Murray Associates | Security Report

IT Data Center TSCM Inspections

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

You Think You Have IT Covered…

☑ Thick concrete walls.
☑ Data, comms, and power redundancy.
☑ Mantrap entry control, CCTV and alarms.
☑ Stratified internal access controls.
☑ Locking server cabinets.
☑ Documented procedures.
☑ And, a SOC to knock your socks off.

But, what about…

□ Electronic surveillance device detection.
□ Wi-Fi security and compliance verification.
□ Employee information policy compliance.
□ Decaying security hardware discovery.
□ Improper sensitive wastepaper disposal.
□ Office equipment technology threats.
□ Emerging information security threats.

These are the Achilles' Heels of IT data centers. The solution… Conduct periodic Technical Surveillance Countermeasures (TSCM) inspections.

Let's look closer at a few of these information security loopholes.

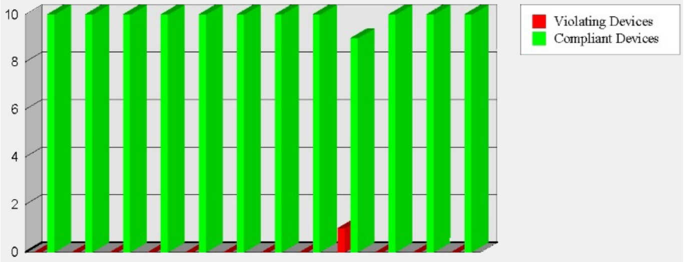
Electronic Surveillance

Old fashioned bugs and wiretaps probably come to mind first. While they remain a threat, under appreciated items like cellular and Wi-Fi malicious USB cables and GSM bugs are favored by tech-savvy attackers. Miniature voice recorders and covert spy cameras are next on the list.

Finding these devices is the primary, but not the only, function of periodic TSCM inspections.

Wi-Fi Security & Compliance

Wi-Fi is used by printers, VoIP phones, security cameras, and all other IoT devices.



Just one loophole…
Hackers are in.
Data is out.
&
"You are out of compliance."

A common scenario… The IT department secures the Wi-Fi system when it is first installed. Then, an executive orders a printer from Amazon on their own. It comes with unsecured Wi-Fi turned on by default. Instant Achilles' Heel. Hackers attack. Once this far in, they gain sensitive data, passwords, and can attempt further pivots into the network.

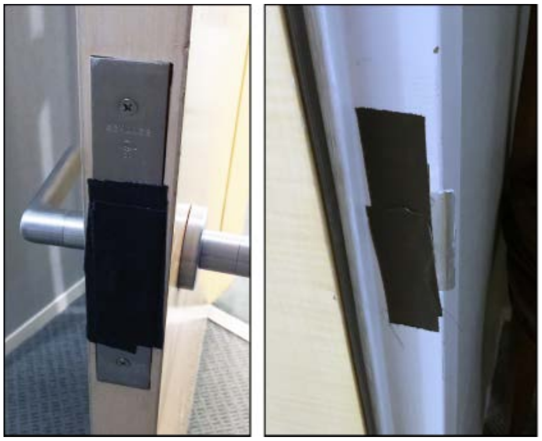
Competent TSCM inspections include Wi-Fi security and compliance audits.

Information Security

You probably have an information security policy. Does it include the proper storage of unattended sensitive paperwork, a clear desk policy, and the shredding of sensitive wastepaper? Are employees abiding by the policy? A TSCM inspection will identify and help you solve these issues.

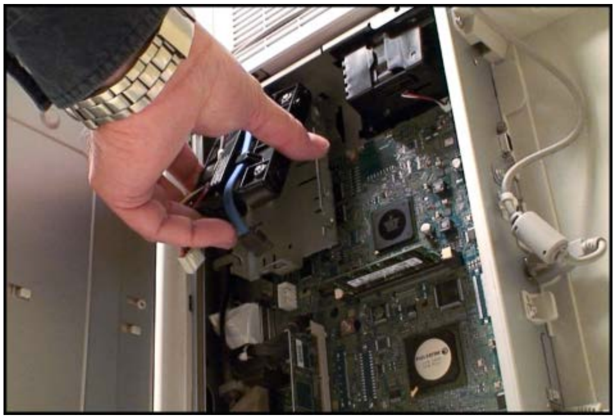
Security Hardware Fails

Security hardware may have been improperly installed, can break, decay in effectiveness, or be crippled on purpose, like this taped door lock. This compromise was invisible when the door was closed. IT data center TSCM inspections uncover security hardware fails like these.



Office Technology Threats

Advanced office equipment can be very helpful. Networked print centers are a good example. Their dark side, however, is that all print jobs are stored into memory and can be remotely extracted, or have their hard drive swapped out.



TSCM inspections will alert you to office security vulnerabilities, and offer solutions.

***

If you have any questions, or would like to schedule a TSCM / information security audit, just let me know.

Kevin

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

Murray Associates[1] 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.

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