— BRIEFING / 003 · JULY 2026

THE INSIDER AT THE SIGNING TABLE.

Every architecture for holding digital assets terminates in a person who can approve. Cryptography changes who that person is and where they sit. It never removes them.

EXECUTIVE RISK SERVICES

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

info@executiveriskservices.com · referral or invite only

— 01 / THE PREMISE

SECURITY SPENDING HAS MOVED. THE THREAT HAS NOT.

The digital asset industry has spent a decade hardening the wrong end of the problem. Exchange breaches, smart-contract exploits, and bridge failures drove enormous investment in cryptographic and infrastructural defense. That investment worked. Stealing digital assets by defeating the technology has become genuinely difficult.

So the attack moved. It did not disappear. When the cryptography holds, the rational adversary stops attacking the cryptography and starts attacking the people who operate it. This is not a hypothetical shift. It is the observable pattern of the last twenty-four months, and it is accelerating.

This briefing makes a single argument and follows it to its conclusion. Every architecture for holding digital assets, however sophisticated, terminates in a human being who can authorize a transaction. The insider threat in this industry is not a data-exfiltration problem borrowed from the enterprise world. It is a problem about the small number of people who, at the final step, can make value move.

THREE CUSTODY ARCHITECTURES

ONE TERMINAL CONTROL: A HUMAN

ZERO FRAMEWORKS THAT ENUMERATE IT

— 02 / THE CONTROL SURFACE

THREE ARCHITECTURES, ONE TERMINAL CONTROL

Firms holding digital assets sit somewhere on a spectrum of custody sophistication. The engineering differs enormously across that spectrum. The human terminus does not.

TIER I — AD HOC SELF-CUSTODY

Keys live on hardware wallets, in seed phrases, or in a multisig where the signers are the founders. There is frequently no dedicated security function. The people who built the company are the people who hold the keys.

At this tier the insider threat and the physical threat are not two problems. They are one problem viewed from two angles. The key cannot be reached remotely because it was never exposed to a network. It can only be reached through the person. That makes the human the entire attack surface, and you cannot firewall a founder's house.

TIER II — MPC AND WALLET-AS-A-SERVICE

Key material is sharded and the single private key ceases to exist. This is a real and worthwhile security investment, and many firms emerge from the migration believing they have solved custody risk.

They have not solved it. They have relocated it. What replaces the key is a policy engine, a set of quorum definitions, and a platform operator — each a control surface, each administered by a human. Whoever can edit transaction policy or approval thresholds can move funds without ever touching key material. And a 3-of-5 signing policy is only 3-of-5 if the five are genuinely independent: if two report to the same executive and one is a contractor, the cryptographic threshold and the real-world threshold are different numbers.

You cannot wrench-attack a key shard. You can absolutely wrench-attack a quorum member.

TIER III — QUALIFIED CUSTODIAN

Custody is delegated to a regulated institution with hardware security modules, a fiduciary duty, and an audit trail. For the asset owner this feels like the problem has been solved by delegation.

It has been split into two insider problems, and one of them is still yours. The custodian is a company staffed by people whose insider-threat program is now load-bearing for your assets and which you have almost certainly never reviewed. And delegating custody does not delegate authorization: somebody at your firm still instructs the custodian to release funds. When that person is compromised or coerced, the custodian faithfully executes a perfectly authenticated instruction. The theft is fully authorized, because the authorizer was the target.

— 03 / THE UNGOVERNED SEAM

TWO CONTROL ESTATES, ONE UNGOVERNED SEAM

Most firms operate two mature and entirely separate control estates.

The cyber estate is owned by the CISO, mapped to a recognized framework, instrumented with telemetry, and audited. It contains perhaps forty controls spanning identity, endpoint, network, detection, and response. It is the estate a security questionnaire asks about.

The physical estate is owned by facilities, or by a landlord, or in practice by nobody. It contains perimeter, access control, surveillance, and life-safety controls. It is assessed episodically, and its telemetry does not reach the security operations center.

Between them sits the authorizer: the small set of humans who can cause digital assets to move. Neither estate is scoped to them. The cyber estate protects the systems the authorizer uses. The physical estate protects the building the authorizer sits in. Neither protects the authorizer at home, in transit, or under coercion — and neither treats the authorizer's own compromise as the primary loss scenario.

An adversary who cannot defeat the cryptography and will not defeat the SOC does not need to. They can coerce a single authorizer at their residence on a Sunday, and every control in both estates will report green while the funds leave, correctly signed and fully authorized.

— 04 / SELF-ASSESSMENT

FOUR QUESTIONS FOR YOUR BOARD

A firm does not need to hire anyone to begin. It needs to answer four questions honestly. In our experience, the discomfort of answering them is itself the finding.

Who, by name, can cause value to move — alone or in a reachable quorum of two? If the list is longer than you expected, or you cannot produce it quickly, that is the finding. Building it takes an afternoon and costs nothing.

For each of those people, does anyone own the risk to their person, their home, and their family? In most firms the answer falls between physical security and duty of care and lands on nobody.

If a custodian or platform vendor holds part of your control surface, have you reviewed their insider-threat program? Extending trust without audit is not delegation. It is assumption.

If an authorizer were coerced tonight, who would you call — and have you spoken to them before? If the honest answer is a search engine, you do not have a response capability. You have a hope.

— 05 / SOURCES AND METHOD

SOURCES AND METHOD

A companion technical document — the ERS Fused Control Reference Architecture — maps the authorizer-specific controls referenced here against NIST CSF functions and an existing enterprise control catalog, at a depth a security engineer can implement and an auditor can test. It is available on request.

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 is an analytical argument drawn from ERS's operational experience advising principals in digital assets, and from the public record of coercion and insider events across the sector. As a matter of editorial policy, ERS briefings name no victims and describe no attack methods. Where this briefing describes a threat, it describes the pattern and the protective principle. It does not provide a method. That restraint is a credibility signal, not an omission.