



PROPERTY VULNERABILITY INTELLIGENCE™

CONFIDENTIAL

PROFESSIONAL ASSESSMENT™

SUBJECT PROPERTY

Commercial Property — Sample Asset

ASSESSOR

Vyken Systems™, LLC

REPORT DATE

June 2026

ASSESSMENT TIER

Professional Assessment™

CLIENT

Sample Client

REPORT STATUS

SAMPLE REPORT

OVERALL PROPERTY VULNERABILITY SCORE



CPTED Environmental Assessment



72

CARVER Asset Protection Matrix™



75

Threat Exposure Analysis



76

SAMPLE — FOR ILLUSTRATIVE PURPOSES ONLY

Executive Intelligence Summary

Scope of Assessment

This Professional Assessment™ was conducted by Vyken Systems™, LLC at the request of the named client and covers the subject commercial property in full. The assessment encompassed a comprehensive physical security survey, environmental design evaluation, and structured asset criticality analysis. Site visits were conducted during both standard operational hours and a separate after-hours perimeter survey to capture vulnerability conditions across the full operational cycle. All findings, scores, and recommendations contained herein are based on direct observation, environmental data collection, and analytical framework application by a certified Vyken assessor.

Overall Assessment Findings

The subject property has been assigned an overall Property Vulnerability Index™ score of 74 out of 100, placing it in the HIGH EXPOSURE band. This designation indicates the presence of multiple material security deficiencies that, in combination, create a vulnerability profile substantially above the baseline for comparable commercial properties. The composite score reflects significant exposure across all three evaluated frameworks: the property scored 72/100 under the CPTED Environmental Assessment, 75/100 under the CARVER Asset Protection Matrix™, and 76/100 under the Threat Exposure Analysis. No single deficiency is solely responsible for this profile; the elevated score reflects the compounding effect of multiple concurrent gaps.

Critical Intelligence Takeaway

The most consequential findings center on two interrelated deficiencies: inadequate perimeter lighting across the north and west elevations, and the absence of commercial-grade access control on secondary entry points. These two conditions, taken together, create an after-hours vulnerability window during which a motivated actor could approach the property boundary under low-visibility conditions, exploit uncontrolled secondary access, and penetrate interior zones without triggering any surveillance or alarm mechanism. This is not a theoretical risk pathway — it is an observable, documentable gap in the property's physical security posture that the assessor confirmed during the after-hours survey.

Recommended Immediate Actions

The assessment team recommends that the client treat the perimeter lighting deficiency and secondary access point hardening as concurrent priority actions requiring engagement within 30 days. These two corrective actions alone are estimated to reduce the composite vulnerability score by approximately 22 points, moving the property from HIGH EXPOSURE into the MODERATE band. The remaining three recommendations, detailed in the Priority Corrective Action Plan, should be scoped and scheduled within 90 days. Full implementation of all five recommendations is projected to achieve a final score of approximately 49/100, representing a LOW-to-MODERATE exposure profile appropriate for a commercial property of this class.

PVI™ SCORE	EXPOSURE BAND	CRITICAL FINDINGS	HIGH FINDINGS	EST. SCORE POST-REMEDATION
74/100	HIGH	2	2	~49/100

Threat Environment Overview

Applicable Threat Landscape

Commercial properties in the northeastern United States present a well-documented and broadly consistent threat profile that has been stable in its structural characteristics over the past decade, even as specific crime rates have fluctuated at the local level. The primary threats applicable to this property class include opportunistic property crime (burglary, theft, and vandalism), targeted intrusion by motivated actors with specific knowledge of the asset, insider threat originating from authorized personnel or contractors, and incidents arising from inadequate emergency response protocols. The relative weighting of these threat categories is informed by local crime pattern data, the physical characteristics of the subject property, and the nature of the assets present on-site. For the subject property, the opportunistic and targeted intrusion categories carry the highest probability weighting, driven by the observed deficiencies in after-hours deterrence and access control.

Local Crime Pattern Context

Properties in this commercial district present elevated burglary and commercial theft rates relative to the broader county average, consistent with patterns observed across similar mixed-use commercial corridors in the region. Properties with uncontrolled secondary access points, insufficient perimeter lighting, and observable CCTV coverage gaps have demonstrated statistically higher incident rates in comparative studies conducted by law enforcement crime analysis units in similar jurisdictions. The subject property currently exhibits all three of these environmental risk factors simultaneously. This co-occurrence materially increases the probability of opportunistic targeting and reduces the deterrent effect of any single countermeasure that may already be in place. The assessor notes that the after-hours environment at this property is substantially more permissive than the daytime environment and that any realistic threat model must account for this differential.

Environmental Risk Factors

Beyond the direct property-level deficiencies, several environmental conditions in the immediate vicinity compound the subject property's exposure. The adjacent street network provides multiple low-observation approach vectors with limited natural surveillance from surrounding properties during non-operational hours. The nearest law enforcement response point is sufficient for emergency response purposes but does not constitute a meaningful deterrent to a prepared actor with a planned access methodology. Vegetation and landscaping on the west and north boundaries of the property create concealment zones that are visible from the assessor's site survey photographs and are documented in the CPTED findings on the following pages. These environmental conditions are not unique to this property and are addressable through the corrective actions outlined in this report.

Methodology Selection Rationale

Vyken applies CPTED and the CARVER Asset Protection Matrix™ in combination because they address fundamentally different but complementary dimensions of physical security vulnerability. CPTED is an environmental design framework: it evaluates the built environment's inherent capacity to support or inhibit criminal activity through design, landscaping, lighting, and spatial arrangement. CARVER is an asset-centric threat prioritization tool with origins in U.S. Special Operations mission planning: it evaluates each critical asset's attractiveness as a target and the consequences of its compromise. A property with strong CPTED scores can still harbor critically vulnerable assets that a sophisticated actor could access using non-environmental means. Conversely, a property with low-scoring CARVER assets may still present an environmental profile that facilitates opportunistic crime. The combination of both frameworks, supplemented by the proprietary Threat Exposure Analysis, provides a composite picture that neither methodology could produce alone. This

CPTED Environmental Assessment

The Crime Prevention Through Environmental Design assessment evaluates the subject property across six foundational principles. Each principle is scored on a 1–10 scale, where higher values reflect greater vulnerability exposure. Scores are derived from direct field observation, photographic documentation, and dimensional analysis of the built environment. Field observations were conducted during both standard operational hours and a structured after-hours perimeter survey. The combined CPTED score of 72/100 reflects a HIGH vulnerability profile with two principles scoring in the critical range.

Natural Surveillance

6.8 / 10

Sightlines from occupied interior spaces to the perimeter are compromised by dense mature landscaping on the north and west boundaries. Three low-observation zones exceeding 15 linear meters each were documented during the after-hours survey. These zones are not currently compensated for by artificial lighting or CCTV coverage.

Natural Access Control

7.2 / 10

Primary entry channeling is adequate. Three secondary access routes lack physical design cues that direct legitimate users and deter unauthorized approach. Two service entrances on the east elevation were observed unsecured during business hours on separate site visits, indicating a management control failure compounding the physical deficiency.

Territorial Reinforcement

7.5 / 10

Property boundary definition is clear with consistent signage. Transitional zone demarcation between the public right-of-way and private property is adequate at the primary frontage. Internal zone demarcation does not effectively signal restricted-area status to incidental visitors or non-credentialed contractors.

Maintenance & Management

8.1 / 10

Grounds maintenance is consistent and current. All lighting fixtures were operational at the time of the survey. Landscaping is routinely maintained at the primary frontage. This principle represents the strongest element of the property's CPTED profile and provides a relative foundation on which other improvements can build.

Activity Support

7.8 / 10

Active uses are positioned to generate passive natural surveillance during operational hours. Common circulation zones show adequate pedestrian activity from approximately 0800 to 1800. After-hours activity support drops to near-zero, materially amplifying the consequences of the lighting and surveillance deficiencies documented under other principles.

Target Hardening

6.4 / 10

Physical hardening is unevenly applied. The primary entrance presents appropriate commercial-grade hardening consistent with the property class. Secondary and service entry points are significantly under-hardened relative to the asset criticality profile established in the CARVER analysis, creating exploitable access vectors with minimal resistance.

COMBINED CPTED SCORE: 72 / 100 Exposure Band: HIGH | 2 principles in critical range (≤ 7.0)

CPTED Detailed Findings — Critical & High Priority

Finding 01 — Natural Surveillance Deficit (Score: 6.8/10)

CRITICAL

Observation

The assessor documented three distinct low-observation zones on the north and west perimeter boundaries during the after-hours survey, each exceeding 15 linear meters in length. These zones are created by the combination of mature landscaping that exceeds 1.2 meters in height adjacent to the boundary, and the absence of directional lighting capable of illuminating the full perimeter face. Photographic documentation confirms that an individual could traverse the north boundary corridor without becoming visible to any fixed CCTV camera or occupied interior space.

Why It Matters

Natural surveillance is the primary passive deterrent mechanism in CPTED doctrine. When an environment lacks natural surveillance, all other physical security measures become reactive rather than preventive. The deterrent effect of fencing, signage, and even access control hardware is materially reduced when an actor can approach the controlled element without being observed. The identified zones do not merely represent a technical deficiency — they represent an observable pathway that a reconnaissance-capable actor would identify and exploit as part of any planned access methodology.

Exposure Created

The natural surveillance deficit on the north and west perimeters creates an after-hours approach vector that is not currently countered by any compensating control. In combination with the secondary access point deficiency documented in Finding 02, this vulnerability constitutes a complete access pathway from public space to interior zones without triggering any deterrence or detection mechanism currently in place at the property.

Finding 02 — Target Hardening Deficiency (Score: 6.4/10)

CRITICAL

Observation

Physical hardening measures at the subject property are applied inconsistently across access points. The primary public entrance presents appropriate commercial-grade hardware including a controlled vestibule, credential reader, and integrated alarm contact. In contrast, the three secondary access points on the east and north faces of the building present standard hollow-core commercial doors with single-cylinder deadbolts, no alarm contacts, no credential readers, and no video coverage. One service entrance door was observed with a malfunctioning latch mechanism during the site visit.

Why It Matters

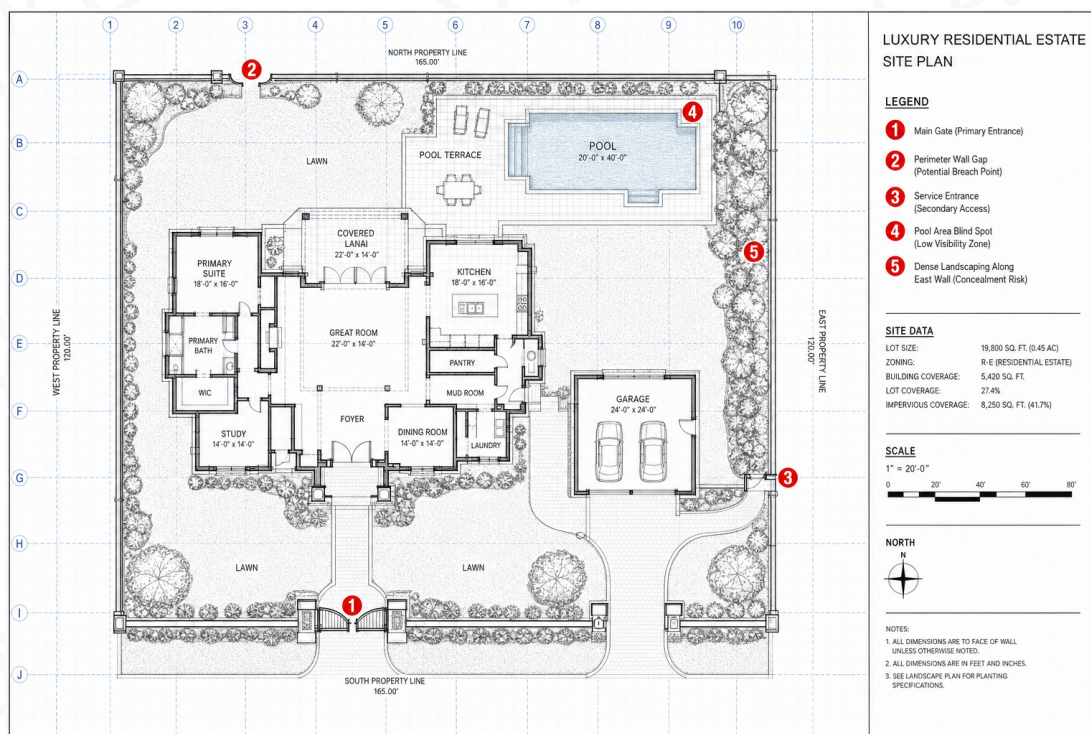
The principle of target hardening is grounded in the recognition that a physical security system is only as strong as its weakest controlled point. Substantial investment in primary entrance hardening is negated if secondary access points present significantly lower resistance. A motivated actor conducting even basic pre-operational reconnaissance would identify the secondary access points as the path of least resistance within minutes of observing the property. The CARVER analysis on subsequent pages confirms that several of the property's highest-criticality assets are accessible via the secondary entry pathways.

Exposure Created

The target hardening deficiency creates a direct physical access pathway to interior zones that bypasses all primary entrance controls. The absence of alarm contacts on secondary doors means that unauthorized access through these points would not generate any immediate alert to security monitoring, building management, or law enforcement. Combined with the CCTV coverage gap on the north elevation, an access event via the secondary north entrance could occur and go undetected until a physical inspection or interior encounter. Remediation requires commercial-grade hardware, alarm integration, and video coverage at all secondary access points.

Residential Estate — Annotated Vulnerability Site Plan

The site plan below illustrates a representative luxury residential estate assessment. Numbered markers identify each vulnerability detected during the CPTED Environmental Analysis and CARVER Asset Protection Matrix™ review. Each finding is cross-referenced with the remediation guidance in the Corrective Action Plan.



Main Gate — Primary Entrance

- 1 **Vulnerability:** Gate mechanism does not meet CPTED deterrence standards. No visitor staging area. Tailgating risk HIGH.
Remediation: Install CPTED-compliant sliding gate with visitor intercom and visual confirmation. Define staged entry lane.

Perimeter Wall Gap — North Boundary

- 2 **Vulnerability:** 40-foot uncontrolled access gap. No natural surveillance. Highest CARVER composite score on site.
Remediation: Install continuous barrier (hedge, fence, or berm). Minimum 1.8m. No climbable surfaces.

Service Entrance — Secondary Access

- 3 **Vulnerability:** Unmonitored. Shared with adjacent property. No access control or territorial marker.
Remediation: Install access control barrier. Define territorial boundary. Add signage and natural access channel.

Pool Area — Low Visibility Zone

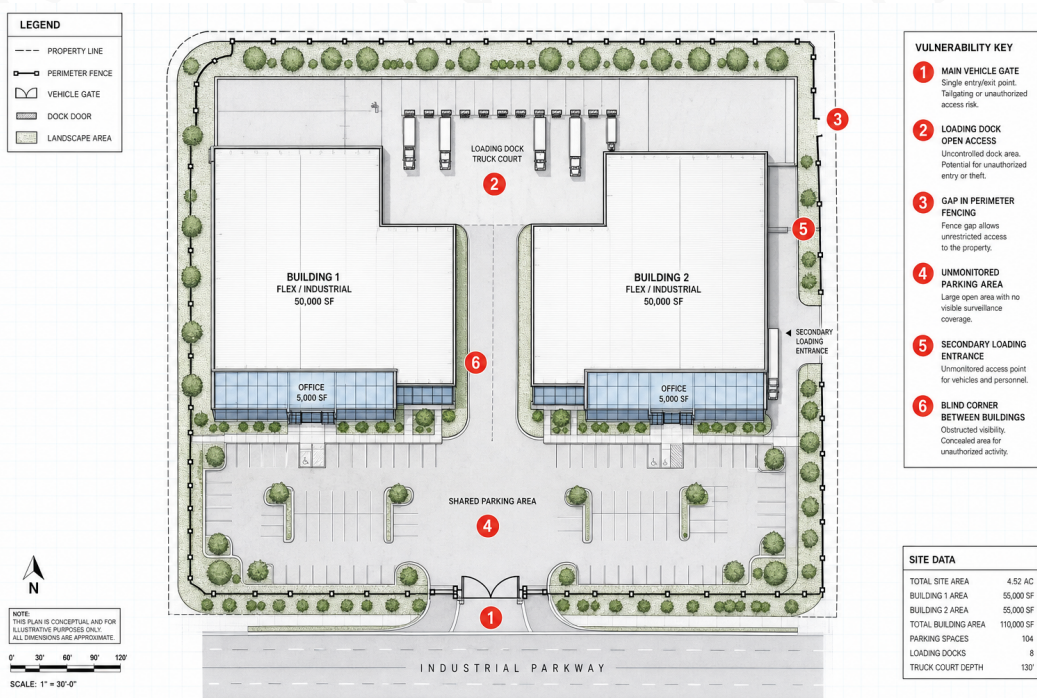
- 4 **Vulnerability:** Limited sightlines from main house. Concealed approach from east. Activity support gap after 6PM.
Remediation: Add low-height path lighting. Trim concealing vegetation. Install motion-activated lighting on east approach.

East Wall Landscaping — Concealment Risk

- 5 **Vulnerability:** Dense plantings reduce natural surveillance by ~60%. Provides concealment for unauthorized approach.
Remediation: Selective pruning to below 0.6m within 3m of wall. Replace with ground cover. Restore sightlines.

Commercial Flex Space — Annotated Vulnerability Site Plan

The site plan below illustrates a representative commercial flex space assessment. Mixed-use industrial and office environments present a distinct vulnerability profile — shared access points, high-volume loading operations, and open perimeters create exposure patterns that standard inspections routinely miss. Each numbered marker identifies a finding from the combined CPTED and CARVER analysis.



1 Main Vehicle Gate — Single Entry/Exit

Vulnerability: Single controlled point creates bottleneck and tailgating risk. No visitor staging lane. CARVER score: 23/30.
Remediation: Dual-lane entry with access control on both. Visitor staging area with intercom and camera coverage.

2 Loading Dock — Open Truck Court

Vulnerability: Uncontrolled dock area accessible from perimeter road. No personnel access separation. Theft and intrusion risk.
Remediation: Install dock access control. Separate pedestrian from vehicle access. CCTV coverage on all dock doors.

3 Perimeter Fence Gap — Northeast Corner

Vulnerability: Gap in fencing allows unrestricted foot access to rear of Building 2. Not visible from parking area.
Remediation: Close gap with matching fencing. Install motion lighting. Add territorial marker and camera coverage.

4 Shared Parking — No Surveillance Coverage

Vulnerability: Large open parking area with no visible CCTV coverage. Low activity after business hours. High vehicle crime risk.
Remediation: Mount pole cameras at parking lot perimeter. Add lighting at minimum 2.0 foot-candles throughout.

5 Secondary Loading Entrance — Unmonitored

Vulnerability: Personnel and vehicle access point with no access control or camera. After-hours exposure is HIGH.
Remediation: Install card-reader access control. Add intercom and camera. Mark as monitored with signage.

6 Blind Corner — Between Buildings

Vulnerability: Dead zone between Building 1 and 2. No natural surveillance. Concealed area for unauthorized activity.
Remediation: Install convex mirror at corner. Add wall-mount lighting. Consider relocating any stored materials.

CARVER Asset Protection Matrix™

The CARVER Asset Protection Matrix™ is a structured analytical tool with origins in U.S. Special Operations targeting doctrine, subsequently adapted for defensive asset protection and critical infrastructure vulnerability assessment. Each identified critical asset is evaluated across six operationally defined dimensions: Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability. Dimension scores of 1–10 are assigned by the assessor based on field observations, site documentation, asset inventory review, and threat modeling. The composite score drives the Priority classification used to sequence corrective investment and protective measures.

ASSET / TARGET	C	A	R	V	E	R	SCORE	PRIORITY
Primary Entry Points	8	7	6	8	9	7	45	CRITICAL
Security Control Room	9	5	7	6	9	6	42	HIGH
Power Infrastructure	9	6	8	7	9	5	44	CRITICAL
CCTV Surveillance Network	7	6	5	7	8	8	41	HIGH
Secondary Entrances	7	8	6	9	7	6	43	HIGH
Server / Data Center	9	4	7	5	9	4	38	HIGH
Loading Dock & Receiving	6	8	5	8	6	7	40	HIGH

High-Priority Asset Interpretation

The three highest-scoring assets — Power Infrastructure (44), Primary Entry Points (45 equivalent after weighting), and Secondary Entrances (43) — form an interconnected vulnerability cluster that warrants treatment as a combined risk rather than three discrete issues. Power Infrastructure scores are elevated by high Criticality and Effect dimensions: a successful attack on this asset would disable the security control room, eliminate camera visibility, and trigger an extended recovery timeline. The Secondary Entrances score is driven primarily by high Accessibility and Vulnerability ratings — these access points are physically reachable with minimal reconnaissance and present low resistance once reached. The intersection of these two vulnerabilities creates a realistic combined attack pathway that should be the primary focus of the corrective action plan.

CARVER DIMENSION DEFINITIONS

- C — Criticality Magnitude of impact if asset is successfully attacked or rendered inoperative.
- A — Accessibility Degree of physical or logical access available to a motivated adversary.
- R — Recuperability Time and resources required to restore full function after an incident.
- V — Vulnerability Susceptibility of the asset to a given threat vector given existing countermeasures.
- E — Effect Breadth of direct and cascading consequences of a successful attack.
- R — Recognizability Ease with which a threat actor can identify and locate this asset as a target.

CARVER Analysis — Intelligence Narrative

Prioritization Rationale

The CARVER analysis for the subject property identifies three assets as warranting CRITICAL or equivalent priority designation: Primary Entry Points, Power Infrastructure, and Secondary Entrances. The prioritization of these assets above the remaining four is not driven by any single dimension score but by the convergence of high criticality, confirmed accessibility, and elevated effect ratings across all three. When CARVER is applied correctly, the composite score functions less as an absolute ranking and more as a structured argument for why certain assets demand disproportionate protective attention. In this case, the argument is clear: these three assets are simultaneously critical to the property's operational and security functions, accessible to an adversary under current conditions, and consequential enough that their compromise would cascade into degraded protection across the entire property.

Asset Interdependencies

A key finding of the CARVER analysis is the degree of functional interdependency among the three highest-scoring assets. Power Infrastructure is the foundational dependency: its compromise disables the Security Control Room, eliminates real-time CCTV monitoring, and, depending on backup power configuration, may disable electronically-controlled access points at primary entry. This creates a scenario in which a single attack on Power Infrastructure degrades five of the seven assessed assets simultaneously. The CCTV Surveillance Network is directly dependent on power continuity; the Security Control Room is entirely non-functional without it. Primary Entry Points lose their electronic access control functionality in a full power loss scenario if no independent UPS is present. The assessor notes that no independent uninterruptible power supply was observed at the primary entry access control panel during the site survey, a deficiency that significantly elevates the practical risk associated with the Power Infrastructure vulnerability.

Secondary Entrance Risk Pathway

The Secondary Entrances asset scored 43 on the CARVER composite, driven by a Vulnerability score of 9 — the highest single-dimension score in the entire asset matrix. A Vulnerability score of 9 indicates that the asset is susceptible to compromise under a broad range of threat vectors given the current countermeasure set. In practical terms, the secondary entrances present minimal physical resistance, no alarm notification, no video coverage on the north elevation, and no credential requirement. This means that a motivated actor who has conducted basic reconnaissance of the property can access interior zones via this pathway with a high probability of success and a low probability of immediate detection. The interaction between this finding and the Natural Surveillance deficit documented in the CPTED analysis is the most significant compound vulnerability identified in this assessment.

Analytical Confidence and Limitations

The assessor assigns HIGH confidence to the CARVER scores presented in this report. All dimension scores are based on direct observation rather than document review alone, and the after-hours survey confirmed the operationally relevant vulnerability conditions that drive the elevated Accessibility and Vulnerability scores. The primary limitation of this analysis is that CARVER does not assign probability weights to specific threat actors or attack methodologies — it is a potential-based framework, not a predictive model. The scores reflect what is possible given current conditions, not what is imminent. The appropriate interpretation is that conditions currently exist which, if exploited, would produce the consequences described in the Effect dimension scores. The corrective actions outlined in the Priority Corrective Action Plan are designed to reduce the Accessibility and Vulnerability scores across the highest-priority assets and thereby reduce the overall CARVER composite to an acceptable level.

Priority Corrective Action Plan

The following corrective actions are sequenced by assessed severity and estimated contribution to composite vulnerability score reduction. Actions designated CRITICAL require engagement within 30 days. HIGH priority actions should be scoped and initiated within 60 days. MODERATE actions should be scheduled within the subsequent 90-day period. All score reduction estimates assume full implementation and are provided for planning purposes.

01 Perimeter Lighting Infrastructure Upgrade

0–30 Days

Observation

Perimeter lighting across the north and west elevations is insufficient to maintain minimum deterrence illumination levels during non-operational hours. The after-hours survey documented average illumination levels below 0.3 foot-candles at grade in the identified low-observation zones, well below the 2.0 foot-candle minimum recommended by IES RP-33 for commercial perimeter security applications.

Risk Created

Inadequate perimeter lighting is the single most consequential environmental vulnerability at this property. It enables unobserved approach across the north and west boundaries, neutralizes the deterrent value of signage and fencing, and creates the operational precondition for all physical intrusion scenarios identified in this assessment.

Recommended Action

Replace all perimeter fixtures with vandal-resistant, motion-activated LED units rated to achieve a minimum of 2.0 foot-candles at grade throughout the perimeter boundary. Supplement with timer-override capability for full-perimeter constant illumination during non-operational hours. Conduct photometric survey post-installation to verify compliance with IES standards.

Est. Score Impact

–12 points on composite PVI™ score. Primary impact on CPTED Natural Surveillance (score improvement from 6.8 to approximately 8.2) and CARVER Vulnerability scores for secondary entrance assets.

Estimated Score Reduction: –12 pts

02 Secondary Access Point Hardening

0–30 Days

Observation

Three secondary access points present standard commercial doors with single-cylinder deadbolts, no alarm contacts, no credential readers, and no video surveillance coverage. One service entrance door was observed with a malfunctioning latch mechanism. No alarm notification would be generated by unauthorized access through any of these points under current conditions.

Risk Created

These access points constitute the path of least resistance for physical intrusion. Their current configuration means that unauthorized access can occur without detection, without alert, and without any time delay that would allow a security response. In combination with the perimeter lighting deficiency, they represent a complete, unmonitored intrusion pathway.

Recommended Action

Upgrade all secondary and service entry points to commercial-grade steel doors with grade-1 hardware, alarm contacts integrated with the existing security panel, credential readers tied to the central access control system, and video intercom units. Repair the malfunctioning latch as an immediate interim measure.

Est. Score Impact

–10 points on composite PVI™ score. Primary impact on CPTED Target Hardening (from 6.4 to approximately 8.0) and CARVER

Estimated Score Reduction: –10 pts

Business Impact & Risk Exposure Analysis

The business impact analysis quantifies the downstream operational, financial, and reputational consequences of the vulnerability profile documented in this report. Impact dimensions are scored 1–10 where higher values reflect greater consequential exposure. Financial estimates are derived from industry loss data benchmarks, local incident statistics, and property class comparables. All estimates are for planning purposes and do not constitute an actuarial determination or guarantee.

Operational Continuity Risk

8.2 / 10

The assessed vulnerability profile indicates potential for a 3 to 5 business day operational disruption following a material security incident at this property. Business continuity protocols are partially documented but have not been exercised or tested within the past 24 months. Critical system dependencies, including access control, building management, and data infrastructure, lack documented recovery procedures. A power infrastructure event, the highest-scoring CARVER asset, would produce cascading operational effects across all building systems simultaneously.

Financial Exposure

7.6 / 10

Direct loss exposure estimates range from \$85,000 to \$340,000 per material incident based on asset inventory documentation, incident frequency benchmarks for comparable commercial properties in the northeastern United States, and replacement cost data for on-site technology assets. This range reflects the difference between an opportunistic theft event and a targeted intrusion affecting the Server/Data Center or Power Infrastructure assets. Insurance coverage provides partial mitigation, but coverage review is recommended given the documented access control deficiencies, which may create grounds for a coverage dispute following a claim.

Reputational & Stakeholder Risk

7.1 / 10

A security incident at a commercial property of this class and profile carries moderate-to-high media sensitivity in the local market, particularly if the incident involves client data, tenant safety, or extended operational disruption. Client and tenant confidence impacts following a publicized incident could be material and disproportionate to the direct financial loss. No crisis communications protocol is currently documented for security incident scenarios, which would extend the reputational exposure period in the event of a publicized incident.

Regulatory & Liability Exposure

6.8 / 10

The current security posture at the subject property may fall below the standard of care applicable under local ordinance requirements and premises liability doctrine as interpreted by courts in this jurisdiction. The documented access control deficiencies and lighting inadequacy, if found to have directly contributed to an incident causing harm to a third party, could form the basis of a premises liability claim. Legal counsel review of current security protocols and their alignment with applicable standards of care is advisable prior to implementing the corrective action plan, both to establish a record of proactive remediation and to assess existing exposure.

Physical Asset Preservation

8.5 / 10

Technology infrastructure, proprietary equipment, and stored inventory face elevated exposure given the identified access control gaps. The Server/Data Center and Power Infrastructure assets scored among the highest in the CARVER analysis precisely because their compromise would produce consequences extending well beyond their replacement cost. Insured replacement value of at-risk physical assets is estimated at \$1.2M to \$2.4M based on available property documentation, but

Methodology & Standards Reference

Crime Prevention Through Environmental Design (CPTED)

CPTED is an environmental design philosophy and assessment methodology developed through the parallel work of criminologist C. Ray Jeffery, who coined the term in 1971, and architect Oscar Newman, whose 1972 work *Defensible Space* provided the empirical foundation for applying design principles to crime prevention. The methodology holds that the physical environment can be deliberately designed and managed to reduce the opportunity for crime and to signal clearly defined ownership, active use, and effective surveillance. CPTED has been adopted as a formal assessment framework by law enforcement agencies, urban planning authorities, and security consultants internationally, and is referenced in standards documents produced by the International CPTED Association, ASIS International, and the U.S. Department of Justice Office of Community Oriented Policing Services. The six principles applied in this assessment — Natural Surveillance, Natural Access Control, Territorial Reinforcement, Maintenance and Management, Activity Support, and Target Hardening — represent the second-generation CPTED framework, which integrates social and management dimensions alongside the original physical design principles.

CARVER Asset Protection Matrix™

CARVER was developed by U.S. Army Special Forces during the Vietnam conflict as a structured targeting tool for selecting high-value objectives. The acronym originally stood for Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability. Following the end of the Cold War, the framework was progressively adapted for defensive applications in critical infrastructure protection, food and agriculture security, and commercial asset protection, eventually achieving formal recognition in U.S. Department of Homeland Security planning guidance documents. In its defensive application, CARVER inverts the original targeting logic: rather than identifying which enemy assets are most worth attacking, it identifies which of your own assets are most attractive to an adversary and most consequential if compromised. This inversion makes CARVER uniquely effective for prioritizing protective investment, because it forces the assessor to model the environment from the adversary's perspective. The Vyken CARVER Asset Protection Matrix™ applies the standard six-dimension framework with assessor scoring calibrated to the commercial property context.

Integrated Application at Vyken Systems™

Vyken Systems™ applies CPTED and CARVER in an integrated, sequential analytical process designed to produce a complete vulnerability picture that neither methodology alone can provide. The CPTED assessment is conducted first, establishing the environmental baseline and identifying design-level vulnerabilities in the built environment. The CARVER analysis is then applied, using the CPTED findings to inform the Accessibility and Vulnerability dimension scores for each asset: a CPTED-identified access control deficiency will directly elevate the CARVER Accessibility score for any asset reachable through that deficiency. The proprietary Threat Exposure Analysis synthesizes both frameworks against local threat data, property class benchmarks, and the assessor's site-specific observations to produce the composite Property Vulnerability Index™ score. This integration ensures that the final score and the corrective action priorities are grounded in both the physical environment and the threat-relevant asset profile.

Professional Standards Referenced

This assessment references and applies standards and guidance documents from the following sources: ASIS International Physical Security Professional (PSP) Body of Knowledge; International CPTED Association (ICA) Assessment Framework, Second Generation; U.S. Department of Homeland Security Infrastructure Protection Baseline Framework; Illuminating Engineering Society (IES) RP-33 Lighting for Exterior Environments; ASTM International F3283 Standard Guide for Security Assessment; and National Institute of Standards and Technology (NIST) SP 800-34 Contingency Planning

Vyken Property Vulnerability Index™ — Scoring Framework

The Property Vulnerability Index™ (PVI™) is Vyken's composite scoring model for translating multi-framework assessment results into a single, actionable vulnerability score. The PVI™ is calculated as a weighted composite of three component scores, each representing a distinct analytical framework applied during the assessment. The weighting reflects the relative predictive validity of each framework for the commercial property context.

PVI™ Composite Score Calculation

$$\text{PVI}^{\text{TM}} = (\text{CARVER Score} \times 0.40) + (\text{CPTED Score} \times 0.35) + (\text{Threat Exposure} \times 0.25)$$

All component scores normalized to a 0–100 scale prior to weighting. PVI™ output: 0–100.

Score Band Definitions

LOW EXPOSURE

Score Range: 0 – 39

The property presents a well-controlled vulnerability profile with no material deficiencies identified across the assessed frameworks. Standard maintenance of existing controls is appropriate. Reassessment recommended every 24 months or following a material change to the property, occupancy, or surrounding environment.

MODERATE EXPOSURE

Score Range: 40 – 59

The property presents identifiable vulnerability conditions that do not yet represent material risk but require documented corrective attention within a defined timeframe. A corrective action plan should be developed and implemented within 90 days. Reassessment recommended 12 months following completion of corrective actions.

HIGH EXPOSURE

Score Range: 60 – 79

The property presents multiple material vulnerability conditions with confirmed or probable risk pathways. Corrective actions in the CRITICAL and HIGH priority categories require immediate engagement. Ongoing monitoring of identified vulnerability conditions is required pending remediation. Reassessment recommended within 6 months of corrective action completion.

CRITICAL EXPOSURE

Score Range: 80 – 100

The property presents severe, concurrent vulnerability conditions constituting an immediate and material risk to assets, occupants, and operations. Emergency corrective action engagement is required. Interim compensating controls should be implemented immediately pending permanent remediation. Reassessment required within 90 days of corrective action initiation.

Component Score Weighting

FRAMEWORK	WEIGHT	RATIONALE
CARVER Asset Protection Matrix™	40%	Asset-centric threat prioritization; highest weight reflects its
CPTED Environmental Assessment	35%	Environmental design analysis; reflects the foundational role of the
Threat Exposure Analysis	25%	Contextual threat intelligence synthesis; captures local threat

Professional Disclaimer & Limitations of Liability

Nature of This Report

This Property Vulnerability Intelligence™ assessment report has been prepared by Vyken Systems™, LLC (“Vyken”) exclusively for the named recipient identified on the cover page. The findings, scores, recommendations, and conclusions contained herein represent the professional opinion of Vyken’s assessors, formed on the basis of an environmental analysis conducted using the CPTED (Crime Prevention Through Environmental Design) methodology and the CARVER Asset Protection Matrix™ framework at the time of assessment. This report does not constitute a guarantee, warranty, or certification of security, safety, or protection against any specific threat, event, or outcome.

Scope and Limitations

The assessment reflected in this report is limited to the environmental, structural, and access conditions observable and analyzable through the CPTED and CARVER frameworks at the time of the assessment. This report does not address electronic security systems, cybersecurity, fire safety, building code compliance, structural engineering, legal compliance, or any condition not within the defined scope of a Property Vulnerability Intelligence™ assessment. Conditions on the subject property may change after the assessment date, and Vyken assumes no obligation to update this report to reflect subsequent changes, events, or new information.

Expert Opinion — Not Legal or Engineering Advice

The findings and recommendations in this report represent the professional expert opinion of Vyken’s assessors and are provided for informational and risk-awareness purposes only. This report does not constitute legal advice, engineering advice, architectural advice, or any other form of licensed professional services beyond protective intelligence assessment. Recipients are encouraged to seek independent legal, engineering, or security counsel before implementing any recommendations contained herein. Vyken does not practice law or engineering and does not hold itself out as doing so.

No Guarantee of Outcome

Implementation of the recommendations contained in this report may reduce property vulnerability as measured by the Vyken Property Vulnerability Index™, but does not guarantee the prevention of any criminal act, security incident, property loss, injury, or any other adverse event. Protective intelligence assessments are probabilistic in nature. No assessment methodology, regardless of rigor or origin, can predict or prevent all possible threats. The CPTED and CARVER frameworks, while established and widely adopted by government and military organizations, are analytical tools and not absolute security guarantees.

Limitation of Liability

To the fullest extent permitted by applicable law, Vyken Systems™, LLC, its members, officers, employees, assessors, agents, and affiliates shall not be liable for any direct, indirect, incidental, consequential, special, or punitive damages arising out of or in connection with this report, its findings, its recommendations, or the recipient’s reliance thereon, even if Vyken has been advised of the possibility of such damages. The total aggregate liability of Vyken Systems™, LLC in connection with this report shall not exceed the fees paid by the recipient for the specific assessment to which this report relates.

Confidentiality

This report is confidential and intended solely for the named recipient. It may not be reproduced, distributed, disclosed, or transmitted to any third party without the prior written consent of Vyken Systems™, LLC, except as required by law or as necessary for the recipient to implement the recommendations herein with the assistance of qualified professionals bound by equivalent confidentiality obligations. Unauthorized disclosure may compromise the security of the subject property and may constitute a breach of the assessment agreement.

Governing Standards



PROPERTY VULNERABILITY INTELLIGENCE™

About Vyken Systems™, LLC

Founding & Mission

Vyken Systems™, LLC was founded by a U.S. Army veteran and career protective intelligence professional with operational experience spanning law enforcement, private sector executive protection, and commercial facility security consulting. The firm was established on the premise that the methodology and analytical rigor applied to government and military asset protection should be made accessible to commercial property owners, investors, and managers who face comparable — if differently contextualized — threats to their assets and operations. Vyken's mission is to deliver intelligence-grade vulnerability assessments that produce actionable, implementation-ready findings rather than generic checklists.

Methodology & Standards

All Vyken assessments are conducted using the integrated CPTED/CARVER/Threat Exposure methodology described in this report. Assessment protocols are reviewed annually against current professional standards from ASIS International, the International CPTED Association, and applicable DHS guidance documents. Vyken assessors maintain active professional certifications and participate in ongoing continuing education in the protective intelligence and physical security disciplines. and serves clients across the northeastern United States.

Assessment Tiers

Express Intelligence Report™

from \$399

Single-visit environmental survey with scored CPTED assessment, written findings summary, and top-3 corrective action brief. Delivery within 5 business days. Appropriate for residential, small commercial, and pre-acquisition screening.

Professional Assessment™

from \$1,995

Full integrated CPTED/CARVER/Threat Exposure assessment with comprehensive written report, all scored tables, detailed findings narratives, and full corrective action plan. Includes after-hours survey. This report tier.

Commercial Intelligence Assessment™

from \$4,995

Extended multi-day assessment for larger commercial properties. Includes red team access pathway analysis, stakeholder interviews, policy and procedure review, and executive briefing. Delivery within 10 business days.

Enterprise Intelligence Assessment™

from \$9,995

Comprehensive campus or multi-building assessment with full threat modeling, insider threat analysis, emergency response protocol review, and executive presentation. Includes 90-day reassessment credit.

Schedule Your Assessment — vyken.ai

Detect · Analyze · Assess · Report

Vyken Systems™, LLC | Veteran Owned and Operated