www.execsecurity.com
914-819-5400 / 800-337-2001

Understanding Proactive TSCM

My company has been providing professional TSCM services for over 25 years. We have found three categories of why professional TSCM may be requested for a corporation.
These include

- Proactive TSCM
- Special Event TSCM
- Incident Response.

Proactive TSCM may be the most significant. It involves establishing ongoing security practices, conducted on a regular basis, that help to secure communications and information. TSCM for special events such as board meetings could also be considered also proactive in nature, but events require special considerations to ensure proper coverage. Management or board meetings may be held off-site, in less secure areas, or have a significantly higher threat level.
Incident response, or "reactive" TSCM, is often, unfortunately, the reason a company starts looking into TSCM sweeps in the first place, when a possible leak or theft of information has been discovered. Proactive TSCM provides the foundation that the other sweep categories depend on.

When considering any solutions for information and communications security, it is important to be able to see the larger picture of what is really needed to do the job well.

TSCM or Technical Surveillance Countermeasures is often mistakenly thought of as "bug sweeps", or just using simple receivers to detect radio signals that could be coming from a listening device. That concept is very outdated as well as inaccurate and misleading.

Protection against technical surveillance requires a complicated array of technical procedures and tests. They work together to help combat the multitude of ways that information and communications may be compromised today through various technical means.

One of those methods certainly could be via radio signals. Signals found in any area need to be analyzed with scrutiny and understanding. No longer can you just tune into a signal and listen to it and determine if it is from the secure area, digital and encrypted signals abound everywhere. There are a large number of expected and authorized signals in any area that may appear identical to a malicious signal that could be in the same room. Coordinating the variety of TSCM tests can be thought of as helping to create a tight web or net, so that any suspicious or malicious activity will not slip through and will stand out and be detected.

When a company is planning to spend large sums of money on any aspect of security, especially protecting their confidential data and communications, they should be able to do so with confidence that the chosen solutions have been proven in the field. They do not want to open themselves up to other security concerns or vulnerabilities perhaps by being over-confident in some simplified steps they have taken.

www.execsecurity.com
914-819-5400 / 800-337-2001

In-place monitoring or continuous monitoring of an area for suspicious signals is one technique that can help detect suspicious signals. It was often considered to be more effective in years past, when radio signals were less abundant and most were analog in nature. Analog signals could be easily recognized and then listened to for determining if they were coming from the secure area. With today's digital signal environment it is much more difficult to do effectively as there are numerous "authorized" signals everywhere, from cell phones, to watches, to light switches, motion sensors, climate control, and more.

A number of companies offer systems that can provide continuous monitoring of radio signals within a facility. They typically involve numerous expensive sensors that need to be installed throughout the facility and networked together, along with the need to transmit their detection results to an outside provider for analysis. This could work well, but there are a number of challenges for such a system to be effective. This not only includes the cost of installation and ongoing monitoring costs, but also difficulty in setting up of the signal detection system - determining authorized vs unauthorized signals. The detection results will need to be analyzed, usually being sent to an outside service for such analysis. Then there will also be the need to be able to provide an appropriate response to any alerts that are received. All of which require highly trained and knowledgeable personnel.

If implemented well, such systems could help address that part of TSCM that involves radio signal analysis. It would not at all, though, eliminate the need for professional TSCM sweeps as there are many other aspects left unaddressed. These could include such threats as a voice recorder left under a table, a hardwired mic run through the ceiling, even a dormant cellular transmitter waiting to be woken up at the appropriate moment. Such a transmitter might reveal itself to the "in place system" once it begins transmitting - but how quickly would you get that alert and would you be confident enough to stop the meeting and have the room and all attendees searched at that time? If your executives are on board with that type of security response, then consider yourself among the very privileged.

Radio signals are just one potential threat to be considered. A professional TSCM team will know that multiple areas of testing and inspection are needed, as mentioned, threats from radio transmissions are just one aspect. Of the many professionals I know, they generally agree that most malicious discoveries are made through a serious and thorough physical inspection in combination with the other TSCM techniques. Even when suspicious radio signals are detected, finding the source still requires an in depth physical search to be conducted.

When looking at the holistic security view, there is also the need for strict policies to be implemented covering such things as cell phone usage, electronic devices allowed on site, establishing secure meeting rooms, etc. You must also have staff that can help to implement these policies. Unfortunately, most companies now cannot even get their board members to turn off their cell phones during confidential board meetings. Security directors need to consider this bigger picture. How much do their executives understand the concerns at hand?

If a company is serious about protection of their communications and information, they should certainly consider all of the many aspects of security available, but they should also not think that other procedures are no longer necessary just because they have been sold a "do it all" kit.

www.execsecurity.com
914-819-5400 / 800-337-2001

It is a common misconception that TSCM is just "bug sweeps" or "hidden camera detection" which can be done with inexpensive equipment and in a short amount of time. That might be like saying that having a first-aid kit plus a basic first-aid class is as good as having paramedics with a full ambulance on site. There is really no comparison. Yes, any amount of first-aid training is better than none, but that may not be sufficient to address your needs. The TSCM professional will have hundreds of thousands of dollars invested in their equipment plus hundreds of hours of high level training as well. A professional TSCM provider can also provide the necessary consultation to ensure the client has appropriate security measures in place.

We have been encouraging proactive TSCM for many years. What that really means is first understanding the risks and threats that you are facing, and then establishing appropriate security practices that take place on a regular basis. This might include installation of RF sensors, or requiring all employees to go through electronic screening when entering or leaving the property, but it is important to understand that no one step will solve all of the concerns.

Any security planning should also involve a developing a relationship with a professional TSCM provider. They can help with identifying the areas that need protection the most, as well as conducting regular, professional TSCM sweeps of those areas. This will be a critical step. Then conducting inspections prior to all important meetings is also a key consideration. Changes in the RF environment as well as changes in external environment will be noted by the TSCM team during the regular proactive inspections. Small differences from one sweep to the next may point to possible malicious activity as well as other vulnerabilities. A professional TSCM provider will also be able to assist with selection of any long term solutions such as RF monitoring, window films, x-ray machines, or sound masking.

Having proactive sweeps performed regularly will also make any "reactive" or incident response much more effective. The TSCM team will already be familiar with the site and they will have logged baseline information such as RF signals and other data that will assist in determining if and where a malicious event has taken place.

When your company is dealing with high value, confidential data and communications, remember the importance of proactive professional TSCM services.