Technical Surveillance Counter Measures

"Do You Know Who is Listening?"

INTRODUCTION

In today's business landscape consideration of threat levels and protecting your intellectual property against outside entities is a growing concern for every organization. What is the cost of not utilizing a Technical Surveillance Countermeasure (TSCM) program in your daily business? Is the cost associated with the implementation of an effective TSCM program worth a loss on the bottom line of your business? Have you considered the negative impact on the reputation of your organization and the embarrassment to your Executives and Leaders?

DISCUSSION

When considering implementing a TSCM program an organization must identify exactly what type of information is to be protected from external threat elements. This may be intellectual property, critical business information, ideas, business processes, materials or its employees as whole. As a business, you need to know and understand where the threat is coming from. It could be business competition, foreign governments or an insider threat attempting to do harm to the organization for personal or financial gain. Although, the technology and techniques used in the deployment of surreptitious recording devices is ever evolving, Presidia has identified the foremost technical processes in today's environment to protect your organization from the following attacks:

- Acoustic and microphone hardwired electrical, telephone and computer feeds, photocopier lines, VoIP or Wi-Fi devices used to capture private communication during telephone conversation or board meeting scenarios commonly known as "wiretapping";
- Radio frequency (RF) and microwave transmitters with both analog and digital capabilities capturing both audio and video signals;
- Laser technology, a threat being utilized from a distance to gain information from your organization and business prospects;
- Hidden audio and video devices hand carried into your business by your staff or guests who have been invited into your organization. This method may come in the form of gifts, cleaning materials or daily administrative tools, such as staplers or general items utilized within the office environment;

- Overt recording devices with audio capturing capabilities on smart phones and computer devices brought directly into meeting rooms; and

- Finally, and often overlooked are corporate automobiles. A great deal of information can be gathered from within company vehicles in which executives travel in daily. Often this method is easier than infiltrating boardrooms and offices due to the lack of security placed on corporate automobiles when they are parked.

These threats have been observed by the Presidia team in both the corporate business environment and within government organizations. These types of technical strikes have caused a great deal of damage to both business reputations and profitability. How does senior management mitigate and institute preventative measures to eliminate such intrusion by outside entities? Some areas for consideration are:

- Adopting a robust TSCM program, which uses state of the art technical equipment and well trained TSCM Technicians with expertise, training and abilities to ensure your exposure to such technical threats are removed and mitigated;

- Using experienced TSCM professionals to identify, isolate and nullify vulnerabilities and weaknesses. TSCM professionals can also ensure that security needs are identified to assist the organization in preventing technical attacks;

- Conducting evaluations to identify best practices and recommend security measures to eliminate threats and vulnerabilities. Recommendations may include training of security staff or enforcing high security zones, which may eliminate the potential introduction of electronic devices into high level meetings;

- Educating employees so they understand that security is everyone's responsibility; and

- Maintaining a cost effective TSCM program that identifies regular technical sweep activities, pre-sweep activities and post sweep activities to prevent the loss of intellectual property and to ensure privacy for clients during sensitive negotiations.

CONCLUSION

In conclusion, a TSCM sweep should be considered as one-part of an ongoing and evolving security program. Building a defence to possible threats will assist with mitigating the risk to an organization. As the capability to intercept communications becomes more advanced and inexpensive to manufacture there will be a never-ending opportunity to access and steal information and intellectual property. Selecting a reputable TSCM provider who utilizes and deploys the latest technology in conjunction with well trained technicians will assist in protecting your company and its information.

About the Author

Dave STEVENS | Executive Security Specialist

Dave is a police and security professional with over twenty-five years of experience. He has managed the provision of security services to Canadian High Commissions and Canadian Embassies throughout the world as well as holding the position of Security Manager for the Canadian High Commission in New Delhi India. In addition, he has extensive experience in technical and mobile surveillance operations.

ADDITIONAL ARTICLES FROM PRESIDIA SECURITY

What Makes a Good Security Leader?

The list of traits attributed to great leaders is long and varied indeed: courage, strength, intelligence, honour, energy, adaptability, innovation, initiative – and there are many, many more. In fact, when it comes to discussing leadership attributes, journalists, historians and social scientists seeking to chronicle and analyze the exploits of great leaders are constrained only by vocabulary and imagination.

Ask the Question – What is My Security Strategy?

Security is often thought of as a tactical issue that should remain at the "gates and guards" level. While these tactical security pieces may be important they are most effective as part of a security strategy that is designed to mitigate the threats and risks to your company and its operations. True security strategy is integrated into a company's "C Suite" and is seen as an enabler. The questions and discussion that follow outline the framework for a company security strategy.

Assessing and Tracking Threats - Protecting Your Employees and Your Company

Recent incidents of violence in the workplace in Canada tragically illustrate what happens when threats materialize into actions; they serve as a stark reminder to businesses across the country of their responsibility to protect their employees in the spirit of "due diligence" and "due care and attention." Rarely, if ever, do these violent situations manifest themselves without some sort of prior indicators. This underscores the importance of having proper procedures in place to track and assess threats to your employees. Take the time to review the following recommendations to determine whether your company is prepared to address threats to employees.

Executive Protection Considerations

In todays fiscally challenged business environment it may be difficult to justify providing an Executive Protection Program for an organization's key executives. However, in making this important decision one also has to consider what the cost would be to the organization's bottom line and, perhaps more importantly, to its reputation should a key member of the senior leadership team be the target of an act aimed at harming or embarrassing the individual and the organization.

Due Diligence Investigations

If asked, many companies would say that they have "due diligence investigation" processes in place; however, these processes are often designed to review the financial and operational affairs of a particular company and fail to closely inspect the background of the main principals or executives of the company. In addition, many companies do nothing more than cursory checks on individuals they are about to hire. The lack of a robust background investigation can result in wasted time and can cause legal and financial problems. There is an abundance of legal findings across Canada, as well as internationally, that clearly articulate the liability facing companies who do not carry out appropriate due diligence investigations. In order to inspect this issue closer one must first begin with a definition and understanding of what "due diligence" consists of.

Take a Moment to Celebrate Success

Take a moment today to think about the successes you have had and the team that got you there. It is well worth it.

A Solid Foundation for Administrative Investigations

"Is it time for the implementation of standards, including proper training and oversight, as it pertains to the conduct of "administrative investigations"? It could be argued that administrative investigations are purely "administrative" in nature and as such there is no requirement for an enhanced capability. However, it can also just as easily be argued that these types of investigations can have a very negative impact on the lives of those being investigated, including the potential loss of their livelihood. They also bring with them a large degree of "personal and institutional liability" on the part of those individuals conducting the investigations and the" "organizations for which they are employed."

Marine Port Security - Published in FrontLine Magazine

"Since 9/11, marine port security has been the subject of increased scrutiny as it is clear that contraband flows - undetected and uninterrupted - through access and egress points of both Canada and the United States. Numerous reviews initiated by the United States Government Accountability Office (GAO) and the Canadian Standing Senate Committee on National Security and Defence have clearly articulated that ports are a haven for criminal activity and organized crime, as well as targets for potential terrorist activity. Both these reviews demand

an increase in the level of intelligence sharing among partner agencies focused on policing and security of marine port operations."

Setting up an Intelligence Hub - Published in FrontLine Magazine

Intelligence in some form is in use today across a broad spectrum. No longer just the purview of Government entities, business intelligence is a common term and practice among corporations. Today, in the internet age, there is an abundance of readily accessible information about any given topic, organization or person. The immense growth of social networking in recent years has added to a rich information bank that is readily accessible to anyone with an internet connection. The challenge today is to sift through vast quantities of information to uncover and piece together the information you require into an intelligence picture that supports your operations. The value of your own information can increase exponentially when combined with open source research and information from other entities with whom you are willing to share.

Security Policy

"Policy writing: next to cleaning the coffee break area, doing personnel assessments or wrestling a hungry grizzly bear, it is probably one of the least desirable tasks in any organization. Its mere mention can send employees scrambling over desks and seeking cover in the hopes of being spared the mind-numbing drudgery of documenting the company's rules, procedures and practices. There is a good reason for this: writing is hard work – and writing clearly, concisely and meaningfully is even harder still. When it comes to communicating an effective security policy, capturing that policy on paper (or, in today's digital environment, electronically) is only the first – albeit most critical – step. Disseminating the policy and ensuring compliance are close second and third priorities, followed by periodic reviews to ensure the aforementioned policy continues to meet your organization's requirements. "

Travel Security

"Media reports continue to include stories about company executives, oil field workers and regular travelers who have been the victims of kidnappings, armed robberies and murder while visiting foreign countries. Recent events have seen a Canadian woman kidnapped in northern Nigeria and her captors demanding $136,000 for her release. This woman was a financial advisor who was in Nigeria with other Canadians as part of an exchange program and she was kidnapped

as she was entering a house after attending a social event. There are also ongoing reports of oil workers being kidnapped by rebels in South America and Africa; it would appear that these types of incidents are increasing rather becoming a thing of the past. "

Duty of Care

"The dynamic threat environment that persists in today's business climate demand constant vigilance and discipline. Under the Canadian Criminal Code, companies owe a duty of care to their employees. This means businesses must take "reasonable steps" to protect workers, whether they are in Canada or working internationally. If companies do not meet this duty of care, they can be found criminally and financially liable under the Criminal Code. In the most extreme cases, the company can face hefty fines and the executives can be prosecuted and potentially jailed. In addition to the criminal prosecution, individuals can also face personal civil litigation. "