— WHITE PAPER · JULY 2026

THE TARGET HAS MOVED.

Physical coercion, digital asset wealth, and the new protective standard for principals, families, and firms.

EXECUTIVE RISK SERVICES

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

info@executiveriskservices.com · referral or invite only

— 01 / SUMMARY

EXECUTIVE SUMMARY

In 2025, physical violence became a structural feature of digital asset risk. Verified coercive attacks against cryptocurrency holders rose 75 percent year over year, kidnappings rose 66 percent, and Europe overtook North America as the most affected region, with France recording more incidents than any other country. Both major tracking firms state plainly that the confirmed numbers understate reality: many cases are resolved privately and never reported.

The pattern is not random street crime. It is targeted, researched, and increasingly organized. Attackers select victims whose wealth is discoverable, whose movements are predictable, and whose assets can be transferred irreversibly in minutes under duress. The household, not the exchange, is now the soft point: spouses, children, and parents are within scope because they are leverage.

This paper explains why digital assets break the assumptions underlying traditional executive protection and kidnap response, how exposure accumulates around a principal, and what a credible protective architecture looks like. Its central argument is simple: for anyone holding or controlling significant digital assets, **custody design is now a personal safety control**, and personal security is now a custody control. Firms and families that continue to treat these as separate problems are defended against the previous decade's threat, not this one's.

— 02 / THE DATA

2025 WAS THE INFLECTION POINT

The numbers no longer describe an edge case. Blockchain security firm CertiK verified 72 physical coercion incidents against crypto holders worldwide in 2025, up from 41 the year before. Kidnapping was the most common method. Physical assaults rose 250 percent. Confirmed losses exceeded 40 million dollars, a 44 percent increase, a figure the firm itself describes as significantly understated due to under-reporting, silent settlements, and untraceable payments.

+75% VERIFIED PHYSICAL ATTACKS, 2025 VS 2024 (CERTIK)

+66% KIDNAPPING INCIDENTS YEAR OVER YEAR

>40% OF GLOBAL INCIDENTS OCCURRED IN EUROPE; FRANCE LED ALL COUNTRIES

~2× CHAINALYSIS: 2025 TRACKED TOWARD DOUBLE THE PRIOR RECORD YEAR

Chainalysis reached the same conclusion from independent data, and added a finding that matters for planning: the frequency of physical attacks correlates with the forward price expectation of bitcoin. Rising asset values do not merely enrich holders. They recruit attackers. Periods of market strength should be treated as periods of elevated physical threat.

Two further shifts deserve attention. First, targeting has moved down-market: victims now include individuals with moderate holdings who are simply known to own crypto, not only funds and founders. Second, the attacks are increasingly the work of organized, transnational crews using open-source research to select and locate targets, rather than opportunists. Publicly reported cases across France, Austria, the UAE, and the United States in 2025 involved planning, surveillance, and coordination across borders. Several ended in the death of the victim.

— 03 / THE STRUCTURAL PROBLEM

WHY DIGITAL ASSETS BREAK TRADITIONAL PROTECTION

Executive protection and kidnap-for-ransom response matured around the mechanics of traditional finance. Those mechanics quietly did protective work. Moving large sums required banks, institutions, business hours, and time. Transfers could be delayed, flagged, frozen, or recalled. That friction created negotiating room, gave responders time to operate, and made the victim more valuable alive and unharmed over a period of days or weeks.

Digital assets held in self-custody remove nearly all of it. A private key or a recovery phrase is a bearer instrument: whoever holds it holds the asset, and a coerced transfer settles in minutes, irreversibly, at any hour, from anywhere. The consequences cascade through every legacy assumption:

- **Time-to-loss collapses.** The window in which trained responders, insurers, and law enforcement traditionally operate can close before anyone knows an incident has begun.
- **The person becomes the vault.** Where custody is concentrated in one individual's knowledge or devices, that individual is a single point of failure, and coercing them is the attack.
- **Recovery is not a fallback.** There is no issuer to reverse the transaction and no insurer of the rails. What is gone is gone, which raises the value of prevention relative to response.
- **The family is in scope.** Because leverage is the mechanism, anyone the principal will trade assets to protect is a target: spouses, children, parents, and in some reported cases, colleagues.

None of this means traditional protective disciplines are obsolete. It means they are insufficient on their own, and that the custody architecture itself must be designed to hold under physical duress, not just cyber attack.

— 04 / THE EXPOSURE CHAIN

HOW EXPOSURE ACCUMULATES

Principals rarely become targets through one mistake. Exposure accumulates across layers that individually look harmless:

- **On-chain transparency.** Public ledgers are permanent and searchable. Wealth that would be invisible in a brokerage account is legible to anyone with analytic tooling, and address clustering can connect holdings a holder believed were separate.
- **Breached identity data.** Exchange and service breaches have repeatedly exposed customer names, contact details, and home addresses. The 2025 insider-enabled leak at a major U.S. exchange demonstrated the mechanism publicly: identity data joined to known holdings converts a cyber incident directly into a physical targeting risk.
- **Professional visibility.** Funding announcements, conference speaking, company pages, and media profiles establish that a person controls or influences significant assets. This is often unavoidable; it should at least be deliberate.
- **Lifestyle signal.** Social posts that display wealth, holdings, trading results, locations, or family routines materially assist target selection. Both major analytics firms now list social discipline among their primary recommendations.
- **Pattern of life.** Predictable routines between residence, office, school runs, and travel are what convert interest into opportunity. Reported European cases have clustered around residences and routine movements, not offices or events.

The protective takeaway is that exposure review must span all five layers at once. Reducing any single layer helps; the compounding across layers is what an assessment must map, because it is what an organized crew maps.

— 05 / THE FRAMEWORK

THE PROTECTIVE FRAMEWORK

ERS organizes protection around one moment: the incident, the X. Everything a principal, family, or firm can do falls before it or after it, and the disciplines reinforce each other.

Before the X: prevention and preparation

Reduce what is discoverable. A structured exposure assessment across on-chain footprint, breached data, public records, and social presence, followed by systematic reduction: data broker removal, registration hygiene, address separation, and family social media discipline. Protective intelligence then monitors for the early indicators that typically precede targeting, including impersonation, doxing, and hostile reconnaissance.

Design custody to fail safely under duress. The objective is that no single person, under any pressure, at any hour, can move everything. Multi-party approval, transaction limits, time-locks, allowlisted destinations, and formal duress protocols convert a coercive attack from a minutes-long transfer into a stalled negotiation, which is the environment traditional response was built for. Done well, this is also a deterrent: crews select targets by expected yield, and architecture that visibly cannot pay quickly changes the calculus.

Train the principal and the household. Situational awareness, surveillance recognition, travel discipline, and family crisis protocols, rehearsed rather than merely briefed. Most executives have never been trained to recognize hostile surveillance or to manage the first minutes of an incident; capability, not awareness, is the objective. Training must include spouses and, age-appropriately, children, because the household is in scope.

Harden the fixed points. Residential security assessment and remediation, vetted drivers and secure movement for elevated-threat periods and travel, and technical measures including device hardening, clean travel devices, and communications discipline. Reported incident patterns concentrate at homes and in transitional spaces; protective weight should match.

After the X: response and recovery

Response quality is decided before the incident. A credible posture includes a pre-agreed response protocol that defines who communicates, who decides, and who engages law enforcement and counsel; duress signals and pre-positioned decision rights; kidnap and ransom insurance coordinated with a professional response capability; and law enforcement liaison established in the jurisdictions where the principal actually lives and moves. After any incident or near-incident, a disciplined after-action process feeds back into the Before-the-X controls.

— 06 / GOVERNANCE

IMPLICATIONS FOR BOARDS, FUNDS, AND FAMILY OFFICES

For organizations, this threat class lands as a duty-of-care and continuity issue, not only a personal one. Key management staff are targets precisely because of their organizational role, and an attack on an executive's family is an attack on the firm's ability to operate. Boards and investment committees should be able to answer four questions:

- Which individuals, including family members, could be coerced into moving material assets, and what stops a transfer executed under duress?
- What identity and address data about those individuals exists in third-party systems, and what happened to it in the last breach?
- Have at-risk principals and their households received scenario-based prevention training, or only a briefing document?
- If an incident began tonight, who would know, who would decide, and within how many minutes?

Where the answers are unclear, the gap is usually organizational: custody sits with the CISO or operations, personal security with a separate vendor, and the family with no one. The threat exploits exactly that seam. Converged risk requires a converged program with single-point accountability.

— 07 / CLOSING

THE STANDARD HAS CHANGED

The industry spent a decade hardening its technology, and largely succeeded; that success is part of why adversaries moved to the person. The protective standard for digital asset wealth now spans exposure management, duress-resistant custody, trained households, and rehearsed response. None of these is exotic. All of them exist today, and the cost of implementing them is small against a single incident.

Executive Risk Services operates at the intersection of cyber, physical, and human risk for principals in digital assets, finance, and technology. Engagements begin with a private conversation and are accepted by referral or direct invitation.

— SOURCES & METHOD

Incident statistics: CertiK, Skynet Wrench Attacks Report (February 2026); Chainalysis, 2025 Crypto Crime Mid-Year Update. Incident references reflect public reporting by international news organizations. Consistent with ERS editorial policy, this paper discusses targeting and attack patterns at the level required for protection and omits operational detail, victim identification, and ransom specifics.