— BRIEFING / 006 · JULY 2026

YOUR FAMILY IS THE PERIMETER.

The principal has a clean footprint, a hardened residence, and a travel protocol. The spouse's fitness app publishes the same running loop every Tuesday. The teenager's account geotags the house. Attackers do not defeat a perimeter when they can route around it, and in most families, the perimeter only covers one person.

EXECUTIVE RISK SERVICES

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

info@executiveriskservices.com · referral or invite only

— 01 / THE MATH

THE EXPOSURE MATH

Protective programs are usually purchased for the principal because the principal holds the assets, the signing authority, and the public profile. The targeting logic runs the other way. Coercion does not require access to the person with the keys. It requires access to anyone the key-holder cannot accept harm to. That set includes a spouse, children, and often parents, and each of them carries their own footprint, routines, and habits, almost always with none of the principal's discipline and none of the principal's protection.

The result is a perimeter with one hardened gate and open fence line everywhere else. In the incident patterns this series has covered, the residential and family-adjacent approach is not the exception. It is the emerging norm, precisely because it is the path of least resistance.

— 02 / THE LEAKS

WHERE THE HOUSEHOLD LEAKS

The leakage is rarely exotic. A fitness app that publishes a route and a start time. A geotagged photo taken from a kitchen window. A school named in a tagged post. A domestic routine visible to anyone who watches a street for two mornings, or scrolls a feed for ten minutes. Property records, gift-registry entries, event photos, and the social graphs of teenagers knit the rest together.

Individually, each item is trivial. The protective problem is aggregation: the household's combined public record frequently establishes the residence, the routine, and the soft hours with more precision than any single member realizes they have disclosed. And unlike the principal's footprint, nobody owns the problem. The security program stops at the principal. The family assumes someone else has thought about it.

— 03 / THE RESPONSE

EXTENDING THE PERIMETER WITHOUT MILITARIZING THE FAMILY

The objection we hear most is cultural, not financial: nobody wants their household to live like a protection detail. They do not have to. The realistic goal is a family whose public footprint is boring and whose members recognize an approach early, not a family under guard.

Three moves cover most of the distance. First, a household footprint review, done with the family rather than to it: what does the combined public record establish, and which defaults, geotags, public accounts, published routines, can change without changing anyone's life. Second, baseline awareness for the household: what pre-incident behavior looks like, what a surveillance question sounds like, and a simple, rehearsed way to raise a concern without embarrassment. Third, one agreed protocol for the two moments that matter: something feels wrong, and someone is unreachable. Families that have agreed in advance what those two situations trigger remove most of the improvisation that attackers rely on.

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.

This briefing describes an exposure pattern in the aggregate. It references no specific family or incident, and it discusses children only in the abstract, as members of a household footprint. We publish the pattern and the protective takeaway. We omit operational detail, victim identification, and anything that helps an attacker.