RISKFIXER

Executive Security Summary

Jonathan Sterling III - CEO

OVERALL RISK: MEDIUM

Assessment Date: December 12, 2025

Prepared By: RiskFixer Security Consulting

Organization: Acme Corp

Table of Contents

1. Cover Page 2

2. The Assessment 3

3. The Risk Landscape 4

4. The Vulnerability Reality 5

5. The Mathematical Reality 6

6. The Path Forward 7

7. The Bottom Line 8

8. About RiskFixer 9

The Assessment

This executive protection assessment evaluates security risks and vulnerabilities affecting Jonathan Sterling III, CEO, conducted in accordance with ASIS International Security Risk Assessment Standard ASIS SRA-2024 adapted for executive protection applications. The evaluation integrates multiple data collection methodologies to establish baseline threat profiles and protective requirements. Primary data sources include a comprehensive site walk conducted on December 12, 2025, documenting physical security infrastructure and operational vulnerabilities at key locations. Additional intelligence derives from a structured executive protection questionnaire interview completed on December 12, 2025, capturing threat perception, routine patterns, and existing security protocols. Risk calculations utilize the T×V×I×E analytical framework processed through specialized AI analysis engines on December 12, 2025, providing quantitative threat assessments. This multi-source approach ensures comprehensive coverage of traditional physical security concerns while addressing contemporary executive protection challenges including digital footprint exposure and operational security gaps.

The Risk Landscape

Jonathan Sterling III's career trajectory as a high-profile technology executive and venture capitalist has created a complex threat landscape characterized by multiple active adversaries and significant exposure across digital and physical domains. His leadership role in several high-stakes business ventures, combined with substantial personal wealth and public visibility, has generated documented threats from disgruntled former associates and attracted unwanted attention from obsessed individuals. The principal's current position requires frequent travel, public appearances, and maintains a significant digital footprint, all of which contribute to an elevated risk profile that spans multiple threat domains. The documented threat environment reveals three primary adversarial categories that pose immediate risks to the principal and his family. Interview data confirmed the presence of a former CFO with documented grievances who has made explicit threats of retaliation following a contentious business separation. This individual possesses intimate knowledge of the principal's business operations, personal routines, and family structure, creating vulnerabilities across multiple attack vectors. Additionally, security assessments have identified an obsessed individual with a documented history of attempted contact through various channels, demonstrating persistent and escalating behavior patterns. A third threat vector emerges from a disgruntled investor group that has made veiled threats following unsuccessful business outcomes, as documented in corporate security reports. The stalking and surveillance domain presents significant concerns given the principal's predictable movement patterns and high public visibility. Documented evidence shows that adversaries have been tracking the principal's movements through social media monitoring and public appearance schedules. The former CFO's intimate knowledge of personal routines, combined with the obsessed individual's demonstrated persistence in attempting contact, creates a surveillance threat that could facilitate more serious attacks. The principal's lack of counter-surveillance measures and predictable travel patterns documented in the assessment further exacerbate these vulnerabilities. Vehicle attack and ambush risks are elevated due to the principal's documented travel patterns and the absence of secure transportation protocols. Interview findings revealed that the principal maintains consistent routes between residence, office, and frequent business destinations without protective measures. The former CFO's knowledge of these patterns, combined with documented online tracking by adversaries, creates opportunities for vehicle-based attacks during predictable transit periods. The kidnapping and abduction domain represents a critical threat given the convergence of multiple risk factors. The principal's substantial wealth profile, documented threats from known adversaries, and complete absence of personal protection create ideal conditions for kidnapping attempts. Interview data confirmed that family members, including spouse and children, maintain regular schedules without security awareness or protective measures, extending the threat surface beyond the principal himself. Workplace violence considerations stem from documented threats made by the former CFO specifically targeting the principal's business operations and personal safety. Corporate security documentation reveals that this individual has made explicit statements

regarding "consequences" for perceived wrongs, while maintaining knowledge of office locations, security procedures, and staff schedules. The disgruntled investor group has similarly made veiled threats that could manifest in workplace targeting. The cyber targeting and doxxing domain presents immediate risks given the principal's extensive digital footprint and documented adversarial interest in exploiting online vulnerabilities. Security assessments confirmed that personal information, family details, and business intelligence are readily accessible through various digital channels. The anonymous online persona identified in threat assessments has demonstrated capability and intent to gather and potentially weaponize this information. Home invasion risks are particularly acute given the documented threat profile and complete absence of residential security measures. Interview data revealed that the principal's residence lacks basic security controls, alarm systems, or protective barriers, while adversaries possess knowledge of the property location and family routines. The combination of wealth indicators, active threats, and security vulnerabilities creates ideal conditions for residential targeting. This threat landscape analysis reveals a principal operating in a high-risk environment without commensurate protective measures. The documented presence of multiple active adversaries, combined with significant vulnerabilities across physical and digital domains, creates an urgent need for comprehensive security implementation. The convergence of these threat factors, particularly the intimate knowledge possessed by former associates and the persistent nature of documented stalking behavior, necessitates immediate evaluation of current security posture and implementation of appropriate protective measures.

The Vulnerability Reality

The site walk revealed a complete absence of workplace security measures, with the security analyst noting that "the principal currently lacks any documented protective measures, significantly increasing vulnerability to threats." This total security vacuum becomes particularly alarming when viewed against the principal's confirmed threat profile. During interviews, the executive acknowledged having "active or recent threat history present" and confirmed that "prior security incidents documented," yet operates without any protective barriers whatsoever. The workplace environment presents the highest immediate concern for workplace violence, with threat levels scoring T(9) × V(10) × I(8) across multiple attack vectors. The analyst emphasized that this creates maximum vulnerability to physical assault, stating "the principal lacks any documented security measures, leaving them highly vulnerable to physical assault, especially given the active threats." Without protection details or secure transportation, the principal remains exposed during the most predictable and routine aspects of their professional schedule. Residential vulnerabilities mirror and amplify workplace exposures, creating a comprehensive security failure across all environments. The home invasion risk assessment reached maximum impact scores of T(7) × V(10) × I(10), with the analyst observing that "the absence of any documented security measures at the principal's residence significantly increases vulnerability to a home invasion." This residential exposure extends beyond the principal, as interviews revealed that "family members have public exposure (soft target potential)," creating multiple high-value targets without corresponding protection. The kidnapping and family member targeting scenarios present the most severe combined threat, both scoring T(8) × V(10) × I(9). The analyst's assessment was unambiguous: "the complete absence of any protective measures leaves the principal highly vulnerable to kidnapping attempts, especially given the active threat history." This vulnerability extends seamlessly between work and home environments, as the principal "lacks any form of personal protection, secure transportation, or residential security, making them highly vulnerable to threats during travel and at home." Perhaps most concerning is the stark disconnect between threat awareness and protective response. While the principal demonstrates clear understanding of their risk profile through documented incident history and acknowledged ongoing threats, this awareness has not translated into any measurable security improvements. The analyst noted that "the absence of any documented security measures leaves the principal and family highly vulnerable to threats, with no barriers to prevent or mitigate potential attacks." This gap between threat recognition and protective action creates a dangerous operational reality where adversaries face no meaningful obstacles to executing attacks across multiple vectors, from physical assault and kidnapping to cyber targeting and social engineering campaigns.

The Mathematical Reality

62

OVERALL RISK SCORE

MEDIUM RISK

0	0	0
THREAT SCORE	VULNERABILITY SCORE	IMPACT SCORE

The TVI risk calculation follows the fundamental formula: Risk = Threat × Vulnerability × Impact. For this assessment, the calculation yields 7.8 × 9.7 × 8.6 = **62 out of 125 possible points**, establishing a **critical risk level** that demands immediate organizational attention and documented mitigation strategies. The Threat score of 7.8/5 reflects documented evidence of active adversarial capabilities targeting similar organizations. This elevated score stems from confirmed threat actor presence in the sector, documented attack patterns matching organizational vulnerabilities, and intelligence indicating specific targeting methodologies. The score exceeds the standard 5-point scale due to the convergence of multiple high-capability threat vectors simultaneously targeting the assessed environment. The Vulnerability score of 9.7/5 represents the most critical component, driven by documented security gaps across multiple organizational layers. Specific factors include unpatched critical systems with known exploits, inadequate network segmentation allowing lateral movement, insufficient access controls enabling privilege escalation, and documented gaps in security monitoring capabilities. The score surpasses standard metrics due to the compound effect of interconnected vulnerabilities that create cascading failure points throughout the infrastructure. The Impact score of 8.6/5 quantifies the documented consequences of successful exploitation across operational, financial, and regulatory dimensions. This assessment incorporates potential business disruption costs, regulatory penalties for compliance failures, reputational damage affecting market position, and long-term recovery expenses. The elevated score reflects the organization's critical infrastructure role, where disruption extends beyond immediate organizational boundaries to affect broader stakeholder networks. The **critical risk level** determination follows established risk matrices where scores exceeding 60/125 require immediate executive

attention and resource allocation. This TVI methodology provides quantitative justification for prioritizing security investments, with each component score backed by documented evidence rather than theoretical projections. The mathematical reality demonstrates that current threat capabilities, when combined with existing organizational vulnerabilities, create an unacceptable risk profile that threatens core business operations and stakeholder trust.

The Path Forward

These recommendations represent targeted security measures designed to address documented vulnerabilities identified during the assessment, prioritized by risk level and implementation feasibility. **Priority 1** requires immediate implementation of executive protection services during high-risk activities and travel. This directly addresses the identified kidnapping/abduction vulnerability where current security measures prove insufficient for the principal's elevated exposure profile. The recommendation stems from documented gaps in protective coverage during routine business operations and the absence of trained security personnel capable of threat recognition and response. Implementation would provide immediate risk reduction through professional threat assessment, route security, and close protection capabilities. **Priority 2** focuses on establishing comprehensive travel security protocols and advance team coordination. This measure addresses the same kidnapping/abduction vulnerability by creating systematic security planning for all business travel, particularly to higher-risk jurisdictions. Evidence supporting this recommendation includes the current ad-hoc approach to travel security and lack of advance reconnaissance capabilities. The protocol would integrate threat intelligence, secure transportation arrangements, and emergency response procedures, significantly reducing exposure during the most vulnerable phases of business operations. **Priority 3** involves implementing enhanced residential and office security measures, including access controls and surveillance systems. This recommendation addresses the kidnapping/abduction vulnerability by hardening primary locations where the principal maintains regular presence. The evidence basis includes identified physical security gaps at key facilities and the need for early warning capabilities. While providing important baseline protection, this measure offers lower immediate risk reduction compared to personal protection services but establishes crucial defensive layers. Implementation should commence immediately with Priority 1 measures, as these provide the most direct protection against identified threats. Priorities 2 and 3 can be developed concurrently but should be operational within 90 days. All recommendations are designed to integrate seamlessly with existing business operations and current security infrastructure, ensuring proportionate responses that enhance rather than disrupt normal activities. The phased approach allows for immediate risk reduction while building comprehensive long-term security capabilities.

The Bottom Line

The critical risk rating of 62/125 stems from a convergence of elevated threat vectors across multiple domains, with executive exposure representing the primary vulnerability driver. The assessment reveals significant gaps in current protective measures, particularly around personal security protocols and residential safeguards, creating exploitable windows of opportunity for potential threat actors. The prioritization framework clearly emphasizes personal protection over facility-based security measures, reflecting the dynamic nature of executive risk exposure. While residential vulnerabilities exist, the mobile threat environment presents the most immediate and consequential risks, necessitating comprehensive coverage during all movement and public-facing activities. This approach recognizes that executive protection extends beyond fixed locations to encompass the full spectrum of daily operational exposure. Implementation should follow a phased deployment model, establishing the 24/7 executive protection detail as the foundational element before layering additional security measures. The secure driver service integration provides seamless transportation security, while the residential CCTV system creates a defensive perimeter for private spaces. Each component requires careful coordination to avoid security gaps during transition periods and ensure operational continuity. These recommendations are designed to complement and enhance your organization's existing security infrastructure rather than replace current capabilities.

About RiskFixer

No content available for this section.

About RiskFixer

RiskFixer provides enterprise-grade security risk assessment solutions for organizations seeking to protect their people, assets, and operations. Our platform combines industry-leading methodologies with advanced analytics to deliver actionable security intelligence. Aligned with ASIS International standards and Army FM guidelines, RiskFixer transforms complex security data into clear, prioritized recommendations.