often require sweeps to be performed as it may be unknown who had prior access to the space.
- **New construction** both of offices as well as executive's homes may create a concern as the locations will have been accessed by numerous outside contractors, any of whom could have had ample opportunity to install surveillance devices.

The TSCM response to any incident will be better implemented if regular, proactive sweeps have been performed. Working with a TSCM team that has conducted regular inspections means that whenever incidents do occur the team will already be on board, familiar with your facility, and be able to respond in a timely and efficient manner. Records from previous sweeps, such as known radio signals and other findings, will allow for a much more effective inspection after an incident has occurred.

Step 3: Incorporate TSCM in Your Security Policies

Business Policy Development

Policies and procedures should be established that clearly indicate where and how often security sweeps should be performed. Every company will have slightly different needs and requirements. Presented here are a few considerations that can be adapted to various situations. By understanding priorities and how your business conducts its activities, the appropriate TSCM response can be selected.

Policy for Proactive Scheduled Sweeps

Recurring inspections will help provide a baseline which will allow future sweeps, including special events and incident response, to be much more effective. Review of data from previous sweeps can provide comparative data that will improve the value of future inspections.

Regularly scheduled sweeps also set a precedent, establishing that both information and verbal communication are considered confidential and proprietary. This is critical where trade secrets are concerned. If adequate information security measures are not in place, courts may determine that any information that was stolen or leaked cannot be considered a trade secret and was not truly confidential. In such cases the theft of the information may not be prosecutable, and the information no longer classified as private.

Defining a clear proactive TSCM policy will also enable the decision makers in your organization to take a more active role in information security.

Special events

Establishing a policy for special events will help to ensure that the security of events is not overlooked.

The need for TSCM inspections should be brought to the attention of the organizers as soon as event planning begins, and can then be coordinated along with more traditional security requirements. Event planning can be a long and complicated process so the sooner organizers know to address information security needs, the better prepared they will be.

Incident response

Company policies should include the consideration of electronic TSCM sweeps as part of the response procedure for many types of incidents, both security and non-security related. The occurrence of incidents such as a break-in or theft from a sensitive office should automatically trigger a request for an electronic sweep for surveillance devices to be conducted. This does not mean that sweeps are needed for every type of incident, but analysis of each incident should include consideration of information security and privacy.

The same is true for departmental incidents, such as the termination of an employee under suspicious circumstances. Legal, human resources, and financial departments all may have situations that do not fall directly under security responsibility, but may require TSCM inspections for protection of company secrets and privacy.

General Policy

Employees as well as executives should be aware of the need for information security. They should also be encouraged to speak up if they suspect problems with security or privacy.

Clear policies will help employees recognize that the information they handle is considered confidential, and they should know who to contact if they suspect something improper may be going on. Many incidents of corporate eavesdropping are exposed due to another employee reporting a suspicious occurrence or situation.

It can also be helpful for department heads - such as legal, financial, human resources, and others - to know that electronic sweeps to protect their privacy are readily available any time they may suspect a concern.

Shared responsibility and awareness

Based on the assessment of departments, locations, and their confidentiality, company policies can also be designed so that some of the responsibility for requesting TSCM inspections can be shared with the various departments and locations. In this way the burden does not have to fall completely on the security department.

This approach may not be appropriate for all organizations, but it is worth considering. There are a number of possible benefits from this approach.

- Departments and their employees will be prompted to think more seriously about information security.
- Department heads may also have a better understanding of their needs and the confidentiality requirements of their offices than would the general security department.
- Budgetary considerations for sweeps could also be distributed among appropriate cost centers.

Conclusion

Protecting privacy and securing confidential information is one of the most important jobs of security. As evidenced above, there are many reasons why TSCM inspections may be needed and also many ways that sweeps can be implemented.

Large corporations may be working on multi-million and billion dollar contracts. Executive decisions and communications require a high level of confidentiality just as a matter of duty of care.

Small businesses are also in need of protecting their communications and information and are no less a target of espionage. A small company may be providing an important service or product for larger corporations. They then becomes an easier target than a large, more secure corporate facility. Their competitors may also have strong motivation to learn their confidential plans.

Electronic countermeasures should be a welcomed and expected security service in all businesses. There are such a large number of technical threats today, Technical Surveillance Countermeasures should be understood, readily accepted, and easily put into action. Be sure you contact professional TSCM providers for assistance.

As an experienced and professional TSCM provider, Exec Security TSCM is happy work with you to develop a plan that fits both your needs and your budget. Contact us for assistance or with any questions you may have.