



### **MANAGEMENT HAS A LEGAL RESPONSIBILITY:**

Corporate/Industrial Espionage *can* be prevented. Your company's valuable information, just like any other corporate asset, can and must be protected. Remember! Negligence litigation brought by shareholders can hold company executives personally responsible if the information asset is lost or compromised due to inadequate protective measures. The responsibility here is exactly the same as if a fire breaks out, seriously damaging the facility, and it is later discovered that the insurance company rejects the claim because no one paid the fire insurance premium.

Guard services, alarm systems, locks and the like are *not* adequate protection for your company's vital information.

A thorough and professional Technical Surveillance Countermeasures (TSCM) program is the only practical and proven method of protection. And, just like that fire insurance policy premium, the cost can be pennies compared to the magnitude of a loss.

### **THERE IS A GRAND PARADOX HERE:**

No one can accurately determine the full extent of corporate espionage. Equally indeterminable is the magnitude of the actual loss to business, industry and governments brought about by the practice. The reason is quite simple. The successful attempts at eavesdropping are – by way of being successful – never discovered. Only the *failed* attempts are discovered. By extrapolation, only by a guess, can it be inferred how many actual eavesdropping attacks take place. Authoritative sources have stated that the loss to American businesses exceeds hundreds of billions of dollars annually.

Don't let your company become a statistic. Losses due to eavesdropping/ espionage attacks can be mitigated. A thorough and professional Technical Surveillance Countermeasures (TSCM) program can save you *many times* the cost of the service. Inadequate services (the typical "cheap sweep") performed by inexperienced and under equipped persons is invariably money thrown away.