A Guide to Off-Site Meeting Information Security

by Kevin D. Murray, CPP, CISM, CFE

Off-Site Meeting Information Security

Corporate off-site meetings are prime targets for infiltration and information theft. Resorts and conference centers are the worst.

It is not at all unusual to catch the competition (and unidentified others) hanging around, eavesdropping, crashing meetings and banquets, picking up unsecured papers and engaging meeting participants.

Let's start with a true story about a meeting crasher and paper grabber. It's one of our most memorable case histories…

Off-Site Meeting Case History
The Four Year Old Spy

Our client's Board meeting was held at a luxury resort hotel on Miami Beach. The room was prepped, meeting materials laid out, the admin staff left two minutes earlier and called us to begin a Technical Surveillance Countermeasures (TSCM) inspection.

As we approached, from down a long hallway, we saw a man and a little girl, in bathing suits and robes, enter the room. They looked like average hotel guests.

When we arrived at the meeting room door, they were just exiting. The girl was carrying materials which had been laid out for the meeting. Caught in the act, the man explained his daughter wanted some paper to draw on and he thought there was plenty of extra in the room.

We retrieved the materials, asked his name, and passed it on to our client. The security director checked. The man was indeed a registered guest. His wife, however, just happened to be the marketing manager for their arch rival competitor. And the family just happened to be vacationing at this resort, on this particular date.

Just coincidence?

A Guide to Off-Site Meeting Information Security

by Kevin D. Murray, CPP, CISM, CFE

Outsiders often engage meeting participants. The hotel bar is the spy's best web. This type of encounter is especially dangerous. Second to planting listening devices, it is one of the most successful—and the oldest—espionage trick being used. Just one indiscretion can blackmail a loyal employee into becoming a million dollar problem.

Following a few simple rules, however, can dramatically reduce your vulnerabilities…

Many of the following recommendations may be applied to your on-site Board meetings and conferences, as well.

Begin by educating meeting attendees about corporate espionage. Let them know spying is a real threat; what they should do to prevent it, and what their company is doing to protect them from spying.

A key point to mention is the ultimate goal, and the benefits reaped by all concerned when successful information security is practiced.

In a nutshell…

- Information loss reduces profitability. Reduced profitability reduces salaries and job security.
- Retaining corporate information increases the competitive advantage.
- Thus, increased profitability and job security. It's that simple.

Your Pre-Meeting Security Briefing

Include the following points in your briefing.

a) Off-site meetings are major targets for competitive intelligence gathering.

b) Information collection methods used will likely be unethical or illegal.

c) Eavesdropping detection precautions are being employed for your protection.

d) Security will control meeting room access (24/7).

e) Attendees must wear ID badges.

f) Store proprietary information with Security for safekeeping.

g) Do not take proprietary information away from the immediate meeting area.

h) Do not discuss business outside of the secured areas.

i) Be suspicious of strangers who befriend you. Blackmail and elicitation are common spy-craft tactics.

j) Report all suspicious incidents to Security.

k) Clearly define Proprietary Information for your employees and vendors… "Information which is not general knowledge and is related to the company's products, methods, customers, plans, etc. Also, any information which would cause the loss of profit, or a competitive edge, if it fell into the wrong hands."

In some cases, you may want a signed copy of this briefing to emphasize the point.

Security Department Responsibilities

- Conduct pre-meeting TSCM[1] inspections to detect electronic surveillance attacks, and… *real-time monitoring* during meetings to detect wireless bugging devices placed at the last-minute. Be sure to include the hotel rooms of prominent employees and guest speakers.
  Spy cameras are the main concern here.

- Destroy all meeting related wastepaper. Have at least one crosscut shredder available on-site. Units may be rented from the hotel or local business supply sources, if necessary.

- Enforce a cleared desk policy during non-meeting hours and lunch break. Correspondence, manuals, appointment books, agendas and other important paperwork should be kept secured. At the end of each meeting session, double-check that this rule is being followed. Assign this task to corporate security personnel, or a trusted employee.

- Supervise the hotel staff when they are working in your areas. Cleaning crews and other service personnel should always be accompanied by a person who represents your interests.

- Do not allow unauthorized 'visitors' or unauthorized company employees to roam unescorted within sensitive areas.

- Do not allow the use of analog FM wireless microphones.[2] If you must use wireless microphones use ones which employ either digital encryption or infrared transmission to reduce eavesdropping opportunities.

[1] Technical Surveillance Countermeasures

[2] Brief video showing why… https://counterespionage.com/wireless-microphone/

- Check credentials and work orders. Anyone claiming they have to perform technical work in or around your meeting areas needs to have their identification and claims verified. This includes: communication company employees, IT technicians, repair persons, electricians, et cetera.

- Do not record confidential segments of meetings. Safeguard all other recordings.

- Be wary of using cell phones where you can be overheard by the general public. Some people around you may not be the general public.

- Key control at public facilities may be difficult to achieve. Request it anyway. Ask management if you can provide your own locks; have locks rekeyed; or use proprietary security tape over keyways to make sure secured areas are not entered after-hours. (Murray Associates provides complimentary security seals to secure areas they inspect.)

- Mark proprietary written information CONFIDENTIAL or SECRET on the cover page. These markings will clearly indicate that you do not consider them to be public information, and this legally sets them apart from your routine paperwork. If the material is inadvertently left unsecured, these markings should prompt your employees to pick them up and return them to their proper place. Make sure employees are aware that this is their responsibility.

- Provide employees with USB data blockers. These allow device charging, while blocking spyware when using publicly provided charging ports. They are available on-line, or at a lower cost from Murray Associates.

- Employees who handle confidential information should clearly understand, and acknowledge in writing, that they understand such material is proprietary.

- If fax machines will be used in the off-site administration room check them for security vulnerabilities, especially if hotel provided. Some older fax machines store an exact copy of received transmissions on their carbon film printing rolls (similar to old typewriter ribbons), and the newer ones store transmissions in memory. Alert secretaries to this fact.

- Check printers for security vulnerabilities, especially ones supplied by the off-site venue. Print centers store their print jobs

on internal memory, which may later be retrieved. Some printers may have a Wi-Fi signal broadcasting in an insecure mode.

- Provide secure Wi-Fi Access Points (APs) with Virtual Private Network (VPN) capability for meeting participants. Under no circumstances should they use the public AP's as these transmissions are easily intercepted.

- Safeguard company telephone directories / contact lists, especially electronic ones which can be copied easily. Industrial spies, "headhunters", competitors, and telemarketing people consider this to be one of the most valuable documents they can obtain.

- Do not distribute sensitive documents to meeting participants until absolutely necessary.

- Enforce password security on event apps.

- Ask the venue not to place your meeting information on their public information kiosk.

- Secure communications equipment rooms and remote connection blocks at public meeting locations. They are usually very vulnerable to compromise. Admission to these areas should be granted and logged by one responsible person. If necessary, station a security officer in this area. If anyone shows up, verify that the repair work was actually requested.

- Have a high security filing cabinet available. At least one secure storage cabinet is needed while conducting off-site meetings. Confidential paperwork, laptop computers, and other valuables require a safe storage place.

Note: Locks which come with most cabinets are not pick-resistant. Currently owned cabinets can be converted by replacing the original locks with high security locks.[3]

Technical Tips

- Cell phone usage at the meeting may be easily restricted using the Yondr system.[4]

- Wireless motion detection alarms, or IP video cameras (think wireless, Internet accessible baby monitors), can be useful in securing areas on a temporary basis.

- White or babble noise generators can be used to mask and mitigate sound migration to areas adjacent to your meeting rooms.

---

[3] http://www.kenstan.com/

[4] https://www.overyondr.com/

- Check, check, and double-check. Even when you ban analog FM wireless microphone use at your meetings, you still need your TSCM team to check. Our next case history explains why…

Off-Site Meeting Case History
The Wireless Mike

Our client, an international corporation, was planning to hold their annual sales meeting at a resort hotel and conference center. A year's worth of effort involving new products, marketing strategies and pricing would be discussed that week.

Security was going to be tight.

- Rooms would be swept for electronic eavesdropping devices.
- The AV contractor was told wireless microphones were banned.
- Access to meeting rooms would be controlled.
- Paperwork would be collected after each session.
- Participants would be briefed on industrial espionage awareness.

The client's security manager had left nothing to chance.

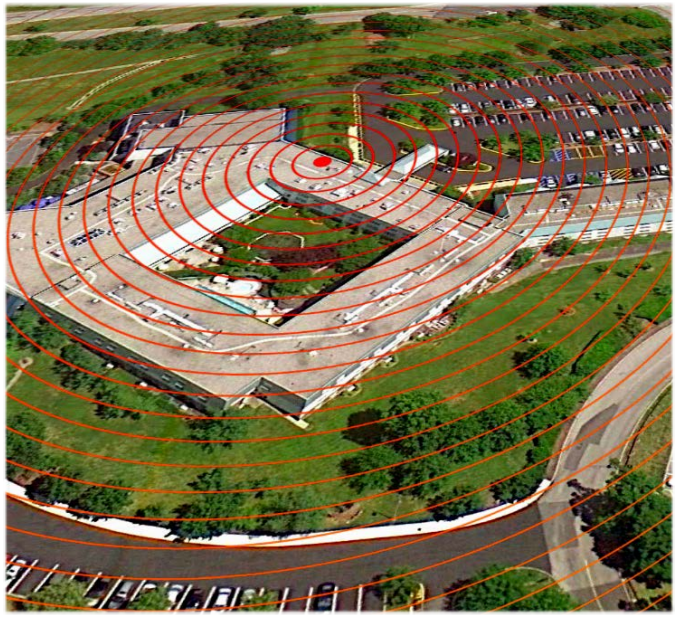
In the early morning hours before the opening of the meeting, the Murray Associates electronic countermeasures team detected a strong radio transmission transmitting sound from the main conference room. The signal permeated half the hotel room wing and out to the parking lot.

Given the strength of the signal, it could be received at a listening post in one of thirty hotel rooms, or by using an automated receiver/recorder hidden in the trunk of any of the dozens of cars parked nearby.

We tracked the signal to a wireless stage microphone. It was found inside a slightly open case, near the podium. The case belonged to the audio-visual contractor.

Mistakenly left on from the day before?

Highly unlikely, the battery was fresh, and the AV contractor was obviously nervous when asked about it.



More Technical Tips

1. Never assume your telecommunications privacy is absolute. It is not. Due to the nature of telecommunications transmission (unsecured terminations, transmission via satellites and in the case of VoIP[5] calls-computer LANs,[6] cellular intercept,[7] etc.) only an average degree of security can be assured without resorting to full encryption techniques. This is especially true of international traffic, much of which is monitored by governments.

2. Analog (old technology) cordless telephones in hotel rooms, wireless headsets and wireless presenter microphones may be encountered occasionally. They are not secure. Interception is especially easy at hotels and convention centers. (see demo video)[8] Their transmissions are easily targeted, and nearby hotel rooms are ideal covert listening-posts. Make sure all equipment has been upgraded to digital transmission for increased (but not absolute) security. Most digital items are also encrypted. (Call us for assistance if you need help making a determination.)

3. Protect telephone conversations from eavesdroppers. Arrange to call in on a number which is not answered with a company name or other identifying information. Be discreet. Use first names; code words to identify special projects; and speak in general terms. Use encryption to protect sensitive communications (Wi-Fi, conference calls, etc.) Meeting planners should consult with the IT department on this. Try to bypass venue-provided systems.

Occasionally we run into the odd-ball espionage tactic. We leave you with our last off-site meeting case history…

Off-Site Meeting Case History
The Bugged Elevator

While inspecting the hotel telephone wiring for wiretaps and audio leakage a live pair of wires was discovered. The emergency phone in the elevator was transmitting audio continuously.

[5] https://en.wikipedia.org/wiki/Voice_over_IP

[6] https://en.wikipedia.org/wiki/Local_area_network

[7] https://en.wikipedia.org/wiki/IMSI-catcher

[8] https://counterespionage.com/wireless-microphone/

A Guide to Off-Site Meeting Information Security

by Kevin D. Murray, CPP, CISM, CFE

At first we thought that this might be normal for elevator emergency phones. We tested the other elevators. None of the others transmitted audio until the phone button was depressed. This was indeed an anomaly.

This particular elevator was the one at the end of the conference center floor; the one that serviced a hotel conference room called "The Boardroom."

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

Murray Associates 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.

https://counterespionage.com/