TSCM & PENETRATION TESTING

When discussing Technical Surveillance Countermeasures with people who are not very familiar with what is involved, they often ask if (or assume) our work is a part of cyber security or even that we are perform pen-testing services.

January 31st, 2020

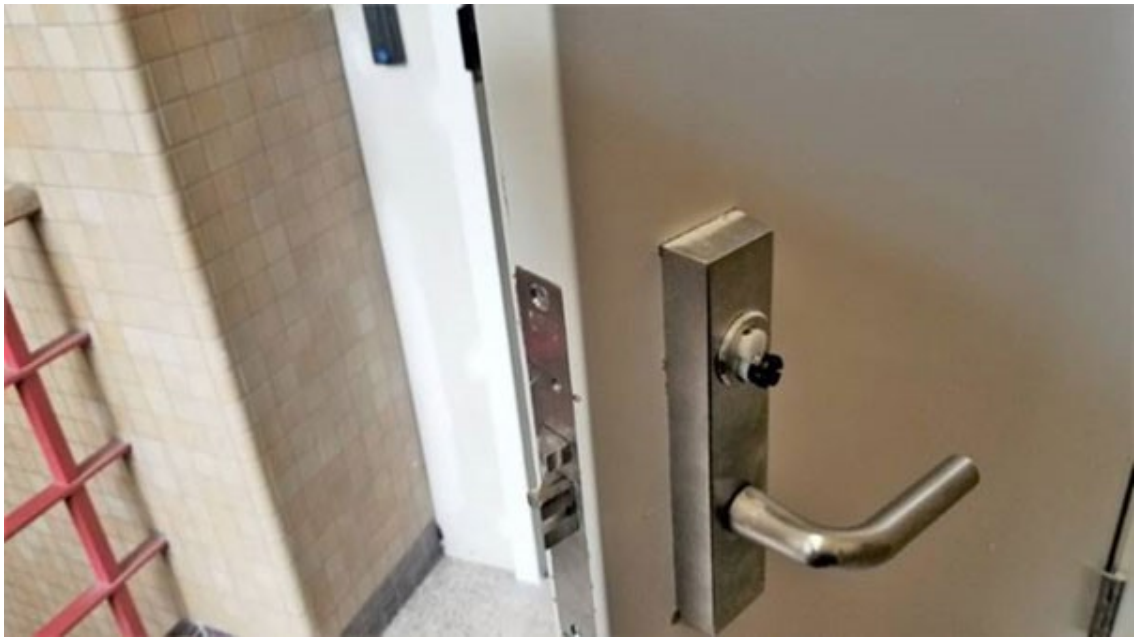
Wifi inspection of one tech facility discovered a rogue access point appropriately labeled "DrkWeb".

In fact, much of TSCM does involve cyber security concerns. We typically, though, are not going to delve deep in to a client's network, but we will often find cyber related vulnerabilities such as inappropriate Wifi signals, breaches in VOIP systems, or physical modifications on data lines that could be used for unauthorized surveillance or eavesdropping. Physical security and access control are also major considerations when conducting a TSCM sweep. If doors are not secure or if access controls can be circumvented prior to any confidential meeting, for instance, then the information discussed in that meeting could easily be compromised. While we may not be actively attempting to penetrate the security of a network or a facility, our tests and observations almost always reveal significant information security and physical security vulnerabilities.

Examples of physical vulnerabilities we found recently include a heating vent passage way that connected from a confidential conference room to a next door office that had been conveniently turned into a coffee break room. While sweeping the room, we heard clear voices coming from the corner. Further inspection found that, yes, the voices were real. There were two employees having a cup of coffee next door. A note to the security director quickly got the coffee pot moved and the air vent stuffed with insulation.

Air ducts and heating vents can allow sound to pass freely between rooms

Another incident involved arriving to sweep a board room and discovering one of the doors had the door strike taped over with gaffer's tape to keep the door from locking. The sweep was being conducted the day before a high level board meeting. The doors to all of the meeting rooms had proximity badge access control, as well as badge access was require just to get to the entire wing of that floor. One might assume that only authorized persons could enter the area. Perhaps an AV technician had temporarily wanted to keep the door open to be able to go back and forth while setting up equipment, and just forgot to remove the tape. But further inspection of the area revealed an even greater problem. There was a fire exit door nearby that opened to a set of emergency stairs, leading down to the street. A quick check of the lock cylinder for the door revealed that it had been damaged. We found that the key way from the outside was clearly in bad shape, so much so that it no longer needed a key. A coin could be used to open the fire door from the stair side, allowing access to the meeting room area.



Damaged fire stair door allowed access to secure area with use of a coin.

The security of this confidential, highly secure, board room had been totally compromised. Access to the room had been open to anyone in the building for who knows how long prior to their board meeting. These types of breaches or lapses in security may easily be overlooked when each falls into a different person's area of responsibility. The maintenance staff responsible for the fire stair door may have no relationship to the person responsible for the meeting room doors. The person setting up the coffee machine may have no awareness of the missing insulation in the heating vent.

A competent TSCM technician will spot the individual problems and should recognize how they link together to create a much greater vulnerability. In TSCM we are not necessarily looking for ways to breach security or penetrate a secure area, but we are finding the ways that confidential information and conversations could be leaked, stolen, and ex-filtrated from an area. After all, all valuable, confidential data has it's beginning as a conversation. Companies serious about information security should have TSCM inspections conducted on a regular basis.

TSCM may be the missing piece to your security.