TSCM - The Other Covid Deep Clean

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

Deep Clean sanitization of offices and facilities is on the minds of organizations everywhere. Covid-19 prevention is the goal. Once this is completed office employees will begin returning to their desks. Everyone will feel safe, at least health-wise.

The blind spot *not being considered* is the health of the workspace itself. Only the most diligent security directors will think of addressing this issue.

Workplaces—unpopulated for months—are easy targets for electronic surveillance infestations and cyber infections. Corporate espionage and foreign government types know this. The pandemic became their golden opportunity to Deep Plant surveillance devices.

During the work-from-home days executive suites were empty. No one was in the buildings except a few security and maintenance folks. The long lock-down afforded plenty of time to prepare an intrusion and deeply embed multiple intelligence collection devices.

"They couldn't get into our place. We have *really* good security," I hear you say.

Consider these scenarios…

1. The night or weekend guard is probably a low-paid, part-timer; more interested in their smartphone than anything else. Would a good pretext and a work-order get the spy in? Posing as a Covid Cleaning Service might open the door. Who wants to turn them away. Not sure a phony work-order would work at your place? What if they simply offered official government paper ($$$$) instead. It would only be a matter of, "how much?"

2. Night and weekend security guard shifts are notoriously hard to fill. So, the Deep Placement tech simply applies for a security guard's job working nights and weekends at the targeted facility, likely alone and unsupervised.

3. Many workplaces can be covertly entered using a can of compressed air[1] instead of a cardkey. This covert entry technique doesn't trip the alarm. It appears to be a legitimate exit. (Compressed air is just

[1] https://counterespionage.com/lock-trick/

TSCM - The Other Covid Deep Clean

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

one of 10+ common covert entry tricks[2] in the spy's kit.) Once in, others in the building think the intruder must be authorized to be there.

4. Has your organization been using the down time to conduct renovations?[3] Think of all the opportunities that endeavor presents for deeply embedding surveillance devices.
   The book, **The Attack on Axnan Headquarters: An Espionage Operation**,[4] explains in detail how this is done. The plot is an actual account (sanitized) of a real corporate espionage operation conducted during a construction project.
5. The average CCTV system isn't much protection either. Recordings, if available, are rarely reviewed unless there is an alarm or incident. By then, the bug installer is long gone, and you have no idea what they did while they were there.

The reality is, organizations just don't know if employees will be returning to hot-wired offices.

If stolen information using deeply embedded surveillance is handled carefully, the target will never become suspicious. Cautious tradecraft like this will yield valuable information for years to come. Remember, the parasite is not out to kill the host, until the host is no longer useful.

This security cluelessness is what unethical competitors, opportunistic freelancers, and foreign interests are counting on. They are betting their bugged victims will not conduct a Technical Surveillance Countermeasures Deep Clean (TSCM/DC).

What is a Technical Surveillance Countermeasures Deep Clean?

Employees need to feel safe about their operational and personal privacy in addition to feeling safe about their health. Periodic inspections for illegal surveillance devices in the workplace is the primary method used to assure these privacies.

[2] https://spybusters.blogspot.com/2020/10/physical-securitys-15-greatest-hits.html

[3] https://counterespionage.com/construction-project-tscm-considerations/

[4] https://amzn.to/3nmUFRU

TSCM - The Other Covid Deep Clean

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

Elements Common to TSCM Deep Cleans

1. Pre-inspection discussion, evaluation and planning.
2. Physical examination of areas at risk.
3. Technical examination of the areas.
4. An information security survey to identify other vulnerabilities.
5. A post-inspection debriefing.
6. A written report documenting findings, recommendations and due diligence.

Each element is discussed in greater detail in **The TSCM Inspection Process**.[5]

During normal times a TSCM/DC is most often conducted on a quarterly basis, within the *most* sensitive areas. As the pandemic comes to an end, a complete TSCM Deep Clean (within *all* sensitive areas) needs to be conducted before employees return.

TSCM Deep Cleans are often conducted after normal business hours because it…

- doesn't disrupt the flow of business,
- doesn't alert employees (who may be involved in planting devices),
- reveals transgressions of company information security policies,
- allows your counterespionage consultant to quickly identify non-electronic security vulnerabilities, and security hardware which has lost its effectiveness.

There are exceptions to off-hours TSCM Deep Cleans. Board meetings and off-site meetings, for example, are preceded by a TSCM/DC. Once complete, the technical investigator relocates to an area nearby the meeting and begins radio-frequency spectrum monitoring. This precaution detects bug transmissions which may come on-the-air at the last minute, or during the meeting.

Plan Ahead

Organizations will be opening their offices at approximately the same time. Plan ahead. You want to employ the most capable and reliable firm to conduct your TSCM Deep Clean. The most competent teams will be booked first, and you know the rule… 90% are not in the top 10% of their class. This matters. An ineffective inspection buys a false sense of security. And, that's worse than a healthy sense of caution.

Thank you for considering our services. If you have any questions, or would like to schedule our services, just let me know.[6]

Kevin D. Murray CPP, CISM, CFE, CDPSE is a business counterespionage consultant and TSCM specialist with over four decades of experience.

Murray Associates[7] is an independent security consulting firm, providing eavesdropping 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.

[5] https://counterespionage.com/tscm-inspection-process/

[6] https://counterespionage.com/contact-murray-associates-tscm/

[7] https://counterespionage.com/about-murray-associates/electronic-eavesdropping-detection/