The TSCM Enigma

Effective Use of Technical Surveillance Countermeasures Professionals

By Douglas A. Roth

Warriors of the information age, Technical Surveillance Countermeasures practitioners remain a rare hybrid between the technical and security professions. TSCM professionals are being sought with more frequency and concern as emerging technologies continue to expose the soft underbelly of both companies and individuals.

What is TSCM (Technical Surveillance Countermeasures)?

Commonly referred to as "debugging," Technical Surveillance Countermeasures or TSCM, detect the presence and location of active and passive eavesdropping and surveillance systems. TSCM also identifies existing and potential security weaknesses -- wherever encountered.

TSCM is conducted with varying degrees of frequency within government, industry and the private sector worldwide to combat espionage and other identified threats. TSCM is also a routine of life for numerous entertainment and sports celebrities, or other high profile persons.

TSCM is largely directed toward the protection of information, although they will often reveal physical security problems as well.

Typical projects undertaken by a TSCM firm include the discovery and removal of illegal eavesdropping systems, consultation on matters related to information security, support of personal protection details, provision of secure environments for special meetings or activities, and security surveys.

Who are TSCM Professionals?

TSCM trade craft encompasses many seemingly unrelated disciplines including, electronics, security, investigation, communications technology, lock smithing, alarms, chemical munitions, photography, video, automobile systems, building construction, HVAC, fire alarm systems, access control systems, computer science and covert operations.

A legitimate TSCM firm comprises one or more individuals, whom have received extensive training, possess expensive and varied equipment, and through years of experience have acquired valuable knowledge of their profession.

Many TSCM professionals possess a government or law enforcement background. Regardless of their background, competent practitioners maintain active in-service training schedules often offered through manufacturers of telecommunications and computer equipment and in a limited number of specialized private schools.

A TSCM professional can provide insightful and meaningful support for an equally diverse array of security and management concerns. One example can be found in the role TSCM can play in the establishment of legally defensible business or trade secrets when TSCM programs are established on an ongoing basis for such purposes.

James A. Lupori, of Western Research and Investigation, Culver City, California, states "all the equipment in this business is just an aid. The real skill lies largely in the proper reading and interpretation of positive test findings."

It is important to check the technical background and qualifications of a prospective TSCM firm. The integrity and ethics of these contractors should be beyond reproach due to the sensitive nature of their work on your behalf.

The Threat

The threat of a company or individual being targeted for illegal eavesdropping or surveillance is commonly believed to be dependant on industry type and market position. In reality, any person or company with power or money is at risk.

The threat is real, widespread and serious. Some of the more common applications of these eavesdropping and surveillance efforts include litigation support, acquisitions and mergers, and labor relations. Malicious activities have also been perpetrated on companies and individuals by disgruntled current or former employees. The random threat of terrorist activities is also the province of concern for many security professionals who are wise to recognize the financial prowess and technical abilities of elements within these organizations.

In relative terms, electronic espionage is easy, widespread and driven by seemingly endless financial incentives for those who choose to cross the line on behalf of others.

A report issued by the US State Department [1] recently estimated illegal eavesdropping devices entering the United States with an estimated value exceeding $500,000,000 annually. The sources of these shipments have been traced back to several countries of origin including France, England, Israel and Canada. This same report would indicate there now exist an entire underground industry and economy driven by the sales, installation and monitoring of illegal eavesdropping and surveillance devices which is estimated to be 2.2 billion dollars annually in the Unites States alone. This economy is further augmented by the existence of a growing subculture interested in the pursuit of protected information and proprietary resources. Law enforcement and security professionals have struggled to cope with the emergence of this subculture and the problems they pose -- real or imagined. It is estimated that law enforcement efforts in this area are running at least 15 years behind the industry.

Industry experts state that as much as $50,000 in illegal bugging or wiretapping equipment can easily be concealed in a laptop computer. This same laptop computer could be carried onto an airplane through normal security checkpoints and would be difficult to detect. U.S. Customs has also stated that they lack the training and resources to detect such activity.

Eavesdropping can be passive or active. That is to say the threat of losing critical information, for example, could be suffered when an opportunistic employee overhears a sensitive communication or when a computer modem is secretly exchanged for a pre-bugged modem. While many of these problems can be prevented or eliminated with proper access control methodologies, others elude easy detection. This is the province of the TSCM professional.

Today, it is technologically possible to intercept voice or data communications and processes in virtually all of their forms and manifestations. This includes telecommunications equipment; personal and mainframe computers, their peripheral devices and networks; facsimiles; and photocopiers.

In assessing a specific threat, it is helpful to remember that a full scale wiretapping operation at the corporate level commands an estimated average of $30,000-$50,000 per month depending on the geographic market and can be undertaken by virtually anyone with a technical acumen and minimal training. Similar and often equally effective operations are completed for far less money or cost to their benefactors. The cost of a court approved law enforcement technical surveillance operation is reported to have an average cost of $45,000, according to the Administrative Office of the U.S. Courts.

When and How to Engage TSCM Professionals

If reasonable suspicion exists that you may have become the target of electronic espionage it is important to act swiftly, quietly and without disturbance to the current situation.

Internal policies and procedures often dictate an appropriate response in corporate or government environments accustomed to dealing with such threats. For others, a proper course of action may be somewhat unfamiliar terrain. In either instance, TSCM services are likely in order.

A TSCM professional should only be contacted via controlled means and well beyond the targeted area. It is not recommended that a call or other communication is made to the professional from any telephone, computer, facsimile or other such method associated in any fashion to the targeted organization or individual. The obvious concern here is one

of alerting the eavesdropper or surveillant to your knowledge, suspicion or intent. Any TSCM operation performed subsequent to such an alert will likely be ineffective and a waste of financial resources. Be careful to not initiate the contact on a cellular or cordless telephone. A heavily used public telephone would likely be the most secure method by which you can discuss your problem and attendant needs. Arrangements can be made to cover all identified extenuating circumstances to maintain the desired level of security and integrity of the TSCM operation.

It is essential to provide proper background information to the TSCM professional. As with any professional relationship, trust and confidence are essential components to success. Background knowledge and intelligence will normally be sought and utilized by a reputable firm.

TSCM teams should also be provided a complete and full sized set of blueprints (including all landscaping) well in advance of the actual sweep. It is also beneficial to provide photographs of the facility to assist in the interpretation of the provided design plans.

TSCM sweeps are normally completed within a period of 2-3 days. Some teams will perform vulnerability sweeps preceding the actual TSCM and may require 2-3 days to complete this activity which involves a visual inspection of the premises. A professional and complete TSCM could take as long as 2-3 weeks depending on the size and scope of the operation including executive offices, residences and vehicles.

In general, it is better to schedule TSCM sweeps after hours when able. This arrangement will ensure the least number of personnel encounter the team. Specific case circumstances will ultimately dictate scheduling requirements.

Cost of TSCM Services

TSCM is often priced according to facility size, location, the number of active telephone lines or other transmission lines, and the scope of the matter at issue. Depending on the firm and market, TSCM services are charged on an hourly or daily rate basis, often by retainer agreement. Top industry professionals will receive $3,000 to $5,000 per day. One should be wary of "two week wonders" who will generally offer their services for lower rates than those established in your regional TSCM market.

A good TSCM professional will charge as much as a good attorney or surgeon and have an equally strong education and training background.

TSCM services may appear to generate windfall profits. In reality, a large investment in time, for in-service training, and money, for equipment, is required to maintain the standard of professionalism necessary to be effective in this arena.

Logistical and Security Concerns

It is important to maintain the integrity of communications between the client and the TSCM firm. To ensure an adequate level of security, it is beneficial to select one representative to undertake the responsibilities associated with conducting the TSCM operation. Strive to limit the number of individuals notified of an intended TSCM operation.

Typically, a bonafide professional TSCM team will desire to conduct their operation on their terms and recommendations. For this reason, it is important that concerns are discussed by the client and professional and that general guidelines are established. It is important that a schedule be established and followed to avoid unnecessary scrutiny of the team.

TSCM professionals will normally provide a recommended cover story under which they will conduct their activities. The client's representative may also provide a sturdier cover story given their knowledge of the organization. Cover stories should be designed for a long term relationship with the TSCM professional -- regardless of future intent. A typical TSCM operation involves the use of numerous pieces of electronic test equipment, computer devices, flashlights, and ladders.

TSCM activities could, in some instances, span a period of several days and involve access to numerous facilities. Access issues should be addressed prior to engagement. Specific access issues should be addressed internally and with the TSCM professional. In matters related to government, it may be necessary for the TSCM team to possess a security clearance.

Inevitably, the threat target includes specified key individuals within the company. These individuals are often targeted beyond the workplace. The vehicles, mobile communication devices, computer equipment, alarm systems and residences of these individuals should be subjected to TSCM.

Generally, informed recommendations to competent TSCM firms may be obtained from counsel or within the security and investigative industries. On occasion, it may be necessary to consider using a firm from outside your geographic area or beyond your established industry referral base.

As with any outside contractor allowed access to secured areas or areas containing sensitive information, TSCM personnel should be accompanied at all times when inside a facility or private residence. Serious professionals will not normally oppose these conditions but rather insist on them, providing an individual to answer questions during the sweep.

TSCM Reports

As with any professional undertaking, a verbal and written report should be provided in a timely manner. A verbal report will be provided immediately upon the conclusion of the engagement. At a minimum, the written report should contain a complete descriptive summary of activities and findings, and other actions taken by the firm.

Extremely sensitive findings or issues may necessarily be reported under separate cover or solely in verbal form.

Interpretation of a technical report of the nature common to TSCM can be difficult. Take time to ask questions and seek clarifications when reviewing these reports. A good TSCM report will be written in terms that can be commonly understood, not jargon. The best reports can be passed on to others without explanation and allow the reader to understand what occurred during the sweep even though they may not have been present.

It is advisable to maintain a secure archive of TSCM reports for comparison and reference. TSCM reports often contain valuable recommendations relating to all areas of security. These reports serve as useful guides or reminders when reviewing ongoing security issues and concerns.

Responding to Positive Findings

It is very important that preparations be made at the outset of any TSCM investigation for a positive finding. This is not to say that all or even the majority of sweeps produce evidence of a compromise, but rather to remind the reader of the inherent need should such a finding be made.

It is difficult to imagine what a positive finding could portend for an organization or individual. Eventual scrutiny of action taken during this critical period is very likely. At a minimum, positive findings should be documented by means of x-rays, video imaging, and still photography and a well organized report. All documentation should generate three copies before any law enforcement agency is contacted. The TSCM firm retains one copy, the company retains a second, and the best copy is provided to law enforcement.

If a device or system is discovered, several options would normally be available in response. You may consider the merits of 1) removing the device, 2) recruiting the agent who placed or is monitoring the device, or 3) using the situation to conduct a campaign of misinformation while internal and criminal investigation is pursued.

Criminal violations discovered by TSCM investigations are generally violations of federal law and investigated by the Federal Bureau of Investigation.

In the event of a positive finding of such a nature that requires the involvement of an outside agency, the TSCM team and client's representative should ensure the scene is cleared, secured and maintained as any crime scene. The scene may yield valuable physical evidence when analyzed by a skilled criminal forensics team.

Legal Considerations

Many, but not all, legal issues potentially encountered during the course of a TSCM engagement are contained in United States Code, Title 18, Chapter 119 which prohibits "any person who intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." [2] It is also a violation of state law in the vast majority of US states to install or operate an illegal wiretap or bugging device.

Other areas of the law may be encountered including issues of access to secured or proprietary areas, employees' right to privacy, and premise liability for the workplace as well as the private residence.

State and federal contractors may additionally be required by law to address issues of access control to areas requiring government security clearance.

Advanced Technologies, Advanced Problems

James M. Atkinson, of Granite Island Group, Gloucester, Massachusetts, indicates modern telephone switching systems used by the phone company are extremely vulnerable to external tampering. Telephone switching systems such as the AT&T 5ESS are often accessed by corporate spies (and hackers) whereupon the control programs (called "translations") are modified to allow calls to be remotely monitored. Such a tap requires only a phone line, and a laptop computer with a modem. Such access, when gained, is exceedingly difficult to detect or to protect from. In large measure, security is the province of the telephone utility at this level precluding the implementation of outside countermeasures efforts. Security consultants and professionals with valid concerns have found it valuable to establish working relationships with telephone company security professionals where a mutual threat is realized.

There is now an emerging trend of computers and computer peripherals being compromised by sophisticated bugging devices. These devices range from pre-bugged computer hard drives, video monitors and DAT data backup devices. With these devices, an eavesdropper can transmit a real time copy of information written to the hard drive or DAT drive of the targeted computer virtually simultaneously to a second off-site DAT device. Even computer hard drives can be compromised by two way remote access devices designed to allow remote access to information contained on them.

Closing Statement

Kevin D. Murray, of Murray Associates, Oldwick, New Jersey advises that recommendations provided during the course of a TSCM engagement should be implemented, thus reducing the potential for future problems while increasing the overall level of security.

Perhaps it is best to illustrate the TSCM enigma with one fundamental reality. The moment following the completion of the most proficient of TSCM sweep operations, there is no real assurance of security for yet another van may be passing your TSCM team in the night.

[1] U. S. State Department/DCI, March, 1997
[2] 18 U.S.C. Sec. 2511(1)(a)

About the Author

Douglas A. Roth is President and Director of Investigations of Investigative Resources International.

www.factfind.com | (562) 437-7709 Voice | (562) 437-0489 Facsimile