AEGEAN INTELLIGENCE GROUP

PUBLISHABLE MARKET RESEARCH · 2026

CLASSIFICATION
PUBLIC

PRODUCT ID
PMR-2026-0619-GLBL-006

TIMELINESS
DURABLE

DATE
2026-06-19

Who Owns the Risk?

Physical, Cyber, and Insider Threats Converged Into One Surface. Accountability for It Did Not. The Case for a Single Owner of Integrated Risk.

24%

OF ORGANIZATIONS HAVE CONVERGED PHYSICAL AND CYBER SECURITY

$17.4M

AVERAGE ANNUAL COST OF INSIDER RISK PER ORGANIZATION

~4%

OF DIRECTORS FEEL ABLE TO OVERSEE THEIR CYBER AND AI RISK

EXECUTIVE DASHBOARD

A cyber breach now forces a physical shutdown. A phone call to a help desk defeats a technical control. An insider with a badge and a login is one person. A geopolitical shift reprices them all at once. Risk has merged into a single surface, but the accountability for it remains split across a cyber chief, a physical-security head, a general counsel, and, in family offices, often no one. This brief argues that the binding constraint is no longer spend or tooling. It is ownership.

THESIS

Physical, cyber, insider, and geopolitical risk have merged into one surface on which each threat feeds the others, but accountability for that surface is split across separate functions, and in most enterprises and nearly all family offices **no single executive owns it**. Regulation and case law have made security a board-level and personally liable matter, yet boards park it in the audit committee with near-zero confidence, formal convergence has stalled near its 2019 baseline, and the dominant force reshaping security leadership in 2026 is artificial intelligence, not integration. The binding question is no longer how much to spend; it is **who owns the whole surface**, and the organizations and families that answer it with one accountable owner will convert the same budget into materially better protection.

KEY STATISTICS

24%
of organizations had converged physical and cyber security (2019 baseline; little moved since)[1, 2]

42% / 20%
share of security chiefs reporting to the CEO, two surveys disagree[4, 5]

$17.4M
average annual cost of insider risk per organization[23]

79%
of the S&P 500 park cyber-risk oversight in the audit committee[14]

~4%
of directors confident in their board's ability to oversee cyber and AI risk[15]

73%
of organizations hit by an intrusion affecting operational technology in 2024 (from 49%)[17]

63%
of family offices carry no cyber insurance; 31% have no incident-response plan[27]

first
a corporate security chief criminally convicted over a breach response (Uber, 2022)[13]

Scope & method. Open-source intelligence verified against allowlisted Tier 1 to 3 sources per AEIG source policy. Most prevalence figures in this field are drawn from vendor- or recruiter-commissioned surveys and are flagged as such; the absence of a current independent census of converged security leadership is itself a finding. The headline 24 percent convergence figure is a 2019 baseline and is dated explicitly. Legal and regulatory matters are cited to primary sources; criminal matters are noted with outcomes. Market-size estimates diverge across vendors and are presented as ranges. Timeliness: DURABLE, with the structural argument stable over six to eighteen months even as individual surveys refresh.

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 — Risk has converged into one surface but organizations have not: formal physical-cyber convergence sits near its 2019 baseline of about 24 percent even as 73 percent of organizations suffered an intrusion affecting operational technology in 2024. Technology is converging faster than ownership.[1, 2, 17]

2 High — Regulation and case law have made security a board-level and personal matter. The 2023 SEC rules force board-oversight disclosure and four-day incident reporting, and a security chief has been criminally convicted over a breach response.[10, 13]

3 Moderate — Yet boards are not equipped to own it. About 79 percent of the S&P 500 park cyber oversight in the audit committee, and only around 4 percent of directors express confidence in their board's ability to oversee cyber and AI risk.[14, 15]

4 Moderate — The security-leadership seat is rising toward the top of the house but the picture is contested: CISO-to-CEO reporting is climbing (42 percent on one survey, 20 percent on another) and pay nears $1 million, while AI, not convergence, is the dominant 2026 reshaping force.[4, 5, 6, 31]

5	High	The exposure is most concentrated and least owned in family offices: 43 percent suffered a cyberattack, 63 percent carry no cyber insurance, and only a minority have any formal risk leadership.[27, 28, 30]
6	High	The market is answering with a single-owner seat (the converged CSO or Chief Risk and Resilience Officer) and a fast-growing integrated-risk advisory industry, but adoption lags the threat and competes with AI for attention.[9, 24, 25, 26]

SECTION 01 · CONVERGENCE

One Surface, Many Owners

The risk has merged; the organization has not. Unified systems and shared dashboards are spreading, but a unified owner is not, and convergence stalls on structure rather than belief.

A cyber breach now triggers a physical shutdown, a social-engineering call defeats a technical control, an insider with a badge and a login is one person, and a geopolitical shift reprices them all at once. Yet the most-cited measure of organizational convergence has barely moved: an industry benchmark found only 24 percent of organizations had merged their physical and cybersecurity functions in 2019, and while a 2021 follow-up reported 60 percent partially or fully converged, that broader figure folds in business continuity and counts partial overlaps, so the clean physical-plus-cyber number remains low, and there has been no fresh institutional re-measurement since.[1, 2]

The functional pressure to converge is nonetheless rising. In a 2026 survey of more than 7,000 physical-security professionals, over 70 percent reported running unified or integrated security systems and described information-technology teams taking an increasingly prominent role in physical security, with 40 percent reporting more physical or cyber incidents, climbing to 68 percent at the largest organizations.[7] On the cyber side, 73 percent of organizations suffered an intrusion that affected operational technology in 2024, up from 49 percent a year earlier, as the boundary between the corporate network and the physical plant dissolved.[17]

The barrier is not belief; it is structure. The same research that documents convergence's benefits, with a large majority of converged organizations reporting it strengthened their security, also finds it stalls on budget silos, separate reporting lines, and the cultural distance between teams whose systems and standards evolved apart.[2, 31] The result is a single risk surface defended by separate departments that do not share a budget, a dashboard, or, crucially, an owner.

ASSESSMENT · HIGH CONFIDENCE

Risk has converged into one surface while accountability for it remains divided, and that mismatch, not any single threat, is the structural weakness. Integration is an organizational problem before it is a technical one: unified systems and shared dashboards are spreading, but a unified owner is not, and the benefit of convergence is captured only when one accountable seat spans physical, cyber, and the seams between them. The figure that matters is not spend but whether a single executive owns the combined surface.

Rationale: The stalled ~24 percent convergence baseline set against a 73 percent OT-intrusion rate and 70 percent unified-systems adoption shows technology converging ahead of ownership; the documented barriers are organizational, namely budget, reporting lines, and culture.

SECTION 02 · SEAM FAILURES

Where the Silos Break

The case for single ownership is written in the incidents that fell through the seams, where a threat begins in one domain and surfaces in another and no single-domain owner saw it whole.

The 2021 Colonial Pipeline attack breached only the corporate information-technology network through one stolen password, yet the operator shut down roughly 5,500 miles of fuel pipeline as a precaution, proving an IT compromise can force a physical, economy-scale consequence even when the operational systems are untouched.[18] US authorities now assess that a Chinese state actor has pre-positioned inside critical-infrastructure IT networks specifically to enable later disruption of operational systems, in some cases maintaining access for five years.[19]

The human seam is the most exploited. In 2023 attackers defeated the defenses of two major casino operators not with code but with a phone call to an IT help desk, and one reportedly paid roughly $15 million; US and allied agencies have since formally documented the group's method of researching employees and then voice-phishing the help desk to reset credentials.[21] Independent breach data confirms the pattern: about 60 percent of breaches in 2025 involved the human element and third-party involvement doubled to 30 percent, while the average annual cost of insider risk reached $17.4 million per organization, most of it from negligence and stolen credentials rather than malice.[20, 23]

The physical consequences are escalating. A 2025 ransomware attack halted vehicle production at Jaguar Land Rover for roughly six weeks and was assessed as the costliest cyber event in British history, with an economic impact near 1.9 billion pounds rippling across thousands of suppliers.[22] Each of these is a single event that crossed the cyber, physical, human, and third-party domains at once, precisely the kind of incident no single-domain function is structured to see whole.

ASSESSMENT · HIGH CONFIDENCE

The decisive evidence for integrated ownership is that the costliest recent failures are seam failures, incidents that begin in one domain and surface in another, where no single-domain owner held the whole picture. Confidence is high on the pattern and moderate only on the disputed dollar figures, several of which are vendor-sourced or macroeconomic estimates. The implication is that defending each domain to a high standard is insufficient if the interfaces between them are owned by no one; the marginal risk now lives at the seams.

Rationale: Colonial Pipeline and the Volt Typhoon advisory establish the IT-to-physical seam; the casino breaches and the Scattered Spider advisory establish the human seam; the breach and insider-cost data quantify it; Jaguar Land Rover shows the physical and financial scale; contested figures are flagged.

SECTION 03 · GOVERNANCE

Security Reached the Boardroom. The Board Is Not Ready.

Regulation and enforcement have raised the stakes of security governance without supplying the accountable owner the threat requires. Parking it in the audit committee satisfies the filing, not the risk.

Regulation has pushed security to the top of the house. The Securities and Exchange Commission's 2023 rules require public companies to disclose a material cybersecurity incident within four business days of determining it material and to describe, every year, how the board oversees cyber risk, converting security governance from an operational matter into a board-level disclosure obligation.[10]

Accountability also became personal, then partly retreated. In 2022 a federal jury convicted Uber's former security chief over his handling of a breach cover-up, the first criminal conviction of a corporate security executive for a breach response, a verdict upheld on appeal.[13] The Commission then charged the SolarWinds security chief individually with fraud in 2023, but a court dismissed most of the case in 2024 and the agency dropped the remainder with prejudice in 2025, leaving criminal exposure for concealment real while the civil individual-liability theory receded.[11, 12]

Yet the board that now owns security on paper is not equipped to own it in practice. Most large companies park cyber oversight in the audit committee, about 79 percent of the S&P 500, a body already loaded with financial-reporting duties, while only around 4 percent of directors expressed confidence in their board's ability to oversee cyber and artificial-intelligence risk.[14, 15] Board engagement has risen sharply since the rules, with a large majority now discussing the financial implications of cyber incidents, but the expertise gap and the absence of a clear single owner persist.[16]

ASSESSMENT · MODERATE CONFIDENCE

Security is now a board and personal-liability matter, but the board lacks both the expertise and the structure to own it, and the personal-liability signal has proved sharper for criminal concealment than for civil disclosure judgment. Disclosure obligations and enforcement have raised the stakes of getting governance right without supplying the accountable owner the threat requires; parking it in the audit committee satisfies the filing, not the risk. The governance gap is an ownership gap wearing a compliance label.

Rationale: The SEC rules and the Uber conviction establish elevated stakes; the SolarWinds arc shows the limits of civil individual liability; the 79 percent audit-committee concentration and ~4 percent director confidence show the board is neither structured nor equipped to own the surface.

SECTION 04 · OWNERSHIP

The Search for a Single Owner

The market is converging on an answer, a single senior owner of the combined surface, built in as a role or bought in as a service, even as artificial intelligence competes for the same attention.

The converged Chief Security Officer is now a surveyable population: a 2025 global study reached more than 2,300 of them, though even there 80 percent said their leadership remained more concerned with cyber than physical security, evidence the mandate is real but still tilted.[3] Cyber leadership is also climbing toward the chief executive, with one 2025 survey finding 42 percent of security chiefs now report to the CEO, three times the prior year, though a broader survey put the figure nearer 20 percent, and senior security pay now approaches one million dollars.[4, 5, 6]

Importantly, the role is expanding rather than fragmenting. Analysts frame the trajectory as the security leader growing into an enterprise-risk owner who leads with business judgment, supported by deputies in the business units rather than replaced, and a parallel Chief Risk and Resilience Officer is emerging to own integrated enterprise risk end to end.[8, 9] The honest counter-current is that the single biggest force reshaping security leadership in 2026 is artificial intelligence, not physical-cyber convergence, competing for the same attention and budget.[31]

Where firms cannot build the seat, they are buying it. An integrated-risk advisory and managed-services industry is consolidating physical, cyber, and intelligence under one roof, evidenced by a roughly fourteen-billion-dollar take-private of one global protective-services group and the assembly of enterprise-risk retainers by major advisory firms, with advisory and consulting sub-segments growing at double-digit rates, far faster than the guarding business they sit above.[24, 25, 26] The market

is pricing single ownership of integrated risk as a service before most organizations have built it as a role.

ASSESSMENT · HIGH CONFIDENCE

The market is answering the ownership question with a new seat, the converged Chief Security Officer or Chief Risk and Resilience Officer, and a fast-growing advisory industry that rents the function, but adoption lags the threat and competes with artificial intelligence for executive attention. The next unit of protection value comes from consolidating accountability, not from another tool, and the organizations that either build the single owner or buy it through an integrated retainer will outperform those still defending a converged surface with divided departments.

Rationale: The surveyed CSO population and the rising CEO-reporting trend show the seat forming; the Chief Risk and Resilience Officer and analyst framing show expansion rather than fragmentation; the advisory consolidation and double-digit growth show the buy-side answer; the AI counter-current is flagged.

SECTION 05 · FAMILY OFFICE

Where the Gap Is Widest

Maximum concentration of exposure, minimum integration of ownership. For a principal, consolidating who owns the whole surface is the single highest-return security decision available.

Nowhere is the exposure more concentrated or the ownership thinner than in the family office. These lightly governed entities hold a principal's wealth, data, household, and staff in one place, precisely the profile every preceding threat exploits, yet 43 percent reported a cyberattack, rising to 57 percent in North America, while 63 percent carried no cyber insurance, 31 percent had no incident-response plan, and only about a third maintained a dedicated cybersecurity budget.[27]

The structures to own the risk are largely absent. Roughly 40 percent of single family offices report having cybersecurity controls in place, most outsource cyber rather than build it, and only a minority of even the largest offices have any formal risk or compliance leadership, a share that has risen but from a low base.[28, 30] Surveyed offices themselves admit to being underprepared across cyber, personal, and geopolitical risk together, and the prevailing model keeps oversight in the family's hands while pushing execution to outside vendors.[29]

The advice converging across the field is to consolidate. Practitioners increasingly recommend an embedded Chief Risk or Resilience Officer, or a fractional equivalent, who owns the combined physical, cyber, privacy, and reputational surface, on the argument that family-office risk failures are governance

failures rather than technology ones.[30] That is the same conclusion the enterprise data reaches from the other direction: the binding constraint is ownership, and the family office is where assigning one accountable owner would close the widest gap.

ASSESSMENT · HIGH CONFIDENCE

The family office is the sharpest case of the whole thesis: maximum concentration of exposure, minimum integration of ownership. For a principal the decisive question is not whether each domain is covered but whether one accountable owner, built in or retained, holds the physical, cyber, privacy, and reputational surface as a single mandate, because today, in most family offices, no one does. Consolidating that ownership is the single highest-return security decision available to a wealthy principal.

Rationale: The Deloitte, UBS, Citi, and Simple data establish concentrated exposure and absent structure; the convergence of practitioner advice toward an embedded or fractional single owner matches the enterprise conclusion that risk failures are governance failures.

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 · Spend rises, ownership stays split

CONSTRUCTION CONFIDENCE: HIGH · VELOCITY: GRADUAL

Formal convergence stays near its baseline; boards keep cyber in the audit committee; security-chief reporting climbs slowly toward the CEO; artificial intelligence absorbs the reform energy and budget. Family offices remain under-built, and the integrated-risk advisory market grows as firms rent the function they have not built. The surface stays divided and the seam risk persists even as total security spend rises.

SIGNAL TO WATCH: ANOTHER YEAR OF FLAT CONVERGENCE PREVALENCE AGAINST RISING OPERATIONAL-TECHNOLOGY AND SEAM INCIDENTS; NO FRESH INDEPENDENT RE-MEASUREMENT OF CONVERGED-ROLE ADOPTION

Deterioration · A seam event with personal accountability

CONSTRUCTION CONFIDENCE: MODERATE · VELOCITY: RAPID

A converged-seam incident, a cyber breach producing physical harm, or an insider-plus-access failure, hits a major company or a prominent family, and a security leader or director faces personal liability or public accountability. Boards scramble to assign ownership; demand for integrated leadership and for advisory retainers spikes faster than the talent pool can supply, and insurers reprice around governance maturity.

SIGNAL TO WATCH: A HIGH-PROFILE SEAM INCIDENT WITH NAMED INDIVIDUAL ACCOUNTABILITY; A BOARD-LEVEL RESHUFFLE THAT CREATES A COMBINED RISK SEAT UNDER DURESS

Stabilization · Single ownership normalizes

CONSTRUCTION CONFIDENCE: LOW-MOD · VELOCITY: STRUCTURAL

The converged Chief Security Officer or Chief Risk and Resilience Officer becomes standard, boards stand up dedicated risk committees with real expertise, integrated-risk retainers become a normal purchase, and family offices adopt embedded or fractional owners. The surface gains an owner and the seam risk falls as accountability finally tracks the threat.

SIGNAL TO WATCH: A MEASURABLE RISE IN CONVERGED-ROLE ADOPTION AND DEDICATED BOARD RISK COMMITTEES; FAMILY-OFFICE SURVEYS SHOWING MAJORITY FORMAL RISK LEADERSHIP

ASSESSMENT · MODERATE CONFIDENCE

Across all three paths the surface stays converged; the variable is whether ownership converges with it. Baseline, rising spend against divided ownership, is the most probable path; Deterioration is the fast risk that a single seam event with personal accountability would trigger; Stabilization is the slow structural fix that depends on organizational change and, for families, on a decision to assign one owner. The planning constant is that the binding constraint is accountability, not budget, and the return on consolidating it is highest exactly where it is least present.

Rationale: The stalled convergence baseline, the elevated-but-unequipped board, the contested leadership picture, and the family-office gap jointly make divided ownership the default and consolidation the decisive, lagging variable.

SOURCE REGISTRY

1. ASIS Foundation, "The State of Security Convergence in the United States, Europe, and India," 2019.
2. ASIS Foundation, "Security Convergence and Business Continuity: Reflecting on the Pandemic Experience," 2022.

3. Allied Universal / G4S, "World Security Report 2025," 2025.
4. Heidrick & Struggles, "2025 Global Chief Information Security Officer Compensation Survey," 2026.
5. Deloitte, "Global Future of Cyber Survey," 2024.
6. IANS Research & Artico Search, "CISO Compensation Benchmark," 2025.
7. Genetec, "2026 State of Physical Security Report," 2025.
8. Gartner / Forrester, "Trends for Security and Risk Leaders; the BISO role," 2025.
9. World Economic Forum / PwC, "Chief Risk Officers Community; the Chief Risk and Resilience Officer," 2025.
10. U.S. Securities and Exchange Commission, "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (final rule)," 2023.
11. Sullivan & Cromwell / Harvard Law School Forum on Corporate Governance, "Court Dismisses Most of SEC's Claims Against SolarWinds," 2024.
12. Jones Day / U.S. Securities and Exchange Commission, "SEC Dismisses Remaining SolarWinds Claims," 2025.
13. U.S. Department of Justice (N.D. Cal.), "Former Chief Security Officer of Uber Convicted for Covering Up Data Breach," 2022.
14. Zscaler, "An Analysis of Board-Level Cybersecurity Risk Oversight," 2026.
15. PwC, "2024 Annual Corporate Directors Survey," 2024.
16. National Association of Corporate Directors (NACD), "2024 Director Survey," 2024.
17. Fortinet, "2024 Global State of Operational Technology and Cybersecurity Report," 2024.
18. U.S. Department of Energy (CESER), "Colonial Pipeline Cyber Incident," 2021.
19. CISA / NSA / FBI, "PRC State-Sponsored Actors (Volt Typhoon) Advisory AA24-038A," 2024.
20. Verizon, "2025 Data Breach Investigations Report," 2025.
21. CISA and partners, "Scattered Spider advisory; MGM and Caesars breaches," 2025.
22. Cyber Monitoring Centre / Cybersecurity Dive, "Jaguar Land Rover cyber incident economic-impact assessment," 2025.
23. DTEX Systems / Ponemon Institute, "2025 Cost of Insider Risks Global Report," 2025.
24. Kroll, "Enterprise Security Risk Management and Enterprise Risk Retainer," 2025.
25. GardaWorld / Crisis24, "Take-private transaction (~C$14B)," 2025.
26. Mordor Intelligence / Kings Research, "Security services and risk-advisory market sizing," 2026.
27. Deloitte Private, "The Family Office Cybersecurity Report 2024," 2024.
28. UBS, "Global Family Office Report 2025," 2025.
29. Citi Wealth, "2025 Global Family Office Report," 2025.
30. Simple (andsimple.co), "Family Office Security & Risk Report 2025," 2025.
31. Security Industry Association, "Security Convergence 2024; 2026 Security Megatrends," 2026.

AEGEAN INTELLIGENCE GROUP

Publishable Market Research

Timeliness: DURABLE. The structural argument here, a converged risk surface defended by divided ownership, is durable on a six-to-eighteen-month horizon. The supporting figures refresh on the cadence of annual security-leadership, board-governance, and family-office surveys, and the legal frame moves with SEC enforcement and case law. An Update Addendum will follow on a material change in any of these.

Classification: PUBLIC. Prepared on open-source intelligence verified against allowlisted sources. Survey figures are attributed to their publishers and flagged where vendor-commissioned; legal and regulatory matters are cited to primary sources; analytic judgments are Aegean's.

contact@aegeanintel.com · aegeanintel.com