When Executives Travel, Digital Risk Travels With Them

Compromised devices, unauthorized eavesdropping, and physical exposure outside the organization's trusted digital environment.

RISCCO | June 5 2026 | 8 minutes | 1881 words

Contents

1. The problem and risks

Every time an executive travels, sensitive organizational information travels with them.

Outside the office, the controls stop.

The moment the executive leaves the office and is at the airport, taxi, hotel, or restaurant, most of the security controls that protect the rest of the organization cease to apply to him or her.

Routine, not theoretical.

According to Uber's 2026 Lost & Found Index, phones, wallets, passports, and laptops remain among the most commonly forgotten items — a reminder that executive travel risk is routine, not exceptional.

One device. The whole organization.

A single phone or laptop can carry a company's — or a government institution's — most sensitive data, credentials, and decision-making power. The attacker does not need to reach the office — only the executive, once, anywhere.

The most dangerous network is often the one that looks the most convenient.

1. The problem and risks

Risks	Airport Lounges	Taxi or Ride-share or Airplanes	Restaurant Cafes	Hotel Room or Lobby
Device theft or loss in transit. Devices get lost or stolen. A single lost device containing login credentials, offline email, or unencrypted files can become a security breach.	✓	✓	✓	✓
Compromised public Wi-Fi and untrusted networks. Hackers can create fraudulent Wi-Fi hotspots that impersonate legitimate ones. An executive who connects to one of these hotspots could unknowingly expose login credentials and sensitive organizational and personnel information.	✓	✓	✓	✓
Public USB charging station compromise. A fraudulent charging port, cable, or adapter can expose a device to data theft or malware while the executive is charging a phone, notebook, or tablet in a public place.	✓	✓	✓	✓
Unattended device tampering in hotel rooms. Hotel rooms are routinely accessed by authorized personnel. A device left unattended may be exposed to physical tampering, unauthorized access, or firmware manipulation.				✓
Phone or device forgotten in a taxi or ride-share. A forgotten device may contain company or personal information and allow direct access to sensitive files or systems.		✓		

Note: *"Devices" includes laptops, phones, tablets, earphones,smartwatches, and smart glasses.*

RISCCO

What to do if the device is already gone?

2. Steps to follow if I lose the device

Speed beats perfection. *The first 15 minutes determine whether this becomes a recoverable incident or a severe breach.*

First 15 minutes

1. **Trigger remote wipe.** Call your organization's IT or security staff for guidance on the procedure. If that's not possible, do it yourself. Log in to your account at https://www.icloud.com/ (iPhone) with your credentials or consult your phone's manufacturer documentation if you have an Android device.
2. **Reset primary credentials from a clean device.** Email, SSO, VPN, password manager, financial portals.
3. **Start using the backup phone.** The backup phone (mentioned on page 8) should be used to approve logins or MFA authentication. If you don't have a backup phone, call your IT or security personnel for guidance on an emergency MFA reset. The absence of a backup phone will slow down the entire process of getting back online.
4. **File a police report.** The taxi, airline, or hotel operator will always request the report number for insurance purposes, to block your phone number, and/or for any other emergency procedures.

Lost, stolen, or tampered, respond differently

LOST *(taxi, restaurant, lounge)*

Recovery is still possible. Monitor the phone's location signal (Find My – Iphone or Find My Device - Android) and treat the device as compromised and potentially recoverable until proven otherwise.

STOLEN

Assume compromise immediately. Perform remote wipe, reset credentials, file a police report, and alert company or friends on any in-flight sensitive transactions.

TAMPERED OR OUT OF SIGHT *(customs inspection, immigration, or to access an office)*

If you have any doubts about the device's tampering, do not connect it to the corporate network until IT or security personnel have reviewed it. Use your backup phone instead.

Tip: The recovery wallet card. *Carry a printed wallet-sized card with: IT's direct phone number, the Security Officer's mobile number, your assistant's number, your master password manager credentials (if you have one), and the recovery codes for the 2 or 3 most critical accounts that aren't already protected by your backup phone. Use account pseudonyms (not your real name). Review and update the card every six months. The first instinct after a loss is to restore connectivity at any cost. Without a recovery card, this is very complicated and frustrating.*

RISCCO

3. Recovery architecture and continuity

A “backup” phone does more than just keep you connected. It allows you to keep working, but only if the phone keeps you ready.

The backup phone in the hotel safe should be ready, not left empty.

A backup phone is useful only if it is kept prepared: synchronized where possible, loaded with critical applications, periodically tested, and supported by documented recovery methods. Contacts, calendar, and email can usually remain synchronized; apps such as WhatsApp, Signal, mobile banking, and MFA tools must be configured or validated in advance according to each platform’s restrictions

When the primary phone is lost, the backup phone isn't an empty device to be set up; it's the phone that allows you to quickly get back online and working.

- If only the primary phone is lost, with the backup phone, voice, MFA, banking, WhatsApp, and email are restored in fifteen minutes. The trip goes on.
- If it's the laptop that's lost, the backup phone is the mobile office. Email, calendar, documents, video calls, messaging—everything from the device.
- If you lose both your primary phone and laptop, your backup phone is your lifeline. It makes calls, runs important applications, and keeps you connected to the office and your family.

The backup phone and its true cost: Two phones. Two lines. Two monthly bills. The objection is predictable. But the cost of a backup phone has never exceeded the cost of being cut off in a foreign hotel room, without IT support, without MFA, without messaging, without a way to call home, at the exact moment the executive needs all of that. A backup phone isn't an expense. It's the cheapest insurance an executive will ever buy. For an executive whose decisions move transactions, board votes, and more, the cost is a rounding error compared to a single hour of being unreachable.

4. Reducing the odds

Three tiers. Pick what your organization can actually sustain.

TIER 1
Non-negotiable

Every trip. Every executive.

Device hardening

- Full-disk encryption verified before departure
- Webcam covers and privacy filters on every device

Recovery readiness

- Spare phone enrolled, synchronized and tested.
- Recovery codes printed and stored separately (recovery wallet card).

Network discipline

- No public Wi-Fi for sensitive work unless using a VPN.
- Wi-Fi and Bluetooth off when not in use.
- No public USB charging. Use personal charger.

Physical custody

Never leave devices unattended. Use the room safe for your backup phone. Never leave your laptop on if you can't monitor it.

TIER 2
Sensitive trips

When the trip involves information that the organization cannot afford to lose or that unauthorized third parties cannot access.

- Regular travel security awareness talks or pamphlets for executives.
- If possible, a dedicated travel laptop loaded only with essential travel data and applications.
- With the assistance of IT and security staff, delete cached login credentials and offline email files before the trip.
- Enable automatic locking (30–60 seconds) on the phone and 5 minutes for the laptop.
- Verify with IT staff that remote wipe settings are enabled before the trip.

TIER 3
High-risk destinations

Borders with inspection authority, hostile-intelligence environments, persistent surveillance.

- Travel with a laptop that has a reinstalled disk image, without historical data or organizational branding.
- Use tamper-evident seals on each device; inspect carefully before reusing the device.
- If the device was serviced or inspected by a third party, upon its return, have IT or security personnel review it before connecting it to the organization's network.
- Treat any device that you lose sight of as compromised.

Each tier includes the one before it. *Tier 3 assumes Tier 2; Tier 2 assumes Tier 1.*

RISCCO

5. How can RISCCO help?

Two articles. One perimeter.

Helping you to:

1) Build an executive travel protocol
2) Create a risk and control matrix
3) Deliver executive awareness orientation sessions.

Sharing Executive Articles to Mitigate Risk:

INSIDE THE BUILDING

Your Confidential Meetings Are Not Private

Eavesdropping, unauthorized recording, and digital espionage in boards, committees, and government agencies. *Access here.*

RISCCO — January 2026

OUTSIDE THE BUILDING

When Executives Travel, Digital Risk Travels With Them

Device compromise and physical exposure outside the organization's trusted environment.

RISCCO — June 2026

Different threats, same goal: protect the conversation, the decision, and the data — wherever the executive is.
Most firms write articles. RISCCO writes a doctrine, one article at a time.

A 30-minute conversation is the next step.

Antonio Ayala I., CEO — **aayala@riscco.com**

RISCCO

Bibliography

Images

1. https://openai.com/

Sources

1. https://www.uber.com/nz/en/newsroom/lost-found-index-2025/
2. Kaspersky — DarkHotel APT campaign: https://www.kaspersky.com/about/press-releases/darkhotel-aptattacks-high-profile-executives-through-hotel-wi-fi
3. FCC — Cybersecurity Tips for International Travelers: https://www.fcc.gov/consumers/guides/cybersecurity-tips-international-travelers
4. FBI — Public advisory on juice jacking: https://www.fbi.gov/contact-us/field-offices/denver/news/tech-tuesday-avoiding-juice-jacking
5. CISA — Cybersecurity While Traveling: https://www.cisa.gov/news-events/news/cybersecurity-while-traveling
6. NIST — Guidance on telework and travel security https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/telework-and-travel

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

Jeniffer Escoto
Sales Executive
jescoto@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