— BRIEFING / 009 · JULY 2026

THE HOUSEHOLD IS THE SUPPLY CHAIN.

Corporations learned this lesson expensively: the breach rarely comes through the front door of the network, it comes through a vendor with legitimate credentials. Households learn it the same way. The residence with cameras, sensors, and a hardened perimeter still hands keys, codes, schedules, and trust to a rotating population of staff, drivers, contractors, and their subcontractors. That population is a supply chain, and almost nobody manages it like one.

EXECUTIVE RISK SERVICES

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

info@executiveriskservices.com · referral or invite only

— 01 / THE SEAM

TRUSTED ACCESS IS THE SEAM

Residential security design concentrates on the uninvited: perimeter, detection, response. But the people most capable of enabling an incident are the invited. A housekeeper knows the family's rhythm better than any surveillant could learn it. A driver holds the schedule, the routes, and the school run. A contractor's crew has seen the interior layout, the safe room, and the camera positions. None of this requires anyone to be malicious. Information that concentrated will leak through carelessness, through social pressure, through a bad hire three layers down at a vendor the family never met.

The pattern in residential incidents across sectors is consistent: some element of inside knowledge, orientation, timing, or access, shortened the attacker's work. The question a protective program has to answer is not whether the household staff is trustworthy. Most are. It is whether the household would notice when one person, once, is not.

— 02 / THE FAILURES

WHERE HOUSEHOLD PROGRAMS ACTUALLY FAIL

Three failures repeat. Vetting happens once, at hiring, and never again, though circumstances change: debts accumulate, relationships end, pressures arrive years into good service. Access is granted by convenience and never retired: the code shared for one delivery still works two years later, the departed gardener's key was never collected, the alarm code is the same one the previous nanny knew. And the vendor tier is invisible: the family vetted the firm, not the person the firm sends, and not the person that person brings.

None of these are exotic problems. They are the same identity-and-access failures every corporation manages, transplanted to a home where nobody holds the administrator role.

— 03 / THE POSTURE

MANAGING THE CHAIN WITHOUT POISONING THE HOME

A household is not an office, and treating staff as suspects destroys the thing worth protecting. The workable posture is structural, not accusatory. Tier the access: who can be where, with what, at which hours, and let the tiers, not personalities, carry the rules. Vet at the person level, not the vendor level, and re-screen on a cycle rather than once at hiring. Retire access on every departure, the same day, as routine hygiene rather than as suspicion: codes rotated, keys collected, credentials closed. Put one named person, family office, estate manager, or advisor, in the administrator role, because access nobody owns is access nobody retires. And brief the staff themselves as part of the protective perimeter: the housekeeper who knows what an elicitation question sounds like is a sensor, not a liability.

Done this way, the program reads to staff as professionalism, the same structure a serious employer runs anywhere, and long-serving staff tend to prefer it: clear rules protect them, too, when something goes missing or wrong.

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.