Implementing Electronic TSCM Sweeps

The Process to Enhance Corporate Privacy and Security
with Technical Surveillance Countermeasures

by Charles Patterson, President, Exec Security TSCM

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

Technical Surveillance Countermeasures, or TSCM, is also known as eavesdropping detection and electronic bug sweeps. It includes methods of defense against technical, electronic, and cyber surveillance used for corporate and industrial espionage and other unlawful or unethical activities. Businesses need to understand that protecting the information and privacy of their business and their employees 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. They should include electronic TSCM sweeps in their security programs. When preventative security measures are undertaken many problems can be avoided.

Many high profile companies have successfully implemented TSCM as an integral part of their information security strategy. Smaller companies, as well, have found that implementing such proactive security measures early on helps prevent major problems later. Understanding the importance of protecting communications and information helps to create an atmosphere where security inspections are not only accepted but expected, and it helps to increase security awareness throughout the company.

Corporations should work to develop an atmosphere where proactive TSCM sweeps are an accepted part of security in the workplace, protecting information assets as well as protecting privacy. We have developed a simple three step 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 visit execsecurity.com/tscm.

This information was prepared by the team at Exec Security TSCM, www.execsecurity.com. We have been providing professional TSCM services for over twenty 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 simply with discussions over the phone, 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 immediately be 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. It is 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 can help you start the process of establishing which areas need the most protection.

A. Identify the critical areas that require confidentiality:

- Examples of departments that may need attention
  - Human Resources

    Vulnerable information:
    - Hiring and firing of staff
    - Salary information
    - Personal information
  - Legal Department
    - Ongoing law suits
    - Litigation strategy
  - Research and Development
    - New plans and products
    - Trade secrets
  - Business Development
    - Product launch dates
    - Mergers and Acquisitions
  - Financial
    - Competitive bids
    - Other financial information
  - Supply Chain Management
    - Interceptions of product data
    - Sabotage
- Event Planning
  - Locations and schedules of meetings
  - Attendees or guest speakers
- Executive Scheduling / Travel
  - Protection against kidnapping or attacks
  - Those seeking to harass, intimidate, or embarrass
- Executive Protection and Security Details
  - Compromise of protection plans and procedures
  - Organized attacks
  - Most serious physical attacks on principals were 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 Sweeps
- Special Event Sweeps
- Incident Response Sweeps.

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

Proactive and Recurring Sweeps

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

Scheduling proactive sweeps establishes corporate due diligence which is a critical part of conducting duty-of-care for information security.

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

1. **Quarterly:** A quarterly schedule is recommended for highly confidential, high priority, active spaces. Depending on the nature and confidentiality of your business activities a more frequent schedule of sweeps of sensitive areas could be in order. These would include the C-Suite executives 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.
2. **Semi-annual:** Semi-annual inspections may be adequate for less critical areas that continue to have confidential meetings and discussions periodically. Providing the sweep inspections twice a year provides a good foundation for your TSCM provider to familiarize themselves with your facility and the electronic environment. This becomes even more significant in situations where an incident has occurred and a rapid response is needed.
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.

Having your TSCM provider visit your facility regularly, especially during construction and other infrastructure changes to your offices, is very 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 will be compared. If an incident were to occur in an office that is swept regularly then your organization would be better able to understand what information may have been compromised as well as have a better chance to discover the persons responsible.

Keep in mind that changes may occur over time in the functions or activities in your facilities that could cause a need to adjust the priority level assigned to a certain location. The TSCM schedule should be re-evaluated periodically.

Special Event Sweeps

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

Event planners and those organizing the 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 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.

The importance of electronic sweeps for off-site events is also underscored due to the fact that security and access control at such locations are often 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, are also dealing with multiple guests and a variety of 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
- Shareholder Meetings
- Senior Management Conferences
- 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-meeting sweeps:

- Real-time monitoring and 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 sweep has been performed, other personnel, such as hospitality staff or set up teams as well as attendees that have legitimate access to the space, 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.
- Control of cellular phones or other electronic devices (such as laptops) entering the meeting may be desired. The banning of cell phones is one measure to help secure highly sensitive meetings. This could also require physical inspection of attendees through the use of magnetometers, X-ray machines, or other countermeasures including walk-through cellular phone detection.
- These should be planned well in advance of the 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 TSCM sweeps. Could confidential information have been leaked, surveillance devices installed, or privacy breached in some way?

Security related incidents:

- **Break-ins or theft** may be more serious than they initially appear. An apparent theft may have been a cover to hide the planting of eavesdropping devices.
- Access by **Contractors** or other persons to unauthorized areas may indicate that the security of confidential offices was breached.
- **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 professional inspection be performed of that area as well as other locations.
- **Reports of suspicious activity** by employees may call for further investigation. Many eavesdropping incidents are revealed because the perpetrator's actions or comments raised suspicion in fellow employees.
- **Cyber 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 is equipped 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 information.

Other types of incidents:

- Whenever an **employee or executive is terminated** or suddenly quits, 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.
- **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 one of whom would 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 provided regular sweeps means that whenever incidents do occur they will already be 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 network attributes 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 when and where security sweeps should be performed. Every company will have slightly different needs and requirements, but 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 sweeps will help provide a baseline by which future sweeps, including special events and incident response, can be measured. Records kept from each sweep can be reviewed to provide comparative data that will assist future inspections.

Regularly scheduled sweeps also set a precedent, indicating 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 conclude that the information that was stolen or leaked was not truly confidential and therefore its theft may not be prosecutable, and the information no longer classified as private.

Defining a clear proactive sweep 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 about 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 an electronic sweep for surveillance devices. This does not mean that sweeps are needed for every 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 conversation.

Department heads, such as legal, financial, human resources, and others, should know that electronic privacy sweeps 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 scheduling 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. Benefits from this approach are multifaceted.

- Departments and their employees will be prompted to think more seriously about information security.
- Department heads may have a better understanding of the confidentiality requirements of their offices than would the general security department. By working together they will provide better information security for the company.
- Some of the difficulty of scheduling sweeps can be shared with the departments, possibly freeing up security resources. There is still a need to coordinate the scheduling and the results with the security management. The departments can be held accountable, though, seeing that inspections are requested, scheduled, and carried out in timely manner.
- Cost for sweeps can also be distributed among appropriate departments. Departments handling classified information may then feel more responsible for its protection.

It is important, though, to establish protocols that are fairly simple and easy to enact. This will ensure for more effective resolution of problems in the long term.

Conclusion

Protecting privacy and securing confidential information is one of the most important jobs of security today, and as such, it should not be taken lightly. As evidenced above, there are many reasons why TSCM inspections may be needed and also many ways they 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.

Small businesses as well are in need of protecting their communications and information and are no less of a target of espionage. They may provide a service or product for larger corporations. The smaller company then becomes an easier target than a more secure corporate facility. Their competitors may 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, TSCM should be readily accepted and easily put into action. Be sure you contact true professionals 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 with any questions you may have.