TECHNICAL SURVEILLANCE TODAY

THREAT • RISK • PREVENTION

PART I

MSA
INVESTIGATIONS

9 MURRAY STREET, NEW YORK, NY 10007 | TELEPHONE: 212-480-4050 | MSAINVESTIGATIONS.COM

TECHNICAL SURVEILLANCE TODAY: THREAT – RISK – PREVENTION

PART I

THE THREAT: TECHNICAL SURVEILLANCE

In order to protect corporate privacy and sensitive client information, many organizations have recently put considerable effort into strengthening their defense against the threat of cyber-attacks. However, an often overlooked concern is the threat of covert surveillance devices which may be hidden in plain sight. In addition to protecting their networks, organizations concerned about eavesdropping must remain diligent in securing their offices, boardrooms, executive residences, and other places of business. It is important to keep secret not only what is written, but also what is *said*. As covert listening device technology continually adapts and advances, so do the countermeasures available. The considerable resources and effort put into securing a computer network can be circumvented by one rogue employee dropping a $200 cellular bug disguised as a pen onto a boardroom table. The detection of this type of device would require experts trained in current techniques and using cutting edge technology.

> "IT IS IMPORTANT TO KEEP SECRET NOT ONLY WHAT IS WRITTEN, BUT ALSO WHAT IS *SAID*."

If undetected, the theft of confidential and valuable information can lead to a substantial monetary loss or a competitive disadvantage in the marketplace. The Office of the National Counterintelligence Executive ("NCIX"), using estimates from academic literature, has estimated losses from economic espionage to be in the "tens or even hundreds of billions of dollars annually to the American economy." The FBI's Assistant Director of Counterintelligence has been quoted saying that corporate espionage is a reality and the "threat is so significant, and the harm can be so severe, that the FBI has listed it as the second highest priority, second only to countering the next terrorist attack."

The FBI's primary concern, given the agency's overall responsibility for the internal security of the country, is threats from other countries, especially since those hostile to the U.S. Foreign intelligence services have become more creative and sophisticated in their approach to undermine American businesses. Additionally, as the FBI's economic espionage cases increase; the percentage of investigations attributed to a threat from *within* U.S. corporations is also increasing. Those threats typically come from individuals currently or previously employed with

an entity, who have some motivation, either personal or financial, to try and bring harm to the company. However, the threat also includes entities that specifically target U.S. businesses and exploit weaknesses in communications security to steal confidential and proprietary information.

There is no known accumulation of data on companies that have fallen victim to the theft of trade secrets or business intelligence information, likely because occurrences of this nature would often be humiliating or damaging for an organization. Companies have a fiduciary responsibility to their employees and shareholders to safeguard and protect intellectual property and sensitive corporate information. Publically-traded companies, in most instances, have a legal responsibility to report breaches of corporate information to regulatory agencies including the Securities and Exchange Commission (SEC) and others. However, the disclosure of such confidential and proprietary information can have catastrophic consequences which can lead to the ruination of a company and is therefore not always reported.

WARNING SIGNS

Some indicators or warning signs that an organization has been the subject of espionage can include:

- The company's business strategies are revealed
- Internal communications are made public through the media
- Company trade secrets are exposed
- Pricing and sales strategy is known by competitors
- A bid was recently lost that would normally have been won
- There is an unexplained decrease in new sales
- Negotiations for labor and contracts are more difficult

Some companies or organizations are at higher risk of espionage than others because of their occupation, financial position, or legal situation. An intruder must balance the potential gain from an intrusion against the possibility of discovery and the cost of resources used in the effort. Accordingly, a company is most in danger of an electronic eavesdropping attack when:

- Business expansion or reorganization plans are being discussed
- Key executives leave or are leaving
- New products, pricing, or marketing plans are being developed
- Acquisitions or mergers are being planned

- It is engaged in a sensitive or high-profile industry
- Executives or clients are the subject of media attention
- There are ongoing labor negotiations, labor problems, or union activities
- It is involved in any type of litigation, lawsuit, or other civil action
- It is considering, or already in the process of, laying-off or terminating employees. doing so

NEXT, IN PART II: WHERE and HOW technical surveillance is deployed and COUNTERMEASURES to the threat.

To sign up to receive Part II, click here or the icon below.