— BRIEFING / 011 · JULY 2026

THE EXIT INTERVIEW YOU NEVER GAVE.

Offboarding retires the badge, the laptop, and the credentials. It does not retire what the person knows about the principal: the travel rhythm, the family names, the wealth events, the security posture and its moods. Corporate offboarding was designed to protect the company's systems and secrets. Nobody designed the part that protects the principal.

EXECUTIVE RISK SERVICES

Prepared for worst-case scenarios. So you don’t have to.

info@executiveriskservices.com · referral or invite only

— 01 / THE KNOWLEDGE

WHAT A DEPARTING EMPLOYEE ACTUALLY HOLDS

Think about what proximity to a principal teaches over two or three years, with no wrongdoing anywhere. An executive assistant holds the calendar's deep structure: where the principal really is when the calendar says otherwise, which hotel, which restaurant, which gym at which hour. A finance employee has seen the liquidity events, the entities, and roughly what the principal is worth. An IT administrator knows which devices the family uses and how the home network is put together. A driver or office security staffer knows the routes, the residence, and what the protective posture looks like on a normal Tuesday versus a heightened one.

All of it walks out the door at departure, none of it can be deleted, and offboarding as practiced touches none of it. The exposure is not that departed employees become attackers; the overwhelming majority never would. It is that this knowledge now lives outside any duty, system, or relationship the principal controls, subject to the departed employee's future circumstances, grievances, social circle, and susceptibility to elicitation by someone who is hostile.

— 02 / THE GAP

WHY THE STANDARD PROCESS MISSES IT

Corporate offboarding answers the company's questions: return the assets, revoke the access, remind about the NDA. Its threat model is data leaving and IP walking to a competitor. The principal-shaped knowledge, routines, family, wealth, posture, is invisible to that process for a structural reason: it was never classified as anything. No system tags "knows which door the children use." The NDA arguably covers some of it and practically deters little, and the security team usually learns of a sensitive departure after it has happened, if at all.

Departures on bad terms sharpen the exposure, and terminations in roles with principal proximity sharpen it most: the moment the knowledge becomes uncontrolled is also the moment goodwill is at its minimum.

— 03 / THE PRACTICES

RETIRING WHAT CAN BE RETIRED

Knowledge cannot be revoked, but its value decays if the environment changes and its risk drops if departures are handled deliberately. Four practices do most of the work. Maintain a short list of principal-proximate roles, assistant, driver, household-facing IT, close finance, security staff, and treat any departure from that list as a protective event, not just an HR event, with the security function notified before the exit where possible. Rotate what can be rotated on those departures, as hygiene rather than accusation: codes, patterns that were known, standing arrangements the person managed. Close well: how a proximate employee is treated on the way out is itself a security control, since grievance is the most common bridge between knowledge and harm. And for the small set of highest-proximity exits, a respectful protective conversation, what remains confidential, whom to call if anyone ever probes them about the principal, converts a walking exposure into an outer sensor. Former staff who were treated well and briefed simply do report approaches.

ERS provides executive protection, insider-risk advisory, and custody-governance review for principals in digital assets, finance, and technology. Engagements begin with a conversation: info@executiveriskservices.com.