TSCM INSPECTION EXCUSES & MYTHS

by Kevin D. Murray, CPP, CISM, CFE, CDPSE

• Espionage is a Covert Act:
Excuse: "I don't see that we have a problem. No one is bugging our offices and boardroom."
Reality: Yes, you won't see the problem if you never schedule a TSCM inspection.[1] The first rule of espionage is, "Be invisible." This corporate espionage incident[2] is a cautionary tale.

• Fear of Being Labeled Paranoid:
Myth: Peer pressure from upper management.
Reality: Most top management appreciate proactive security thinking from their staff.

• Lack of Awareness:
Excuse: Yes.
Reality: A lack of awareness of the risks associated with electronic eavesdropping, or the need for TSCM security inspections[3] is common. Management may be unaware of TSCM as an available countermeasure.

• Cost:
Myth: TSCM inspections can be expensive. The costs involved[4] in purchasing specialized equipment, or hiring a professional TSCM specialist, can be a deterrent to scheduling TSCM inspections.
Reality: Espionage losses are more expensive, much more. Hiring a TSCM specialist is very cost-effective, if you hire a competent firm.[5] TSCM inspections are cheap insurance. Actually, TSCM inspections are better than insurance; they can prevent losses in the first place.

• Perception of Low Risk:
Excuse: Some businesses may believe that the risk of electronic eavesdropping is low in their industry or specific workplace. They might assume that their organization does not hold valuable or sensitive information that would attract eavesdroppers.
Reality: Being "in business" implies having a competitive advantage, and others do want it.

• Lack of In-House Expertise:
Excuse: Conducting TSCM inspections requires specialized knowledge and equipment.[6] If a business does not have the expertise in-house they may choose not to pursue these inspections.
Reality: Solution… Hire an information security consultant[7] whose speciality is TSCM.

• Fear of Disruption:
Myth: TSCM security inspections can temporarily disrupt normal business operations. The process involves sweeping the premises, potentially causing interruptions or inconveniences to employees or ongoing activities. Some businesses might be reluctant to undergo such disruptions.
Reality: Most inspections are conducted after

---

[1] https://counterespionage.com/what-is-tscm/scheduled-tscm-inspections/

[2] https://counterespionage.com/high-stakes-corporate-espionage/

[3] https://counterespionage.com/what-is-tscm/scheduled-tscm-inspections/

[4] https://counterespionage.com/how-much-does-tscm-bug-sweep-cost/

[5] https://counterespionage.com/competent-tscm-consultant/

[6] https://counterespionage.com/tscm-technology/

[7] https://counterespionage.com/competent-tscm-consultant/

TSCM INSPECTION EXCUSES & MYTHS

by Kevin D. Murray, CPP, CISM, CFE, CDPSE

business hours. When necessary, a TSCM team can assume the same dress and demeanor as employees, develop a plausible reason for being in the area, and will work around employees so as not to disturb them.

• Trust in Existing Security Measures:
Excuse: Businesses may have confidence in their existing security measures, such as physical security, cybersecurity, or access controls. They might believe that these measures are sufficient to protect against eavesdropping and thus forego TSCM security inspections.
Reality: Experience has shown that standard security measures are never sufficient to protect against electronic eavesdropping and other forms of information loss. TSCM inspections always identify unnoticed vulnerabilities and provide recommendations for improvement.

• No Legal or Regulatory Requirements:
Excuse: Depending on the industry or geographical location, there may be no legal or regulatory obligations that mandate TSCM inspections. In the absence of such requirements, businesses may choose not to prioritize these inspections.
Reality: The financial success of a business should be a greater motivator than a legal requirement.

• Perception of Invasion of Privacy:
Myth: TSCM security inspections are invasive or a breach of employee privacy. They might fear that conducting such inspections could harm employee morale or create an atmosphere of distrust.
Reality: Employees appreciate security measures which protect their livelihood and personal privacy. When an employer demonstrates care for information security, employees act more carefully too.

• Limited Resources:
Excuse: Small businesses or those with resource constraints may prioritize other operational needs over TSCM security inspections. They might allocate their limited resources to other critical areas or invest in measures they perceive as more immediate concerns.
Reality: Defense is mandatory for survival. Budget waste and misallocation can usually fund TSCM security inspections without added expense, once corrected.

• Overconfidence:
Excuse: Some businesses might have a sense of overconfidence in their security measures, believing that they are already adequately protected against electronic eavesdropping. This false sense of security can lead to complacency and a disregard for TSCM inspections.
Reality: These businesses are at-risk.

Carefully assess the risks in your workplace. Schedule TSCM security inspections[8], because… corporate espionage is not a myth.

###

Murray Associates is an independent technical information security consulting firm. They provide electronic surveillance detection and counterespionage services to business, government and at-risk individuals.

Headquartered in the New York metropolitan area, a Murray Associates team can assist you quickly, anywhere in the United States, and internationally.

[8] https://counterespionage.com/what-is-tscm/scheduled-tscm-inspections/