Your confidential meetings are not private

Eavesdropping, unauthorized recording, and digital espionage risks in Boards, Committees, and Government Agencies

RISCCO | January 30th 2026 | 8 minutes | 1246 words

Contents

1. Executive Summary

The most confidential information in your meetings is often spoken, not written.

Risk

Modern devices have turned every meeting room into a potential surveillance platform. Smartphones, wearables, smart glasses, and laptops can capture and transmit confidential conversations intentionally or not.

Impact

- **Strategic Advantage Lost:** Leaks regarding pending decisions or negotiations destroy months of preparation and eliminate your competitive edge before execution.
- **Heightened Legal Exposure**: Recordings create permanent records of exploratory discussions. Taken out of context, these can be weaponized as evidence of misconduct in litigation or audits.
- **Collapse of Trust:** Leaks stifle candor. When directors and advisors fear surveillance, open deliberation ceases and decision quality deteriorates immediately

Scope Clarification

This article addresses risks from everyday devices present in meetings, smartphones, wearables, laptops, and room infrastructure that can capture or transmit conversations intentionally or unintentionally.

This article ***does not address state-sponsored spyware*** (such as Pegasus or similar software) that exploits device vulnerabilities to provide remote access to governments or intelligence agencies. Those threats require a different control framework, including device hardening, endpoint detection, and forensic monitoring, which fall outside the scope of meeting-room safeguards.

The controls discussed here focus on the most frequent and practical sources of conversational exposure in real-world meeting settings.

2. What is the problem?

Real risks aren't hypothetical

Council resigns from Los Angeles City Council Seat Amid Furor Over Leaked Audio Recording (*)

Political crisis when Thailand PM faces the risk of losing her seat after the leak of a shocking audio recording with Cambodian Senate President (**)

Famous Company Campbell's leaked audio turned a pantry staple into a Public Relations crisis (***)

Record confidential conversations without authorization

Private meeting conversations were historically protected by physical boundaries a closed door, limited attendees, and paper documents. Today, the same room includes multiple laptops, smartphones, smartwatches, wireless earbuds, smart TVs, and sometimes even voice assistants. Every additional device increases the potential pathways for audio capture and data leakage.

Meeting exposure typically occurs through intentional recording, unintentional device sync, wireless exploitation, or compromised devices.

In our experience, smartphones are the preferred method used to record confidential conversations without authorization.

* https://deadline.com/2022/10/nury-martinez-resigns-from-los-angeles-city-council-seat-1235143013/

** https://moderndiplomacy.eu/2025/06/27/why-might-thai-prime-minister-lose-his-seat-after-leaked-recording-with-hun-sen/

*** https://fortune.com/article/campbell-leaked-audio-pr-crisis-comms-soup-meat/

3. Recording confidential meeting conversations (Risks)

The following risks represent the most common and observed vectors in real meetings.

Risk Explanation	Probability of occurrence
1. **Live audio exfiltration via a "normal" call or app**. A phone can be placed on silent mode and remain in an active call, or a conferencing app can be left running in the background. If the microphone is active, the room becomes a live feed. In some cases, the caller is simply listening; in others, the audio is recorded and transcribed.	High
2. **Offline recording and delayed leakage.** Even without WIFI connectivity, a device can record meeting conversations. The recording can be uploaded later when the device reconnects to Internet.	High
3. **Wireless accessory pathways (Bluetooth earbuds, smartwatches).** A phone outside the room can remain paired with a watch or earbuds inside. These accessories maintain radio signal links and may record independently.	High
4. **Laptop/tablet with microphone on**. A laptop inside the room can record confidential conversation and share it later.	High
5. **Meeting room infrastructure and devices with poor controls.** USB sticks, unknown HDMI dongles, Smart TVs, conference bars, room microphones, and always-on voice assistants can record meeting conversation.	Medium

RISCCO

4. Controls to Protect Confidential Conversations

Consistency matters more than perfection. Keep always in mind, a simple, repeatable process beats a complex policy that no one follows.

The controls of the next page are written to be practical.

They assume directors will keep phones powered on, and that laptops/tablets are required for materials and decision support.

The controls focus on reducing both capture risk (recording) and exfiltration risk (transmission), while keeping the meeting usable.

Examples of physical controls include high-quality Faraday bags and acoustic phone enclosures/lockboxes.

4. Controls to Protect Confidential Conversations

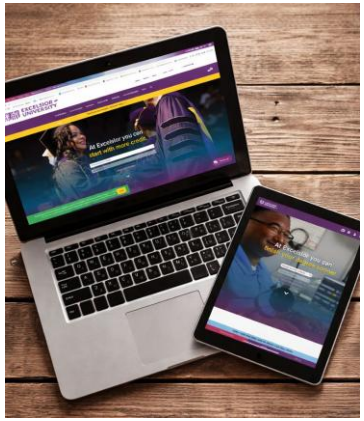
Phones and wearables

a. Use a high-quality Faraday bag for phones, watches and earbuds (devices)

b. Store all bagged devices in an acoustic enclosure/lockbox during confidential conversations.

c. Provide a single emergency hotline phone outside the room.

The bag reduces radio transmission, the enclosure reduces usable audio capture and the hotline keeps usability.



Laptops and tablets

a. Webcam covers mandatory.

b. Wi-Fi and Bluetooth off unless explicitly approved.

c. Prohibit personal hotspots; use a controlled network if internet is needed.

d. No external storage; only host-provided adapters/dongles.

e. Use a dedicated device for presentation.

Once phones and wearables are controlled, laptops become the primary leak surface. Controls must focus on radios, mic/cam, and peripherals.

Meeting room equipment

a. Remove or disable smart assistants; avoid always-on microphones.

b. Use a known, managed display and conference bar; keep firmware updated.

c. Position seating and screens to reduce shoulder surfing.

A secure meeting is not only about the attendees; the room infrastructure can record and transmit confidential conversations.

People and Process

a. Use clear meeting tiers: standard, sensitive, and high-impact.

b. Entry checklist at the door (2 minutes): bag phones, cover cameras, radios off.

c. Assign a gatekeeper and a chair-approved exception process.

d. Document the protocol and train it like a fire drill.

The question is no longer whether confidential conversations can be recorded without authorization; it is whether government institutions and private organizations have the controls to prevent or detect it when it occurs.

At RISCCO, we help boards and government institutions translate these controls into practical, repeatable safeguards that protect confidential conversations while preserving effective decision-making.

Bibliography

Images

1. https://openai.com/

Sources

1. https://marenius.com/noisebox/
2. https://mosequipment.com/collections/tablet-and-laptop-faraday-bags
3. https://www.sentinelone.com/cybersecurity-101/threat-intelligence/cyber-espionage/
4. https://deadline.com/2022/10/nury-martinez-resigns-from-los-angeles-city-council-seat-1235143013/
5. https://moderndiplomacy.eu/2025/06/27/why-might-thai-prime-minister-lose-his-seat-after-leaked-recording-with-hun-sen
6. https://fortune.com/article/campbell-leaked-audio-pr-crisis-comms-soup-meat/

/

RISCCO

CONTACTS

Panama, Central America and The Caribbean

Antonio Ayala I.
CEO
aayala@riscco.com

Rubén Fernández
Consulting Manager
rfernandez@riscco.com

Marinelda Morales
Commercial Manager
mmorales@riscco.com

Dominican Republic and Puerto Rico

Eury Valdez
Sales Executive
efvaldez@riscco.com

El Salvador, Guatemala, Honduras, Costa Rica and Nicaragua

Gari Rojas
Sales Executive
grojas@riscco.com

About RISCCO

RISCCO is an independent international consulting firm committed to transforming how organizations manage risk and adopt Artificial Intelligence. We combine a rigorous approach to GRC (Governance, Risk & Compliance) with advanced data analytics and Artificial Intelligence to help our clients anticipate risks, strengthen governance, and solve complex challenges. Headquartered in Panama with presence in six countries, in 2026 we celebrate 17 years serving more than 200 leading organizations across Central America and The Caribbean.

International rigor. Agile execution. Measurable impact.
We think like strategists. We execute like specialists.

riscco.com