The Current State of Industrial Espionage

It is not within the scope of this site to give you a complete history of IE, or its current state. Many finely researched works exist on the subject. We are technical experts, so we will restrict our overview to what's most relevant-to you-right now. Below are *ten things* you MUST know about the current state of Industrial Espionage via electronic surveillance.

1. **Sales of surveillance devices** are growing at an alarming rate. Clearly these devices are not being used for entertainment purposes, or only by the curious. They are being used somewhere, for some reason-usually in companies, for information, and for profit. Also, common household items (Nanny Cams, old phones, intercoms, mp3 players): can be used effectively.

2. With **technological advancements**, these devices-bugs, audio and video, and other electronic devices-are now smaller, faster, cheaper, and more powerful than at any other time in history. They can be easily hidden, used in ingenious ways, incorporated into any of the familiar electronic devices that surround you daily, and transmit long distances lightening fast. What was once the famous "video camera inside a briefcase full of electronics", is now in your phone or sitting atop your computer.
3. They can easily be purchased at a local spy shop, via the Internet, even in your local electronics or hardware store.
4. It does not take a "sophisticated" device to eavesdrop on a large, sophistically guarded organization. Under the right circumstances, a baby monitor can bring down a large corporation. Did you know that baby room monitors were originally constructed as Bugs? When new privacy laws were introduced into the US, after Watergate, manufactures packaged them to disguise their intent (those in the IE field knew). The funny thing is, much to their surprise, the new marketing caught on!
5. It is often not necessary to even enter the targeted office or premise to bug someone. Communication lines run through several areas; some office electronics (intercoms, speakers, etc.) can be compromised by other means.
6. The wrong information in the wrong hands can create havoc in a divorce, the stock market, a competitive bidding situation, even in employee negotiations. Any situation that calls for security or secrecy is automatically, almost by definition, vulnerable to the attempt of information theft, espionage, or sabotage!

7. Most potential victims are completely ignorant of the threat or compromise.
8. The financial, personal, and business consequences of industrial espionage are usually very serious. Security breaches can lead to the most devastating, untimely end to an advantageous situation-failure is just a small bug transmission away.
9. Security threats from "bugging, or electronic surveillances, are often more detrimental than "computer-based" spying or espionage, yet few companies and individuals give them the same attention.
10. Most bugs can't be seen, and require state-of-the- art specialized equipment, and expertise to detect and remove.

Unless an individual or organization becomes "bug conscious" and creates and elevates security policies and procedures to eradicate and prevent this effective means of industrial espionage, bugs-surveillance devices will creep in. Threats can come from within the organization (over-ambitious employees trying to accelerate their careers, disgruntled staff, family/owner power struggles) or from outside (competitors, brokers, professional industrial spies, or opportunists).