BUILDINGS SMARTER FACILITY MANAGEMENT

How to Handle Counterespionage

by Kevin D. Murray, CPP, CISM, CFE

You know everything about managing facilities, but a request from management to debug your building can throw even the most seasoned FM for a loop. With the help of an outside professional, you can ensure speech privacy and business security.

A Sweeping Problem

Business espionage is a growing concern, yet it's mistakenly thought of as an IT department problem. The reality is that the information IT protects is vulnerable to theft long before it is put into the computer – what people talk about and with whom provides the most valuable information.

Electronic eavesdropping has also become cheap and easy. Spy gadgets, such as bug transmitters, micro voice recorders, and covert video cameras, were once expensive and hard to come by. All are now available online for under $100. Some even use Wi-Fi, Internet, and cell phone networks as communication conduits.

Because building owners are focused on physical security, the chances are slim that a corporate spy will be detected or caught. A technical information security survey, however, can put an end to electronic eavesdropping and remote surveillance.

These surveys, which are a more advanced form of the old technical surveillance countermeasures, should be conducted by a credentialed security consultant who specializes in electronic eavesdropping detection, information security, and nothing else.

In addition to finding proof of intelligence collection activities, technical information security survey will also allow your organization to:

- Double check and improve the effectiveness of current security measures and practices.
- Document compliance with many privacy law requirements.
- Discover new information loopholes before they can be used by spies.
- Help fulfill the legal requirement for "Business Secret" status in court.
- Enhance personal privacy and security.
- Ensure Wi-Fi security and compliance with associated privacy laws.
- Reduce consequential losses associated with espionage, such as preventing an information leak that might spark a stockholder's lawsuit or an activist from releasing wiretaps that could damage goodwill and sales.

How to Conduct a Survey

A technical information security survey is usually conducted after normal business hours. This avoids business disruptions and is why most people are unfamiliar with the service. Inspecting after hours also provides the specialist with a clear view of other information security vulnerabilities present.

Be aware it is very rarely necessary to sweep the entire building. Create a priority list of the sensitive locations requiring a detailed inspection. The radio-frequency inspection for transmitters, for example, may cover the entire building, but not every square foot requires a detailed physical inspection. Focusing the specialist's attention on the most sensitive areas provides better results and keeps costs low.

Determine the proper frequency for follow-up inspections, such as quarterly or biannual. The consultant can then prepare a written proposal for services. Expect professional service fees to be approximately $2.30 per square foot for a small survey to $1.90 for an extensive survey. Subsequent inspections of the same areas will be about 10-25% less.

In the movies, bugs and wiretaps are quickly located as clever actors seem to know just where to reach under the table. The more technically oriented are equipped with bug finding “ubergadgets” fresh from the lab. But your inspection will proceed a little differently. Information (visual, audio, and data) can be transferred from sensitive areas in a variety of ways, so there isn’t a single test or gadget that will detect every method.

Specialists may use the following the methods during an inspection:

Spectrum Analysis – a search for surveillance devices that transmit information via radio waves.

Thermal Emissions Spectrum Analysis – detection of heat emitted by electronic circuits. Heat signatures can be seen even when devices are hidden within ceiling tiles, walls, or furniture.

Communications Systems Analysis – a group of tests that identify surveillance methods used to extract information from telephones, faxes, computer networks, etc.

Mapped Physical Inspection – areas are systematically segmented for physical inspection. Each area is combed with several objectives in mind: locate hidden surveillance devices; locate evidence of prior installations; note future surveillance vulnerabilities; and report on other security issues.

This is the most important phase of the inspection and relies heavily on security knowledge, experience, and intelligence. For example, a clear thread seen in a drape or carpet may look normal. A good technical investigator, however, will suspect a fiber optic microphone and search further.

Non Linear Junction Detection – areas are re-examined using non-destructive radar. This safe technique reveals semiconductor electronic components (transistors, diodes, etc.), which are the building blocks of electronic surveillance devices. Devices hidden in or built into furniture, ceiling tiles, and other objects can be identified with this technology even if they are not active during the inspection.

Upon completion, you should receive a verbal briefing, followed by a detailed written report within a week. Your written report should include a list of locations inspected, findings, non-electronic information security observations, remediation recommendations and resources, and an explanation of the inspection methodology and instrumentation used. Most survey reports will also include photographs and an annual inspection log.

Your report is proof of your organization's due diligence. It is also powerful in court to show your business secrets have fulfilled the requirements necessary for legal protection.

Kevin D. Murray, CPP, CISM, CFE is a technical information security consultant at Murray Associates.