AEGEAN INTELLIGENCE GROUP

PUBLISHABLE MARKET RESEARCH · 2026

CLASSIFICATION
PUBLIC

PRODUCT ID
PMR-2026-0619-USA-002

TIMELINESS
DURABLE

DATE
2026-06-19

The Protection Premium

Executive and Principal Security Became a Priced, Disclosed Function. The Threat Moved to the Data Layer. The Ownership Did Not Follow.

37.8%

S&P 500 FIRMS DISCLOSING AN EXECUTIVE SECURITY PERK IN 2025, FROM 23.6% IN 2021

~70

RECORD VIOLENT 'WRENCH' ATTACKS ON CRYPTO HOLDERS LOGGED IN 2025

24%

OF ORGANIZATIONS HAVE CONVERGED PHYSICAL AND CYBER SECURITY

EXECUTIVE DASHBOARD

In the eighteen months since a health-insurance chief executive was shot dead on a Manhattan sidewalk, corporate America has repriced the safety of its leaders. Security perquisites that boards once buried or omitted are now disclosed, benchmarked, and defended in proxy statements. At the same time, the people most worth protecting, executives, founders, and the principals behind family offices, are being located through a different channel entirely: leaked data, people-search brokers, and their own online footprints. This brief maps where the protection money is going, where the threat actually originates, and the gap between the two.

THESIS

Executive and principal protection has crossed from a discretionary perk into a priced, disclosed, board-level function, but the threat it is bought to manage has migrated to the data layer, where a person's location and wealth are assembled from breaches, brokers, and social media. The binding constraint is no longer whether to spend on protection. It is that **spending is rising on guards and details while the exposure is created upstream, in data nobody is accountable for**. Until physical security, cyber, and privacy are owned as one function, additional protection spending will buy **materially less protection than its price implies**.

KEY STATISTICS

37.8%
S&P 500 firms disclosing an executive security perk in 2025 (23.6% in 2021); median value $130,468[1]

$1.7M
UnitedHealth's first-ever executive-security disclosure, nearly all spent after Dec 4, 2024[3, 4]

10-15x
reported rise in executive-protection assessment requests after the UnitedHealthcare killing[5]

25%
of S&P 500 CEOs received personal or home security for the year to Sept 2025 (18% prior)[7]

~$27M
Meta's 2024 spend protecting Mark Zuckerberg, more than six big-tech CEOs combined[8]

55-72
violent attacks on crypto holders logged by independent trackers in 2025, a record[13, 15, 16]

69,461
Coinbase customers whose names, home addresses and balances were exposed in 2025[21]

63%
of family offices carry no cyber insurance; 31% have no incident-response plan[32]

Scope & method. Open-source intelligence verified against allowlisted Tier 1 to 3 sources per AEIG source policy. Corporate spending figures derive from SEC proxy filings and the compensation-data firms that aggregate them. Criminal matters are drawn from indictments and arrests, are noted as unproven, and defendants are presumed innocent. Attack-frequency counts differ across independent trackers and are presented as a range, not a census; market-size estimates for executive protection and kidnap-and-ransom insurance diverge widely across vendors and are flagged where used. Geographic focus is the United States, with European incidents where they illustrate a shared pattern. Timeliness: DURABLE, with the structural argument stable over six to eighteen months even as individual figures refresh each proxy season and reporting cycle.

KEY JUDGMENTS

Six judgments anchor this assessment. Each is tied to cited evidence in the sections that follow and carries an explicit confidence level.

1 High

Executive protection has structurally crossed from perk to disclosed corporate function. The share of S&P 500 companies disclosing a security perquisite rose from 23.6 percent in 2021 to 37.8 percent in 2025, and the median disclosed value more than doubled. This is a durable governance shift, not a post-incident spike.[1, 2, 7]

2 High

The December 2024 killing of the UnitedHealthcare chief executive was the catalyst, not the cause. Assessment requests, first-time disclosures, and threat counts all stepped up immediately afterward, but they accelerated an existing rise in executive targeting rather than creating it.[5, 6, 9]

3 Moderate

The threat is migrating to the data layer. The dominant enabling vector for physical attacks on wealthy individuals is now their digital exposure, data broken out of corporate breaches, sold by people-search brokers, or volunteered on social media, rather than opportunistic proximity. The end-to-end causal chain is rarely proven in a single case, but the direction is unambiguous.[21, 22, 16]

4 Moderate

Violent attacks on holders of liquid wealth reached a record in 2025 and the method is professionalizing. Independent trackers logged between roughly 55 and 72 attacks, disagreeing on the count but not the trend, and 2025 to 2026 cases show planning, disguises, and remote coordination.[13, 15, 16, 17, 18]

5 Moderate

Regulation is reaching for the address but cannot yet close the exposure. California's deletion platform and a handful of state and judicial privacy statutes are live, but coverage is partial, compliance is uneven, and the central legal questions remain unresolved.[24, 27, 28]

6 High

No single function owns the combined exposure. Physical security, cyber, and privacy remain siloed in most organizations and almost all family offices; only about a quarter of organizations have converged physical and cyber security. This ownership gap, not the level of spending, is the binding weakness.[32, 33]

SECTION 01 · MARKET

From Perk to Priced Function

Boards have repriced the safety of their leaders in public. The spend is real, it is disclosed, and it is no longer optional. But the published numbers capture only the visible tip.

On December 4, 2024, UnitedHealthcare chief executive Brian Thompson was shot dead outside a Midtown Manhattan hotel ahead of the company’s investor day; he had no security detail.[6] The corporate response is now measurable in the one place companies cannot easily obscure: their proxy statements. UnitedHealth’s April 2025 filing disclosed roughly $1.7 million in executive-security spending for 2024, a line item absent from every prior proxy, with almost all of it incurred in the weeks after the killing.[3, 4] Across the market the pattern is the same. Equilar’s analysis of S&P 500 filings shows the share of companies disclosing a security perquisite rose from 23.6 percent in 2021 to 33.5 percent in 2024 to 37.8 percent in 2025, while the median disclosed value climbed from about $55,000 to roughly $130,000 over the same period.[1]

The immediate demand spike is well documented. Allied Universal, which says it serves more than 80 percent of the Fortune 500, reported that requests for protective assessments and executive protection ran 10 to 15 times their pre-December level; Global Guardian received roughly 70 personal-

protection requests in the two days after the killing against a normal run rate of 150 to 175 a month, and corporate security chiefs reported a sharp rise in violent threats to executives through 2025.[5, 6, 12] A separate dataset from The Conference Board found that 25 percent of S&P 500 chief executives received personal or home security for the year to September 2025, up from 18 percent, with median spend near $75,000 and the top decile averaging about $1.2 million.[7] The outlier at the top is instructive: Meta disclosed roughly $27 million to protect Mark Zuckerberg in 2024, more than Apple, Nvidia, Amazon, Alphabet, Microsoft, and Palo Alto Networks spent on their chief executives combined.[8]

Beneath the disclosures sits a services industry whose true size is harder to fix than its growth. The broad United States guarding industry is well measured at roughly $50 billion, but the executive-protection segment within it is estimated only by second-tier market-research firms whose figures for the same year diverge by more than tenfold, so the honest reading is a fast-growing but poorly bounded market rather than a precise number.[10] The threat underneath the spend is clearer. A long-running open-source dataset of attacks on corporate executives recorded that 2025 incidents had already doubled the prior full year by late October, with physical attacks comprising 85 percent of cases and chief executives 64 percent of targets, while an ASIS survey found 72 percent of security professionals reporting more public threats against executives even as only 28 percent had a formal protection policy.[9, 10] The addressable population is also expanding: the global count of high-net-worth individuals rose to about 25.3 million in 2025.[11]

ASSESSMENT · HIGH CONFIDENCE

Executive protection is now a disclosed, benchmarked, board-level cost rather than a discretionary perk, and the shift is durable because it is enforced by proxy advisers, investor scrutiny, and duty-of-care expectations, not by a single news cycle. The strategic implication is that the published figures are a floor, not a ceiling. They capture only what public companies must disclose, omit private companies and family offices entirely, and lag the threat by a full reporting cycle. Reading the proxy numbers as the size of the problem understates it.

Rationale: The Equilar time series, the Conference Board dataset, the post-incident demand indicators, and the gap between rising threat counts and low formal-policy adoption all point to institutionalization with a large undisclosed remainder.

SECTION 02 · THREAT

The Threat Moved to the Data Layer

A guard at the door does not address how the attacker found the door. The defining shift of this threat environment is that physical targeting now begins with data.

The most visible edge of the shift is the wave of violent robberies and kidnappings aimed at holders of liquid wealth, particularly cryptocurrency. Independent trackers disagree on the exact count but not the trajectory: a widely cited public dataset logged roughly 70 physical attacks on crypto holders in 2025, a record, while the blockchain-intelligence firms TRM Labs and CertiK counted approximately 55 and 72 respectively, each noting the true figure is higher because many incidents are recorded only as ordinary robberies.[13, 15, 16] Chainalysis found 2025 on pace for roughly twice the prior record and correlated the violence with bitcoin's price.[14] France alone documented around 40 crypto-related kidnappings since mid-2023, concentrated in a 2025 surge.[19]

The method is professionalizing. In January 2025 a co-founder of the hardware-wallet maker Ledger and his wife were abducted from their home in France, and one of his fingers was severed to extract a roughly 10-million-euro ransom.[20] In Manhattan, two men were charged with holding and torturing an Italian visitor for days to force out a bitcoin password.[35] And on January 31, 2026, two teenagers drove some 600 miles to Scottsdale, Arizona, posed as delivery drivers, and forced their way into a home in a roughly $66 million crypto robbery while being directed by phone over an encrypted app, a remote-coordination pattern that federal prosecutors describe in a parallel indictment of a Tennessee crew which used the same delivery-driver disguise to steal $6.5 million in a single incident.[17, 18]

What connects these cases is not a weakness in any blockchain; it is the targeting data. Attackers build victim profiles from social-media displays of wealth, public appearances, and leaked or brokered datasets. The exposure is concrete: in 2025 Coinbase disclosed that bribed overseas contractors had exfiltrated data on roughly 69,461 customers, including names, home addresses, and account balances, the precise inputs a physical attacker needs.[21] The clearest proof that brokered data translates into physical harm comes from outside crypto. In the June 2025 murder of a Minnesota state legislator and her husband, the accused is documented to have used people-search and data-broker sites to locate home addresses, with a handwritten list of around eleven such sites and dossiers on dozens of officials recovered.[22] A 2026 Senate report estimated that data-broker breaches have cost United States consumers more than $20 billion.[23]

ASSESSMENT · MODERATE CONFIDENCE

Physical protection and data exposure are now the same problem approached from opposite ends. An attacker no longer needs proximity to select a target; a breach, a broker purchase, or a social-media feed supplies identity, address, and an estimate of wealth before any physical step. Confidence is moderate because the breach-to-attack chain is rarely proven end to end in a single case, but the direction is unambiguous and the enabling datasets are documented. The implication is that a detail or alarm system bought without a parallel program to suppress the principal's data footprint defends the last ten feet of a path that was set in motion much earlier.

Rationale: The Coinbase exposure, the documented broker-sourcing in the Minnesota case, the profiling patterns reported by analysts, and the recurring planned-and-disguised method in 2025 to 2026 cases jointly support the data-layer framing; the causal caveat is stated explicitly.

SECTION 03 · REGULATORY

The Law Is Reaching for the Address

Lawmakers and regulators have begun to treat personal data as a physical-safety problem. The instruments are live, but the coverage is partial and the central questions are unresolved.

The most consequential new instrument is California's Delete Act. Its Delete Request and Opt-out Platform, run by the California Privacy Protection Agency, went live on January 1, 2026 as the first state-hosted mechanism letting a resident direct every registered data broker to delete their information through a single request. More than 18,000 requests were filed in the first 48 hours, and more than 242,000 residents had enrolled by early March against more than 575 registered brokers; broker compliance becomes mandatory on a 45-day cycle from August 1, 2026.[24, 25]

Enforcement has teeth but narrow reach. California's privacy regulator stood up a data-broker enforcement strike force in late 2025 and has fined unregistered brokers, including a $45,000 penalty against one firm that had resold lists of people with medical conditions.[26] Yet only four states, California, Vermont, Texas, and Oregon, maintain broker registries at all, and an analysis by the Electronic Frontier Foundation found roughly 750 brokers registered somewhere, with large numbers absent from individual state lists, evidence that registration is incomplete and the deletion right stops at state lines.[27]

A second track protects specific people rather than data in general. New Jersey's Daniel's Law, enacted after the murder of a federal judge's son, lets judges, prosecutors, and police demand that their home addresses be withheld and has driven thousands of assigned claims against brokers; but the New Jersey Supreme Court heard argument in March 2026 on the core question of what mental state a

violation requires, leaving the statute's reach unsettled, and a federal counterpart protects only federal judges through an administrative removal process.[28, 29] The Federal Trade Commission has separately barred data brokers from selling sensitive location data, citing risks that include physical violence.[30] The structural limit is plain: these protections cover officials, or Californians who opt in, or specific data categories, leaving executives and private principals to assemble their own remedies.

ASSESSMENT · MODERATE CONFIDENCE

The regulatory direction validates the threat thesis, lawmakers now treat data exposure as a safety issue, but it does not yet provide a usable shield for the executive or principal class. Coverage is fragmented by state, by profession, and by data type; the most powerful private-enforcement model is under constitutional review; and deletion is a recurring chore against brokers who re-acquire data continuously. The practical implication is that data-footprint suppression remains a private, ongoing operational task for principals, not a problem the law has solved, and any protection program should treat compliance tools as one input rather than a perimeter.

Rationale: The deletion-platform go-live and uptake, the strike-force actions, the four-state registry limits, the unresolved Daniel's Law question, and the category-specific FTC orders together show real momentum but partial, contested coverage.

SECTION 04 · RISK TRANSFER

Insurance Begins to Price the Person

The risk-transfer market is following the threat from the corporation to the individual, broadening coverage and repricing it, while the buyers most exposed remain the least covered.

The kidnap-and-ransom and special-crime market, historically a corporate product, is moving toward private and high-net-worth buyers. A senior private-client broker reported binding personal K&R policies at a rate of roughly one every other day in early 2026, against a historical norm of a handful a year, and argued the cover should be offered to families the way cyber insurance is.[31] The product itself is broadening beyond classic abduction to bundle threat and assault, extortion, express kidnapping, and, increasingly, virtual kidnapping and artificial-intelligence-enabled impersonation extortion, in which attackers use personal details to make a fabricated threat credible.[31]

The market's size is genuinely uncertain. Vendor estimates of the global K&R line cluster between roughly $2 billion and $4 billion for 2024 and diverge by nearly twofold, so the credible claim is rising demand and broadening cover rather than a precise figure.[31] What buyers increasingly pay for is less

the indemnity than the embedded response capability, the crisis consultants and former investigators who manage an incident, which is itself a sign that the market treats prevention and response, not reimbursement, as the value.

The buyers with the most concentrated exposure are the least prepared. Deloitte's survey of family offices found that 43 percent had experienced a cyberattack, rising to 57 percent in North America and 62 percent among those over $1 billion in assets, yet 63 percent carried no cyber insurance and 31 percent had no incident-response plan, and only 22 percent ranked cybersecurity among their top risks.[32] Family-office reporting now records demand for support spanning medical, cyber, and physical security together, an acknowledgment that these exposures arrive as one.[34] A family office concentrates a principal's wealth, data, and household staff in a lightly governed entity, precisely the profile the data-layer threat exploits, and the insurance and preparedness gap is the measure of how far risk transfer still lags the exposure.

ASSESSMENT · MODERATE CONFIDENCE

Risk transfer is repricing the individual, but the coverage gap among the most exposed buyers, family offices and private principals, is the commercial opportunity and the warning at once. The market is correctly migrating from corporate kidnap-and-ransom toward bundled personal-security cover with embedded response, and the value is shifting from indemnity to prevention. Confidence is moderate because K&R market data is vendor-sourced and dispersed. For a private principal the binding question is not whether a policy exists but whether anyone has integrated the cover, the response plan, the data suppression, and the physical posture into one program; today, in most cases, no one has.

Rationale: The broker-reported demand shift, the documented product broadening, the wide vendor dispersion on market size, and the Deloitte preparedness gaps support both the repricing and the under-coverage of the most exposed.

SECTION 05 · GOVERNANCE

No One Owns the Seam

The physical detail, the cyber team, and the privacy function are bought separately, report separately, and defend the same person separately. That division is the real exposure.

For all the new spending, the function that would make it coherent barely exists. The benchmark industry study of security convergence found that only about 24 percent of organizations had merged their physical and cybersecurity functions, even though 96 percent of those that had converged two or

more functions reported positive results.[33] In most enterprises the executive-protection detail, the security operations center, and the privacy or legal team that could suppress a principal's data operate in separate reporting lines, so the person being targeted through their data is defended by a physical program that never sees the data.

The gap is widest exactly where the exposure is most concentrated. Family offices, which hold the wealth and run the households of the principals most likely to be targeted, are under-built across the board: most lack incident-response plans, cyber insurance, and dedicated security staff, and few rank security among their priorities.[32] Where larger institutions have responded, the response is organizational, the elevation of a chief security officer or equivalent who owns physical, cyber, and travel risk together; one large defense contractor's filings show its security chief mandating how the chief executive travels, a small but telling sign of converged authority.[2, 34]

The lesson of the preceding sections is that protection now fails at the seams. Spending rises on guards while exposure is created upstream in data; regulation addresses fragments; insurance indemnifies an incident a coordinated program might have prevented. The organizations and families that are genuinely protected will be those that assign one owner to the whole exposure, treating the principal's digital footprint, physical posture, travel pattern, household, and risk transfer as a single managed surface rather than four separately procured services that happen to defend the same person. Integrated risk ownership, not incremental protection spending, is the differentiator that this threat environment rewards.

ASSESSMENT · HIGH CONFIDENCE

The binding weakness in personal and executive protection is not the level of spending; it is the absence of a single owner for the combined physical, cyber, and privacy exposure. Most organizations have not converged these functions and most family offices have not built them, which means rising protection budgets are deployed against a threat whose origin sits in a function nobody is accountable for. For boards, general counsel, and the principals behind family offices alike, the next unit of protection value comes from integration and ownership, not from another detail or another tool. The firms and families that consolidate the seam will convert the same spend into materially more security.

Rationale: The roughly 24 percent convergence rate, the family-office preparedness gaps, the emergence of converged chief-security-officer authority, and the cross-cutting evidence that every prior section fails at an interface between functions jointly support ownership, not spend level, as the binding constraint.

SECTION 06 · OUTLOOK

Three Scenarios, Twelve Months

Construction confidence reflects analytical quality, not probability. Each scenario carries a risk velocity and the signal that would confirm it.

Baseline · Institutionalization continues, integration lags

CONSTRUCTION CONFIDENCE: HIGH · VELOCITY: GRADUAL

Disclosure and spend keep rising into the 2026 and 2027 proxy seasons, and executive protection consolidates as a standard board-level cost. The data-layer threat persists at or above 2025 levels, with continued attacks on liquid-wealth holders and breach-enabled targeting. California's deletion regime beds in and a few states copy it, but coverage stays partial. Most organizations and nearly all family offices continue to buy physical, cyber, and privacy separately. Risk transfer broadens toward private clients. Protection spending rises faster than protection integration, and the seam stays open.

SIGNAL TO WATCH: A FURTHER RISE IN S&P 500 SECURITY-PERK DISCLOSURE IN THE 2026 PROXY SEASON WITH NO CORRESPONDING RISE IN CONVERGED SECURITY FUNCTIONS

Deterioration · A networked targeting event

CONSTRUCTION CONFIDENCE: MODERATE · VELOCITY: RAPID

A breach or broker dataset is shown to have directly enabled a high-profile attack on an executive or principal, or a coordinated, remotely directed campaign strikes several wealthy targets in a short window. Liability and duty-of-care exposure crystallize; insurers tighten terms or reprice personal cover sharply; regulators and plaintiffs press data brokers harder. Protection demand spikes again, but the supply of genuinely integrated providers is thin, so spending surges into a market that cannot yet deliver the seam.

SIGNAL TO WATCH: A DOCUMENTED, PUBLICLY ATTRIBUTED CHAIN FROM A NAMED DATA SOURCE TO A PHYSICAL ATTACK ON A PRINCIPAL, OR A STEP-CHANGE IN KIDNAP-AND-RANSOM OR PERSONAL-SECURITY PRICING

Stabilization · Integration becomes standard practice

CONSTRUCTION CONFIDENCE: LOW-MOD · VELOCITY: STRUCTURAL

Boards, general counsel, and family offices move ownership of combined physical, cyber, and privacy risk to a single accountable function; data-suppression and protective-intelligence programs become routine; regulation broadens beyond California and specific professions toward a general deletion right; and insurers reward integrated programs with capacity and price. Protection spend flattens or is reallocated as integration converts existing budgets into measurably better outcomes.

SIGNAL TO WATCH: CONVERGENCE RATES RISING MATERIALLY ABOVE THE LONG-STANDING ONE-QUARTER LEVEL, A FEDERAL OR MULTI-STATE DELETION STANDARD, OR INSURER UNDERWRITING THAT EXPLICITLY CREDITS INTEGRATED PROGRAMS

ASSESSMENT · MODERATE CONFIDENCE

Across all three paths the central fact holds: the threat originates in data and the defense is organized by silo, and that mismatch resolves only in Stabilization. The most probable twelve-month path is Baseline, in which spending and disclosure keep rising while integration lags, leaving the seam open. Deterioration is a fast, common-mode risk that can arrive from a single well-publicized data-to-doorstep event. Stabilization is the slowest path, because it requires organizational change rather than procurement, but it is the only one that converts protection spending into proportionate protection.

Rationale: The durability of the disclosure trend, the persistence and professionalization of data-enabled attacks, the partial regulatory coverage, and the low convergence rate jointly make continued spend-without-integration the default and integration the slow but decisive variable.

SOURCE REGISTRY

1. Equilar / Harvard Law School Forum on Corporate Governance, "Early Look: Executive Security Perks on the Rise," 2026.
2. Equilar / Harvard Law School Forum on Corporate Governance, "Executive Security Spending Shifts From Perk to Priority," 2025.
3. UnitedHealth Group, "Form DEF 14A Proxy Statement, U.S. Securities and Exchange Commission," 2025.
4. STAT, "UnitedHealth discloses $1.7 million in security spending after slaying of top executive," 2025.
5. Reuters (via Insurance Journal), "Corporate America Boosts Security Spending After UnitedHealth Murder, Filings Show," 2025.
6. CNN Business, "Companies step up security in wake of UnitedHealthcare CEO killing," 2024.
7. The Conference Board / ESGauge (via Axios), "Spending on CEO security surged over the last year," 2025.

8. Fortune (with Financial Times analysis), "Meta spends more guarding Mark Zuckerberg than Apple, Nvidia, Microsoft, Amazon, and Alphabet do for their CEOs combined," 2025.
9. Security Executive Council (with Mercyhurst University), "Executive Targeting Report: Analysis of Attacks on Corporate Executives, 2003-2025," 2026.
10. ASIS International / Security Management, "How Executive Protection Is Changing One Year After the UnitedHealthcare CEO Attack," 2025.
11. Capgemini, "World Wealth Report 2026," 2026.
12. Allied Universal, "World Security Report 2025," 2025.
13. Jameson Lopp, Physical Bitcoin Attacks dataset (via The Block), "A record year for wrench attacks," 2026.
14. Chainalysis, "2026 Crypto Crime Report; 2025 Mid-Year Update," 2026.
15. TRM Labs, "The Rise of Wrench Attacks and Crypto-Related Violent Crime," 2025.
16. CertiK (via crypto.news), "Crypto wrench attacks push Coinbase security bill to $8.7M," 2026.
17. U.S. Department of Justice, U.S. Attorney's Office, Northern District of California, "Three Tennessee Men Indicted on Robbery, Kidnapping, and Conspiracy Charges Related to a $6 Million Cryptocurrency Robbery Spree," 2026.
18. The Block, "Teens face felony charges after 600-mile drive to allegedly attempt a $66 million crypto robbery," 2026.
19. France 24 / AFP, "France reports over 40 cryptocurrency kidnappings," 2026.
20. France 24, "Suspect in French crypto-sector kidnappings arrested in Morocco, justice minister says," 2025.
21. Bloomberg, "Coinbase Says Former Agent Arrested in India After Exchange Hack," 2025.
22. Electronic Privacy Information Center (EPIC), "Data Broker Harms to Public Officials," 2026.
23. U.S. Senate Joint Economic Committee, "Data Broker Breaches Cost U.S. Consumers More Than $20 Billion," 2026.
24. California Privacy Protection Agency, "Delete Request and Opt-Out Platform (DROP); Information for Data Brokers," 2026.
25. National Law Review (Robinson & Cole LLP), "The Compliance Wave Is Coming: Data Brokers Brace for DROP Deletion Requests," 2026.
26. California Privacy Protection Agency, "CalPrivacy Brings New Round of Enforcement Actions Against Data Brokers," 2026.
27. Electronic Frontier Foundation (with Privacy Rights Clearinghouse), "Why Are Hundreds of Data Brokers Not Registering With States?," 2025.
28. New Jersey Monitor, "NJ Supreme Court hears arguments over Daniel's Law," 2026.
29. Administrative Office of the U.S. Courts, "Congress Passes the Daniel Anderl Judicial Security and Privacy Act," 2022.
30. Federal Trade Commission, "FTC Takes Action Against Gravy Analytics and Venntel for Unlawfully Selling Location Data," 2024.
31. Insurance Business America, "Kidnap-and-ransom insurance demand surges among high-net-worth families," 2026.
32. Deloitte Private, "The Family Office Cybersecurity Report 2024," 2024.
33. ASIS Foundation, "The State of Security Convergence in the United States, Europe, and India," 2019.
34. RBC Wealth Management & Campden Wealth, "The North America Family Office Report 2025," 2025.

35. NBC News / CBS News, "Two men plead not guilty in New York crypto kidnapping and torture case," 2025.

AEGEAN INTELLIGENCE GROUP

Publishable Market Research

Timeliness: DURABLE. The structural argument here, protection institutionalizing, the threat migrating to data, and ownership lagging, is durable on a six-to-eighteen-month horizon. The specific figures refresh on known cadences: proxy-season disclosure each spring, attack-frequency counts each quarter, and regulatory milestones such as the August 2026 start of mandatory broker deletion in California. An Update Addendum will follow on a material change in any of these.

Classification: PUBLIC. Prepared on open-source intelligence verified against allowlisted sources. Corporate and government figures are cited to their published sources; criminal matters are unproven allegations and defendants are presumed innocent; analytic judgments are Aegean's.

contact@aegeanintel.com · aegeanintel.com