HORSEPOWER
ADVISORS

info@horsepoweradvisors.com
horsepoweradvisors.com

White Paper

The Shared Responsibility Gap

Navigating Security Realities in Multi-Tenant Class A Environments

Prepared by
Horsepower Advisors
January 26, 2026

HORSEPOWER
ADVISORS

Company **Overview**

"Horsepower Advisors optimizes security programs much like tuning an engine, aligning people, process, and technology to deliver maximum performance. We serve a diverse client base, delivering tailored, integrated solutions that enhance security and operational efficiency."

- Doug Farber
CEO & Co-Founder

More Horsepower for Your Security Strategy

Horsepower Advisors transforms security from a cost center into a strategic advantage. Leveraging decades of experience across corporate, nonprofit, startup, and government sectors worldwide, we specialize in integrating security as a core business function that drives resilience and operational efficiency.

Our approach mirrors the discipline of performance engineering: carefully controlling variables through expert oversight and tailored guidance to maximize outcomes. Effective security does more than protect, it enhances productivity, reduces risk exposure, and strengthens brand reputation. From comprehensive threat assessments to enterprise-level security program development, we use proven methodologies and modern technology to safeguard people, assets, and information.

What sets Horsepower Advisors apart is our depth of expertise and commitment to customization. We deliver solutions designed for each client's unique risk profile, whether supporting Fortune 100 companies, ultra-high-net-worth family offices, or innovative technology firms, allowing leadership to operate with confidence in an unpredictable threat environment.

Executive **Summary**

The Illusion of "Trophy" Security

In high-end Class A office environments, a dangerous gap often exists between *perceived security* and *actual resilience*. Prestigious addresses, marble lobbies, and uniformed personnel create a “Professionalism Bias”, the assumption that high lease costs automatically equate to high levels of protection.

In practice, the opposite is often true. The more prestigious the building, the more likely security measures prioritize appearance over operational rigor, resulting in what is commonly referred to as *security theater*. These environments can create hidden vulnerabilities that are easily exploited by motivated adversaries.

True resilience requires recognizing a fundamental reality: security in a multi-tenant building is not a service purchased from a landlord, it is a **shared responsibility**. Landlords protect the outer shell of the building, while tenants retain responsibility for risks that begin at their suite door and extend inward to people, culture, and operations.

This paper examines the vulnerabilities inherent in multi-tenant Class A environments, establishes **Protective Intelligence (PI)** as the strategic foundation of modern threat management, and provides a roadmap for moving from an *Operationally Fragile* posture to a **Resilient Stance**, one that enables leadership to act decisively and never be the last to know.

The **Foundation**

Protective Intelligence (PI)

Modern threat management is no longer defined by the thickness of a door or the number of cameras installed. In an era of targeted violence, insider threats, and grievance-driven attacks, the most effective security programs are **proactive rather than reactive**.

Protective Intelligence (PI) is the process of identifying, assessing, and managing individuals who demonstrate the interest, motive, and capability to cause harm, *before* they reach the perimeter. Horsepower Advisors advocates for PI as the foundation of any effective security program for four reasons:

1

Before the X Advantage

PI identifies pre-incident indicators—concerning communications or behavioral shifts—allowing for intervention **before escalation or harm occurs**.

2

Insider Threat Mitigation

Current or former employees and close associates account for a significant percentage of corporate security incidents. PI provides an early-warning system that traditional hardware cannot.

3

Targeted Attack Prevention

Organizations increasingly face threats driven by personal grievances against leadership or brand identity. PI ensures leadership is never the last to know.

4

Grievance Monitoring

Continuous monitoring of social media, open-source intelligence (OSINT), and internal sentiment allows organizations to identify emerging risks early and act decisively.

The Landlords « **Outer Shell** »

Assets & Liabilities

The landlord's primary duty is the protection of common areas and the building's core infrastructure. However, their hospitality-centric approach often creates the very gaps that adversaries exploit.

Critical Gaps in Base Building Security

The Professionalism Bias

Guards are trained for hospitality, not interdiction. An intruder in a high-end suit carrying coffee is rarely challenged, allowing for easy social engineering.

Vertical Transport & Stairwell Roaming

Once an intruder clears the lobby, stairwells often become "fail-safe" (unlocked) during fire alarms. An adversary can trigger a pull-station to bypass electronic locks, moving freely from a basement garage to an executive suite.

The Contractor "Ghost Staff"

Cleaning crews and HVAC technicians, often third-party contractors, frequently hold master-key access to the entire building. Their vetting standards rarely align with the high-security requirements of the tenants they

The "Summer Open Door" Vulnerability

To facilitate airflow or deliveries, garages and loading docks are often left unsecured. This creates an unmonitored "backdoor" that bypasses the hardened front lobby.

The Tenant's « **Inner Sanctrum** »

Behavioral & Technical Duty

The tenant's responsibility begins at their suite door. Relying solely on the landlord leads to Operational Fragility.

KEY TENANT VULNERABILITIES

Credential De-provisioning Lag

A delay in notifying the building of a termination creates a window where a disgruntled former employee retains building access.

Infrastructure "Dead Zones"

Modern Class A construction (concrete and Low-E glass) reflects cellular and emergency radio signals. In a "Safe Room" or internal corridor, employees may find themselves unable to call for help during a crisis.

Hardware Deficits

The use of non-compliant hardware (e.g., NDAA-prohibited devices) creates "cyber-physical" backdoors that can be exploited to pivot from the security network to the corporate broadcast or data network.

The Culture of Compliance

A "Resilient Stance" fails if staff members hold doors for strangers out of politeness. Security is a **culture**, not a product.

The “Shared Responsibility” **Risk Equation**

To quantify these risks,
Horepower utilizes the standard risk formula:

RISK = THREAT \TIMES, VULNERABILITY \TIMES, IMPACT

The Gap	Landlord Assumption	Tenant Assumption	The Reality
Deliveries	"Tenant will meet them in lobby."	"Guards will screen the driver."	Driver goes straight to suite door.
Terminations	"Tenant will tell us if there's a problem."	"Building won't let them in."	Terminated employee tailgates in.
Emergency	"Tenants will follow our fire plan."	"The building will tell us what to do."	Conflicting plans lead to chaos.

Strategic Recommendations **For Resilience**

For the **Tenant**

Hardening the "Bubble"

1. **Threat Management Team:** Create a cross-functional team (Security, HR, Legal) to manage a PI-based watchlist of individuals of concern.
2. **Modernized Security Tech:** Replace non-compliant hardware and integrate access control with AI analytics and silent panic alarms in high-risk areas.
3. **Medical Readiness:** Deploy *Stop the Bleed* kits with AEDs to address hemorrhage, the leading cause of preventable death in crises.
4. **Automated Offboarding:** Trigger immediate credential revocation across tenant and base-building systems via HR software.
5. **estricted Key Control:** Secure critical areas (e.g., IT/server rooms) with tenant-only key cylinders.

For the **Landlord**

Elevating the Standard of Care

1. **Enforce Garage Integrity:** Eliminate "open door" policies and upgrade lighting to LED standards to remove shadows that facilitate tailgating.
2. **Digital Visitor Management (VMS):** Replace paper logs with a digital VMS that scans government IDs and cross-references internal watchlists.
3. **Communication Integrity:** Install a **Distributed Antenna System (DAS)** to ensure first responder radio and cellular signal integrity in the building core.
4. **Improve Information Sharing:** Create a whole of building approach to security where threats are identified early, and the building-to-tenant disconnect is closed via automated tools.

Conclusion **The Resilient Stance**

Security in a multi-tenant building is a partnership, not a passive service. Organizations that rely solely on the Class A designation of their building remain **Operationally Fragile**, exposed to risks hidden beneath polished surfaces.

By combining physical hardening with a robust Protective Intelligence program, organizations transition to a **Resilient Stance**, one defined by awareness, coordination, and proactive decision-making. Leadership gains clarity into emerging threats, automated tools that reduce response time, and “Left of Bang” insights that enable action before disruption occurs.

In today’s threat environment, resilience is not about reacting faster—it is about seeing sooner.

Protective Intelligence (PI) CYCLE

About **Horsepower**

Horsepower is a premier risk management advisory firm specializing in Protective Intelligence and the convergence of physical and technical security. We transform organizations from a reactive posture to a **Resilient Stance.**

Expertise in Protective Intelligence and Risk Mitigation.

For more information on conducting a full Threat and Vulnerability Assessment (TVA), **contact our SME team today.**

HORSEPOWER ADVISORS

191 Main Street, Suite 119,Port Washington NY, 11050
(516) 527-3414 | doug@horsepoweradvisors.com