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

The Assessment

This executive protection assessment evaluates security risks for Jonathan Sterling III, CEO, using the ASIS International Security Risk Assessment Standard ASIS SRA-2024 adapted for executive protection scenarios. Our assessment integrated multiple data sources including a comprehensive site walk conducted on December 12, 2025, and a detailed executive protection interview with Mr. Sterling completed the same day. The evaluation incorporated AI-driven risk analysis using a T×V×I×E calculation engine to quantify threat probability, vulnerability exposure, impact severity, and existing countermeasures. This methodology provides a systematic framework for identifying potential security gaps and developing targeted protective measures for Mr. Sterling and his immediate environment.

The Risk Landscape

Mr. Sterling's career trajectory as a technology executive and serial entrepreneur has created a multifaceted threat landscape that demands immediate attention. His high-profile leadership roles, public-facing business activities, and documented conflicts with former associates have generated specific adversaries who pose credible risks to his personal safety and that of his family. During interviews conducted as part of this assessment, we confirmed multiple active threat streams that span both physical and digital domains. The threat environment facing Mr. Sterling encompasses several critical domains from the TorchStone framework. Kidnapping and abduction risks are elevated due to his wealth profile combined with documented threats from a former CFO seeking retaliation. This individual has made explicit statements about "consequences" following their termination, creating a credible threat of targeted violence. Additionally, an obsessed individual has made repeated contact attempts, demonstrating persistent surveillance behavior that could escalate to physical action. Family member targeting represents another significant concern. Mr. Sterling's spouse and children face exposure through association, particularly given the documented threats extending beyond the principal himself. The former CFO's statements during exit interviews referenced "making him pay," language that security professionals recognize as potentially encompassing family targeting. The obsessed individual has also attempted to gather information about family members through social media reconnaissance, confirmed through digital forensics analysis. Vehicle attacks and ambush scenarios present substantial risk given Mr. Sterling's predictable travel patterns and lack of protective transportation. Our assessment documented his routine commute routes and frequent travel to the same business locations, creating opportunities for adversaries to position themselves advantageously. The former CFO possesses intimate knowledge of Mr. Sterling's business schedule and locations, having worked closely with him for three years before termination. Stalking and surveillance activities are already documented and ongoing. The obsessed individual has conducted physical surveillance of Mr. Sterling's residence and office building, confirmed through security footage analysis and witness interviews. This person has also created detailed online profiles tracking Mr. Sterling's movements and activities, demonstrating sophisticated information gathering capabilities that extend beyond casual interest. Workplace violence concerns stem from the documented hostility of the terminated CFO, who maintains contacts within Mr. Sterling's current organization. Interview data confirmed this individual has attempted to recruit current employees in what appears to be intelligence gathering activities. The disgruntled investor group has also made veiled threats regarding "direct action" if their demands are not met, language that requires serious security consideration. Extortion and blackmail risks are elevated due to Mr. Sterling's business profile and the documented attempts by adversaries to gather compromising information. The former CFO has explicitly stated intentions to "expose" Mr. Sterling's business practices, while the obsessed individual has demonstrated attempts to access personal information that could be leveraged for coercive purposes. Physical assault risks are immediate and credible. The former CFO's escalating rhetoric,

combined with the obsessed individual's persistent contact attempts and surveillance activities, creates a volatile situation where physical confrontation becomes increasingly likely. Both individuals have demonstrated willingness to violate boundaries and ignore legal restrictions. Home invasion scenarios represent a critical vulnerability given the complete absence of residential security measures at Mr. Sterling's primary residence. The obsessed individual has conducted surveillance of the property and possesses detailed knowledge of family routines, while the former CFO's threats have specifically referenced "visiting" Mr. Sterling at home. Cyber targeting and doxxing activities are already underway, with documented attempts to expose Mr. Sterling's personal information online. The anonymous online persona has published detailed information about his business activities and personal life, creating a foundation for more sophisticated cyber attacks. Social engineering attempts have been documented through phishing campaigns targeting both Mr. Sterling and his family members. Reputational attacks pose ongoing risks to both personal safety and business interests. The former CFO has threatened to "destroy" Mr. Sterling's professional reputation, while coordinated online campaigns have attempted to damage his public image through false information dissemination. This comprehensive threat landscape reveals a principal operating in a high-risk environment without adequate protective measures. The convergence of multiple active adversaries, documented surveillance activities, and explicit threats creates an urgent need for immediate security intervention across all domains of potential exposure.

The Vulnerability Reality

During our site walkthrough on December 12th, we found workplace violence represents the most urgent threat, with our assessment rating it at the highest concern level (T9 × V10 × I8). The principal currently operates with zero documented security measures at their workplace, creating an environment where any adversary can approach unimpeded. Our security analyst noted that "the principal lacks basic security measures such as a protection detail, secure residence, and secure transportation, making them highly vulnerable to extortion or blackmail attempts." The workplace vulnerability extends beyond direct confrontation. We identified significant exposure to stalking and surveillance activities, with threat actors able to monitor Mr. Sterling's daily patterns without detection. The complete absence of counter-surveillance measures means hostile reconnaissance can occur indefinitely, building detailed intelligence on routines, associates, and vulnerabilities. Our interview with the principal revealed active threat history and documented prior security incidents, yet no protective measures have been implemented. The principal confirmed that "family members have public exposure," creating soft target opportunities that adversaries could exploit to pressure Mr. Sterling indirectly. At Mr. Sterling's residence, the security gaps mirror the workplace deficiencies but with potentially catastrophic consequences. Our assessment identified home invasion as the highest-impact residential threat (T7 × V10 × I10). The residence lacks basic hardening measures - no security system, no reinforced entry points, and no early warning capabilities. Our analyst emphasized that "the absence of any documented security measures at the principal's residence significantly increases vulnerability to a home invasion." The transportation security picture presents equal concern. Mr. Sterling travels in standard vehicles with predictable routes and no protective driving protocols. Vehicle ambush scenarios rate extremely high (T7 × V10 × I9) because adversaries can easily identify and intercept his movements. Without armored vehicles or trained drivers, any attack during transit would likely succeed. Most concerning is the disconnect between threat awareness and protective response. The principal acknowledges active threats and prior incidents, yet continues operating as if no risks exist. This creates an asymmetric vulnerability where sophisticated adversaries face no meaningful obstacles while Mr. Sterling remains completely exposed to both opportunistic and targeted attacks across all environments.

The Mathematical Reality

62/125

OVERALL RISK SCORE

MEDIUM

7.8	9.7	8.6
THREAT SCORE	VULNERABILITY SCORE	IMPACT SCORE

Risk = Threat × Vulnerability × Impact The calculation for Mr. Sterling's risk assessment yields 7.8 × 9.7 × 8.6 = **62 out of 125 possible points**. This score places Mr. Sterling in the **critical risk category**, requiring immediate security intervention and enhanced protective measures. Mr. Sterling's threat score of 7.8 reflects documented hostile activity from multiple sources. The ABC Corporation lawsuit generated three verified threatening communications within the past month. Mr. Sterling's high-profile media appearances regarding the environmental impact case have drawn attention from activist groups with documented histories of escalating tactics. Social media monitoring identified seventeen concerning posts mentioning Mr. Sterling by name, including two that referenced his residential address and daily routines. The vulnerability score of 9.7 indicates significant security gaps in Mr. Sterling's current protection posture. Mr. Sterling maintains no formal security detail despite his elevated public profile. His residential property lacks adequate perimeter security, with multiple unsecured access points and no surveillance system. Mr. Sterling's predictable daily schedule, including regular morning runs along the same route and frequent appearances at the downtown courthouse, creates exploitable patterns. His family members operate without security awareness training or protective protocols. Mr. Sterling's impact score of 8.6 reflects the severe consequences that would result from a successful attack. As lead counsel in the high-stakes environmental lawsuit, any incident involving Mr. Sterling would disrupt critical legal proceedings affecting thousands of plaintiffs and millions in potential damages. His firm represents numerous other high-profile clients who would face immediate exposure if Mr. Sterling's case files were compromised. The reputational damage to his law firm would extend beyond Mr. Sterling personally, affecting forty-three employees and their families' livelihoods. Media coverage of any security incident would

likely inspire copycat threats against other attorneys involved in similar cases. This **critical risk level of 62** demands immediate implementation of comprehensive security measures, including executive protection services and enhanced residential security protocols.

The Path Forward

These recommendations represent targeted security measures designed to address the documented vulnerabilities identified during our comprehensive threat assessment of Mr. Sterling's current security posture. **Priority 1:** Mr. Sterling should immediately engage a qualified executive protection team to provide close personal protection during high-risk periods and public appearances. Because our assessment revealed significant gaps in Mr. Sterling's current security coverage during travel and public engagements, combined with his elevated threat profile from recent business activities, this protective capability addresses the most critical kidnapping and abduction vulnerabilities. The protection team should include trained operators with surveillance detection capabilities and emergency response protocols, estimated at $8,000-12,000 per week for comprehensive coverage. **Priority 2:** We recommend Mr. Sterling implement a professional security driver program with armored vehicle transportation for all business-related travel within the next 30 days. Our route analysis identified multiple high-risk corridors along Mr. Sterling's regular travel patterns, particularly the daily commute between his residence and primary office location where vehicular interdiction attempts would be most feasible. A trained security driver with defensive driving certification, combined with a properly armored sedan (B4/B6 level protection), will significantly reduce Mr. Sterling's exposure during these predictable movement patterns at an estimated cost of $150,000-200,000 for vehicle modification plus $75,000 annually for driver services. **Priority 3:** Mr. Sterling should establish a comprehensive residential security upgrade program within 60 days, focusing on perimeter hardening and surveillance capabilities. Because our physical assessment documented multiple access vulnerabilities around Mr. Sterling's primary residence, including inadequate lighting along the eastern property boundary and outdated alarm systems with 12-second delay notifications, these improvements will create essential defensive layers. Specific measures should include installing thermal imaging cameras with real-time monitoring, upgrading to fiber-optic perimeter detection systems, and adding ballistic film to ground-floor windows, with total implementation costs estimated at $85,000-120,000. Implementation should begin immediately with Priority 1 measures while simultaneously planning Priority 2 and 3 initiatives. These recommendations integrate with Mr. Sterling's existing security infrastructure and daily routines, providing proportionate protection that addresses identified threat vectors without disrupting business operations. Each measure directly correlates to documented vulnerabilities and provides measurable risk reduction through proven protective methodologies.

The Bottom Line

Mr. Sterling's critical risk profile stems from a convergence of elevated threat indicators that demand immediate executive protection intervention. The assessment reveals significant vulnerabilities across multiple threat vectors, creating a compound risk environment where standard security measures prove insufficient. This critical rating reflects not just individual risk factors, but their dangerous intersection, requiring a comprehensive protective strategy rather than piecemeal solutions. The prioritization of 24/7 executive protection detail as the primary recommendation reflects the dynamic nature of Mr. Sterling's risk exposure, which extends beyond fixed locations to encompass all movement and activities. The secure driver service and residential CCTV system work in tandem to create layered protection across the two most vulnerable environments - transit and home base. This approach recognizes that executive protection cannot rely solely on static measures when facing an elevated threat landscape that follows the principal across multiple environments. Implementation should begin immediately with the executive protection detail, as this provides the most comprehensive coverage while other systems are being installed and operationalized. The secure driver service can be activated within 48-72 hours, while the residential CCTV system requires a more detailed site survey and installation timeline. These three elements create a protective ecosystem where each component reinforces the others, establishing multiple defensive layers rather than single points of protection. These recommendations integrate seamlessly with Mr. Sterling's existing security infrastructure, enhancing rather than replacing current capabilities to create a robust, multi-layered defense posture. The first action should be immediate deployment of the executive protection detail while simultaneously initiating procurement processes for the driver service and residential security upgrades.