

# Outsourced, Exposed, and Out of Time

Why Physical Security Is Failing at the Executive Level

Written by: Briggs and Freeman | 2025 Edition



# Table of Contents

Executive Summary	3
The New Security Stack	4
Securing the Physical Layer	8
The Foreign-Owned Vendor Dilemma	13
Security Metrics That Matter	17
Strategic Recommendation	19

# Executive Summary

The landscape of physical security is being redrawn. AI and robotics are changing what's possible. Tenants and consumers are redefining what's acceptable. And a growing share of U.S. security vendors are now owned and controlled by foreign firms.

For decision-makers in commercial real estate, logistics, healthcare, retail, and private equity, the stakes have never been higher. Security is no longer a commodity. It's a brand issue. A liability issue. A trust issue.

This white paper explores the most urgent shifts reshaping physical security in 2025, from hybrid models and robotic patrols to access control modernization and the underappreciated threat of foreign-owned vendors. It is both a roadmap and a warning. We offer recommendations not just to modernize, but to de-risk your vendor landscape and protect the integrity of your enterprise.

*Because in a world of increasing volatility, trust cannot be outsourced to just anyone.*



# Chapter 1:

# The New Security Stack

## What Modern Protection Looks Like

For decades, physical security meant gates, guards, and good intentions. In most asset classes, security was a visible deterrent—an acceptable, even expected, operating cost. But the world has changed, and with it, the expectations of tenants, insurers, investors, and regulators.

Physical security today is no longer just about protection. It's about perception, liability mitigation, and operational intelligence. The “stack” has evolved—from a single line item to an integrated system of human, digital, and robotic elements designed to provide scalable, measurable, and adaptive risk reduction.

Leading organizations now deploy hybrid security models that combine:

- **Human presence** - uniformed or plainclothes, armed or unarmed, concierge or command-driven
- **Technology augmentation** - AI-enabled surveillance, threat analytics, and biometric access
- **Robotics** - autonomous patrol units and interactive lobby robots
- **Cloud-based controls** - real-time credentialing, mobile authorization, remote lockdown protocols

And increasingly, they do this with strategic intent, not just as a response to incidents or regulation.

# Human Capital, Reimagined

Despite the rise of automation, people remain the front line of any meaningful security operation. But the roles, expectations, and economics have changed.

## Unarmed & Concierge Officers

In low-risk or hospitality-focused environments, unarmed officers and concierge-style staff provide high-value tenant and visitor engagement, access control, and soft-skill de-escalation. These professionals support brand image and customer experience as much as they provide safety. Their relatively low cost and high visibility make them ideal for buildings focused on welcoming experiences.

**Typical Cost:** \$15-\$35/hr

**Best Fit:** Mixed-use properties, retail-facing lobbies, residential towers

**Limitation:** Minimal threat response capability

## Uniformed Armed Officers

Armed personnel remain essential for high-value or high-liability assets—particularly where workplace violence, public risk, or critical infrastructure is a concern. Their presence carries psychological weight and deters most opportunistic threats. But they also carry increased insurance costs, legal exposure, and reputational risk—especially if improperly deployed.

**Typical Cost:** \$25-\$100/hr

**Best Fit:** Corporate HQs, data centers, medical campuses, threat-identified locations

**Limitation:** Public-facing optics and liability challenges

## Plainclothes Armed Security

This tier often goes unnoticed—but not unfelt. Executive-focused or VIP-level clients increasingly request discreet, armed security presence that integrates seamlessly into the tenant environment. This “invisible deterrence” balances protection and public image, especially in buildings prioritizing aesthetics and guest experience.

**Typical Cost:** \$35-\$150/hr

**Best Fit:** Executive suites, media-sensitive locations, legal or private equity firms

**Limitation:** High cost, less visible deterrence

# Technology as Force Multiplier

Physical security is undergoing the same evolution IT experienced in the last decade. Today's systems are intelligent, interconnected, and insight-generating. AI is not replacing guards-but it's enhancing their capability, especially where human fatigue, bias, or oversight would otherwise create risk.

## AI-Powered Cameras & Detection

Modern AI cameras don't just record-they analyze. They learn from movement patterns, detect anomalies in real time, and trigger automatic alerts long before a human operator would act. Many platforms now embed edge-computing capabilities directly in the camera housing, eliminating latency and infrastructure costs. Software add-ons like AI-based gun detection, facial recognition, and vehicle plate tracking create layers of proactive threat awareness without requiring human interpretation in real time.

## Weapons Detection

This remains the holy grail of public security technology: non-invasive, passive systems that can scan crowds or entryways for concealed weapons without interrupting flow. While still imperfect, vendors are racing to develop systems with high throughput and low false positives-particularly for sports venues, hospitals, and transit environments. "The gold standard will be mobile, autonomous detection systems that blend into architectural design while flagging real threats before they cross the threshold."

## Robotic Presence: From Gimmick to Game-Changer

While once dismissed as novelties, robotic security platforms are now making measurable contributions-particularly in submarket assets or environments lacking the budget or infrastructure for full-time human staffing.

## Exterior Patrol Robots

Used in parking decks, open campuses, or industrial perimeters, these autonomous units provide consistent surveillance, record activity, and escalate alerts without distraction or fatigue. They're most effective in large areas that don't justify foot patrol but still require deterrence and monitoring.

## Lobby Robots

Interactive robots positioned in lobbies or entryways can:

- Greet and verify visitors
- Answer common questions
- Alert staff to suspicious behavior
- Serve as an always-on presence where full-time staffing isn't feasible
- **But their value goes deeper:** they reinforce a brand image of modernity, control, and care.

## Case Study: The Parking Deck That Policed Itself

In one Class A mixed-use campus, tenant employees and delivery drivers routinely parked in customer-designated short-term spots, ignoring signage and undermining retail access. Management deployed two roving security officers to patrol levels 1 and 2 of the garage.

### After weeks of monitoring:

- 15-20 citations per shift
- Verbal altercations with violators
- No sustained behavior change

**The cost:** Two officers across 2 shifts, every weekday-pulled from higher-priority tasks. No measurable ROI.

Instead, the team deployed an autonomous robot armed with license plate tracking and tenant data.



Shift 1, Day 1: 98 citations with photo documentation



Shift 2, Day 1: 58 additional citations



By Week 2: Weekly citations dropped to <5 total



Even more: The robot flagged a suspicious vehicle that appeared daily without parking. Cross-referenced with BOLO reports, the vehicle was tied to a string of auto thefts. A timely traffic stop led to multiple arrests.

### The Takeaway

Security today is no longer a guard at the door. It's an ecosystem-an interconnected network of human judgment, technological consistency, and operational design. For organizations seeking to reduce liability, enhance trust, and gain visibility into their own operations, the new security stack isn't optional-it's essential.

### Next-gen security means:

- Staffing with intention, not habit
- Deploying technology where humans fall short
- Using robotics not to replace-but to expand-presence and awareness

And most of all: it means understanding that security, done right, isn't a cost center. It's a strategic advantage.

# Chapter 2: Securing the Physical Layer

## Access Control, Turnstiles, and the Tenant Experience Gap

In today's buildings, access control is no longer just a security tool. It's an operational interface. Every entry point, elevator, or barrier becomes a moment where convenience, risk, and tenant perception collide. Whether you're operating a suburban business park or a high-rise in Midtown, the question is the same: Can you manage access without introducing friction, cost, or liability?

Modern access systems must now balance three overlapping priorities:

- **Operational Efficiency:** Managing dynamic user populations without constant intervention
- **Emergency Readiness:** Ensuring that every door, elevator, and turnstile responds instantly under duress
- **Tenant Experience:** Providing frictionless flow for authorized users without frustrating the people who pay rent

For asset managers and operators, the challenge isn't the concept, it's the execution. Especially in multi-tenant environments, where user needs diverge wildly and infrastructure is often patchworked over decades of upgrades.

## The Multi-Tenant Access Problem

Legacy access systems were not built for the realities of modern occupancy. Most rely on on-premise servers, outdated fob/card infrastructure, and siloed connections between doors, elevators, and common areas.

When these systems were first installed, buildings had static user populations, and most credentials were provisioned annually. Today's post-COVID reality looks very different:

- Multiple tenants with divergent security needs
- Shared spaces, hybrid schedules, and rotating contractors
- Visitors, deliveries, vendors, and part-time occupants
- Employees who work from home 2 or 3 days a week and demand mobile credentials when on-site
- Property managers accountable for both **security uptime** and **tenant satisfaction scores**

## A Common Scenario

One tenant requests full biometric access on their executive floor. Another demands open access to the parking garage for delivery drivers during business hours. A third wants to limit vendor access only to certain elevators, but those elevators are shared with everyone else.

The result? Inconsistent application of security policies across tenants, and worse: inconsistent enforcement. Tenants will notice, and in some cases, document, the disparities.

This can lead to real legal exposure if a security incident occurs, and one tenant can demonstrate they received less protection than another in the same building.

### Modernizing the Stack: From Fragmented to Fluid

To address this, high-performing portfolios are moving toward cloud-based, adaptive access control platforms that offer:

- Centralized credential management
- Granular, role-based access permissions (e.g., by floor, time of day, user type)
- Mobile-first credentialing with smartphones replacing fobs and badges
- Real-time revocation & alerting
- Integration with elevators, cameras, sensors, and lockdown protocols

These systems can flex across different tenant requirements without sacrificing speed or control. And in emergencies, they offer something legacy systems rarely could: a unified response across multiple systems in seconds.



# The Retrofit Challenge: Infrastructure Meets Budget

Unfortunately, access control modernization doesn't exist in a vacuum. Especially for assets built before 2010, retrofitting becomes a careful dance between:

- Electrical infrastructure limitations
- Elevator panel compatibility
- Turnstile configurations
- Budget constraints
- Tenant schedules and disruption tolerance

The true cost of access modernization often hides in the complexity of integration and the scope of disruption not just the sticker price on hardware.

Solution Type	CapEx Range	Use Case
Cloud-based Access Control	\$15K-\$40K	Mid-size to large multi-tenant assets
AI Cameras & Video Analytics	\$20K-\$80K	Lobbies, garages, public corridors
Bullet-Resistant Turnstiles	\$7K-\$25K per lane	Executive floors, public venues, federal tenants
Lobby Security Robot	\$60K-\$90K	Submarket assets, lightly staffed properties

But the investment can be worth it, especially in competitive leasing markets, where security posture is now seen as an amenity.

## Glass Barriers, Turnstiles, and Cultural Fit

In years past, glass barriers were hailed as a breakthrough, combining architectural elegance with access enforcement. But real-world testing has exposed major flaws:

- **Tailgating persists:** users piggyback behind others without scanning
- **Breakage risk:** crowd pressure, panicked evacuations, or intentional attacks can shatter barriers
- **Maintenance fatigue:** dirty sensors, misalignment, and software updates lead to false alerts and user frustration

Where glass fails, some buildings are turning to bullet-resistant enclosures, especially in buildings housing courts, government agencies, or executive leadership. But these come with sticker shock and questions about tenant perception. "Are we creating a secure space or projecting that we expect violence?"

**Again, asset culture matters.**

## Retrofit Barrier Cost Comparison Table

Barrier Type	Cost Metric	Price Range	Notes
Standard acrylic/glass	Per lane/panel	\$500–\$3,000	Basic protection, no ballistic rating
Bullet-resistant glass (material)	Per square foot	\$70–\$500	Labor/framing not included
Compact bullet-resistant panels	Per lane/panel	\$1,000–\$3,500	Retrofit-friendly, but limited coverage
Full lobby enclosure	Per entry structure	\$7,000–\$25,000+	High security, high disruption, high cost

### The Most Overlooked Risk: Inconsistency Across Assets

One of the greatest operational liabilities in a large real estate portfolio is inconsistent security standards across like-kind assets. This often results from:

- Using multiple vendors with different approaches in different markets
- Lack of portfolio-wide assessments
- No shared documentation or escalation protocols
- Contract awards that only shift responsibility to lowest-bid providers

In a legal dispute, plaintiffs may compare the security measures at one asset with those at another in the same portfolio. If one tenant can argue they received less protection from the same owner or operator, the reputational and financial risk grows exponentially.

A fragmented access control program may meet compliance but still fail under litigation.

### Top Operational Liabilities in Large Real-Estate Portfolios

Multiple Vendors

**HIGH IMPACT**

*Different Approaches across Markets*

No Portfolio Assessment

**HIGH IMPACT**

*Lack of standardized evaluation*

Poor Documentation

**HIGH IMPACT**

*Missing escalation protocols*

Lowest-Bid Providers

**HIGH IMPACT**

*Contractual Liability Shifts*

#### Legal Liability Warning

In legal disputes, plaintiffs may compare security measures across portfolio assets. Inconsistent protection levels create exponential reputational and financial risk.

**“A fragmented access control program may meet compliance but still fail under litigation.”**

# Strategic Takeaways



## Security as Experience Layer

Security shapes perception just as much as signage, finishes, or concierge staff



## Portfolio Consistency

Align protocols, review vendors, and document differences across assets



## Cloud-Native Platforms

Systems that communicate during emergencies aren't luxury, they're liability shields



## Retrofitting Investment

Cost reduction in risk, tenant retention, and crisis response capabilities



## Asset Culture Alignment

Security decisions must reflect asset culture and user expectations

## Key Insight

Security infrastructure decisions must balance operational efficiency, legal compliance, and user experience while maintaining consistency across your entire portfolio.



# Chapter 3: The Foreign-Owned Vendor Dilemma

## **When Security Isn't Local**

In a globalized economy, outsourcing is standard. Facilities are managed by national firms. Surveillance is monitored offshore. Even “boots on the ground” are often subcontracted through a chain of vendors. But few organizations realize how deep—and how risky—that outsourcing has become when it comes to physical security.

Some of the largest security firms operating in the U.S. today are wholly owned by foreign parent companies. They wear American uniforms. Their staff live in your market. Their invoices are printed in U.S. dollars. But their ultimate control? Offshore.

## **The Hidden Risk in Your Vendor Stack**

To a property manager or operations executive, this may seem immaterial—until it isn't. The foreign ownership of a security vendor creates a jurisdictional, operational, and legal vulnerability that can surface at the worst possible moment.

Here's how:

### **1. Jurisdictional Ambiguity**

A U.S.-based subsidiary of a foreign company may be subject to laws in its home country, even while operating in compliance with local regulations.

#### **For example:**

- A Swedish parent may be compelled to share sensitive data under the country's transparency laws.
- A Canadian firm may be protected by local labor standards that make termination for performance difficult.
- A Spanish-based vendor may be immune to U.S. civil claims if liability is routed through shell entities.

#### **Now consider what happens when:**

- Your building's access logs are subpoenaed in a domestic investigation
- Your security footage becomes evidence in a civil lawsuit
- Your vendor's contract has indemnity language that shields them but exposes you.

Control is an illusion if your vendor answers to a foreign board.

## 2. Cultural Misalignment

Security is more than a technical service. It's a human-intensive profession rooted in judgment, discretion, and escalation protocols. But what constitutes "appropriate force" or "acceptable delay" can vary significantly between countries.

What's considered a "measured de-escalation" in one country may appear negligent or passive in an American context.

### In real terms, this can manifest as:

- Missed cues in threat escalation
- Inconsistent or delayed reporting
- Poor alignment with U.S. use-of-force laws
- Training that meets international ISO standards but lacks state or local compliance nuance

More importantly, cultural misalignment creates brand risk. If a guard fails to act, or overreacts, the resulting PR crisis is yours to manage, not theirs.

## 3. Data Sovereignty

Physical security now produces massive digital exhaust:

- Entry logs
- Bodycam footage
- Drone feeds
- Incident reports
- Facial recognition scans
- Biometric access attempts

If your vendor stores, processes, or transmits that data outside U.S. borders—even temporarily you may be in violation of:

- Federal or state privacy laws (e.g., CCPA, HIPAA)
- Commercial contracts (e.g., data residency clauses)
- NDA or client security agreements

**Even worse:** many companies don't discover these violations until litigation or breach investigation forces forensic review.



## **Real-World Consequences**

In one case, a regional health system discovered, after a break-in, that their vendor's footage retention was limited to 72 hours due to a global data policy based in Ireland. By the time legal counsel requested footage, it had been overwritten. The incident resulted in a seven-figure settlement.

In another case, a vendor operating under a foreign parent company refused to release incident logs during a wrongful termination suit, citing data protection laws in their country of origin. These aren't hypotheticals. They're emerging liabilities in a globalized vendor ecosystem that's more opaque than executives realize.

## **The Regulatory & Fiduciary Angle**

If you are:

- A public company (subject to Sarbanes-Oxley or ESG reporting)
- A healthcare operator (subject to HIPAA/HITRUST)
- A REIT or fund manager (with fiduciary oversight obligations)

...then foreign ownership in your physical security vendor stack is not just a detail. It's a material risk.

## **Boards and investors are increasingly aware of:**

- Third-party vendor risk
- Data residency compliance
- Continuity of operations during geopolitical conflict

If your security vendor cannot guarantee data control, response timelines, or continuity under U.S. legal jurisdiction, you may be out of compliance, or worse, exposed during crisis.

## **How to Audit for Foreign Control**

Many vendor relationships appear local on paper. Uniformed officers. Regional contact. U.S.-based invoices.

But beneath that surface may lie a chain of control that stretches across borders, shell entities, or private equity holdings.

## **Here's what to look for:**

- Ultimate Beneficial Ownership (UBO) structure
- Where security data is stored and processed
- Jurisdiction of legal entity on contract
- Contingency plans in case of parent company regulatory action
- Liability indemnification clauses and enforcement venue

## The “Control Test”

Chesley Brown recommends a five-question test to assess potential exposure:

1. Who owns your company, ultimately?
2. Where is client security data stored, and who has access?
3. Can your footage or access logs be accessed by any foreign authority?
4. Are you required to report or cooperate with any foreign government agency?
5. In a breach or failure, where is legal jurisdiction for resolution?

If your vendor cannot answer all five clearly, and with written assurance, your organization has a blind spot.

## Why This Matters Now

The U.S. is entering a period of increased geopolitical strain. Rising regulatory scrutiny. ESG audits. Sophisticated cybercrime. Coordinated disinformation.

In this environment, trust becomes a strategic differentiator. The vendors who secure your buildings must be as aligned, compliant, and accountable as your internal teams.

You wouldn't let a foreign state control your IT backbone. Why would you let them control your access logs, camera feeds, and emergency response chain?

## Chesley Brown's Position

Chesley Brown is a privately held, U.S.-based security consultancy with no foreign ownership or offshore control. Our data stays onshore. Our legal jurisdiction is domestic. Our people are trained to U.S. compliance standards, not international abstractions.

## Executive Takeaway

- Foreign-owned security vendors introduce real legal, operational, and reputational risk
- These risks are often hidden behind layered subcontracting and marketing spin
- Executives should treat vendor ownership like they treat cybersecurity supply chains: transparent, auditable, and aligned to business continuity goals
- When crisis hits, trust cannot be outsourced

# Chapter 4: Security Metrics That Matter

## What the Data Actually Show

In a field often driven by headlines and fear cycles, there's increasing pressure on security leaders to anchor their decisions in data. But numbers alone don't tell the full story. Strategic risk leaders need to interpret these metrics in context measuring not just frequency, but exposure, perception, and operational impact.

Recent incident trends from 2024–2025 reveal a nuanced picture of security in the built environment. They confirm what many forward-thinking executives already suspect: while serious events remain statistically rare, the consequences of inadequate preparation are growing—and public expectations have shifted dramatically.

Consider K–12 school shootings. While the total number, 254 incidents, represents less than 0.2% of U.S. campuses, the cultural ripple effect is profound. These events have reset societal expectations. Parents, teachers, and the broader public now demand visible protection measures in shared spaces: not just schools, but malls, offices, and public venues. It's no longer enough to argue statistical rarity; the perception of preparedness is now part of the brand promise for any organization operating in a public-facing asset.

In the commercial sector, the trends are equally instructive. In 2023, nearly 30 percent of all U.S. active shooter events occurred within office buildings. These were not random attacks, but intentional incidents targeting symbolic business locations, often during operating hours and in multi-tenant environments. Most of these buildings had some form of access control or security presence—but those systems were either underutilized, poorly integrated, or procedurally disconnected from actual emergency response plans. Hardware, it turns out, doesn't equal readiness.

Despite these wake-up calls, modernization remains uneven. About half of all commercial real estate assets in the U.S. now feature “advanced access control”—a term that broadly includes mobile credentialing, biometric inputs, and cloud-based authorization. Yet in practice, the actual effectiveness of these systems is undermined by fragmentation. One floor may feature facial recognition while another requires badge scans. Visitors may be screened in lobbies but not in elevators. Vendors may bypass credentialing altogether via manual overrides or back-of-house entries. This patchwork approach leads to operational blind spots and, in high-pressure scenarios, critical delays.

The use of armed guards remains rare—deployed primarily in high-risk, high-liability, or high-visibility settings such as federal buildings, financial institutions, or healthcare campuses with sensitive material. For many operators, the decision not to employ armed personnel stems from valid concerns: insurance liability, tenant discomfort, or brand image in hospitality-driven environments. However, this has also created a security landscape where threat deterrence is often passive or symbolic rather than active or strategic.

**The attached table summarizes select data points and their implications:**

<b>Metric</b>	<b>Value / Trend</b>	<b>Strategic Implication</b>
K-12 school shootings (2024-25)	254	Public now expects visible, proactive security in all venues
Commercial shooter incidents (2023)	14 out of 48 total U.S. incidents	Offices are soft, symbolic targets needing layered response
CRE assets with advanced access control	~50%	Adoption growing, but implementation is fragmented
CRE assets with armed guards	Minority	Armed presence remains situational and culturally sensitive

What this data reveals is not just an evolution in the threat landscape, but a divergence in organizational readiness. Security may be a low-frequency event, but it is no longer a low-impact one. A single incident, especially if mishandled, can result in litigation, tenant loss, reputational harm, and even loss of investor confidence.

Perhaps most tellingly, preparedness is becoming a proxy for organizational maturity. Insurance underwriters, regulators, and even institutional investors are starting to assess physical security posture the same way they evaluate cybersecurity frameworks: as a governance issue, not just an operational one.

Executives overseeing multiple properties should use this data to benchmark their own environments. Do access control systems reflect the tenant risk profile? Are emergency procedures integrated with hardware capabilities? Has the response plan been tested under pressure, in real time, across teams?

**More importantly:** can you demonstrate that your security decisions are proportionate, well-documented, and responsive to the data?

In a crisis, or a courtroom, you will be expected to show your math.

# Chapter 5: Strategic Recommendations

## A Playbook for 2026 and Beyond

Security, like any enterprise function, should be measurable, accountable, and adaptable. Yet in many organizations, it remains siloed-overseen by facility managers, disconnected from IT, or delegated entirely to third-party providers without strategic oversight.

In 2025, that approach no longer holds. Risk is increasingly multidimensional. Cyber and physical vulnerabilities are converging. And the line between protection and perception has blurred. What's needed now is not just vigilance-but vision. The following strategic recommendations are designed for operators, owners, and investors who want to align their security posture with the realities of today's threat landscape and tomorrow's expectations.

### Blend Human and Machine

Security is no longer a binary choice between manpower and automation. High-performing environments leverage both-allocating each to their respective strengths.

Humans bring judgment, emotional intelligence, and dynamic response. Machines bring scale, consistency, and data. Together, they form a model that can cover more territory, respond faster, and adapt over time.

Robotic patrol units can replace static overnight posts or cover hard-to-monitor areas without fatigue. AI surveillance systems can flag anomalies long before a human operator would act. Lobby robots can extend a sense of presence where budgets don't allow full-time staff.

But these tools don't eliminate the need for people. They amplify the effectiveness of your best personnel-freeing them from rote observation and reassigning them to high-value tasks, where real-time decisions matter most.



## **Audit the Vendor Landscape**

Outsourcing is inevitable. But abdication is not.

Executives must treat security vendors the way they treat financial auditors or legal counsel: with scrutiny, transparency, and clear accountability.

Begin with a forensic audit of your existing vendor structure:

- Who owns each company you contract with?
- What subcontractors do they rely on-and where are they based?
- Where is your data stored, and under what jurisdiction?
- Who ultimately bears liability in the event of failure or breach?

Too many organizations rely on vendors with unclear ownership chains or foreign data residency, creating exposure they neither understand nor control. Demand full disclosure. Require written guarantees on data custody and legal jurisdiction. And if a vendor can't-or won't-answer these questions, consider that a risk in itself.

## **Design for Flexibility**

Static systems are vulnerable systems. As threats evolve, so must your ability to respond-without undergoing a full system replacement every three years.

Modern access control platforms should support mobile credentials, biometric inputs, and cloud-based administration. They should integrate with existing video, elevator, and alerting systems. And they should allow permissions to change in real time as roles, tenants, or risk conditions shift.

Critically, choose systems that prioritize interoperability over brand loyalty. A platform that locks you into proprietary hardware will age faster and cost more to upgrade. Look for solutions that are vendor-agnostic, standards-based, and future-ready.

## **Shift from Static to Adaptive**

Most security programs were built for yesterday's threat model: known threats, predictable schedules, and fixed perimeters.

Today, perimeters are porous. Threats are internal and external. And schedules are fluid.

Organizations need to move from static policies to adaptive frameworks.

This means:

- Phasing upgrades based on asset risk-not just budget timing
- Conducting annual threat modeling, not one-time assessments
- Aligning protocols with cultural context, not just compliance standards

An adaptive program treats security as an ongoing investment-one that evolves with tenant behavior, urban dynamics, and geopolitical shifts. It also positions security as a strategic differentiator, not a back-office line item.

## Lead with Intelligence

Data is your most underutilized security asset. Cameras record more than they analyze. Access logs are stored but rarely studied. Incident reports are filed and forgotten.

Leaders should push for intelligence-driven operations—where AI analytics, patrol data, and threat alerts feed into a live risk dashboard. This allows for:

- Better vendor oversight
- Improved incident response
- Early detection of pattern anomalies

More importantly, it enables executives to justify investment decisions with evidence, not anecdotes.

When budget conversations arise—or when incidents occur—the ability to demonstrate data-backed strategy becomes a shield against criticism and a beacon of leadership.

## Final Thought

Security is no longer about hardening the walls. It's about building systems—people, processes, and technologies—that anticipate risk, adapt in real time, and instill confidence in every stakeholder.

At Chesley Brown, we believe strategic security isn't a reaction to crisis. It's a form of leadership. It's a demonstration that your organization doesn't just operate in the world—it understands it.

If the past few years have taught us anything, it's this: resilience is not the result of luck. It's the result of planning.

The companies that win in 2026 and beyond will be those who:

- Treat physical security as a strategic investment—not a checkbox
- Vet vendors with the same rigor as investors or acquisition targets
- Understand that in moments of crisis, **trust cannot be outsourced**



# Conclusion

## **Security is a Strategic Choice**

The physical security landscape is evolving rapidly, driven by technology, reshaped by global events, and defined by new expectations from tenants, investors, and regulators alike. Across industries and asset classes, the message is clear: security is no longer just about protection, it's about leadership.

Your response to risk is no longer invisible. It's on display in your lobbies, in your contracts, and in your crisis playbooks. Every decision from who you hire, what you install, and how you respond is a signal to your stakeholders about how seriously you take your obligations.

And in a world where vendors are increasingly foreign-owned, systems are cloud-based, and incidents can define reputations, it's no longer enough to rely on legacy models or lowest-bid contractors.

This isn't about overreaction. It's about preparation. It's not about fear. It's about foresight.

At Chesley Brown, we don't believe in cookie-cutter security. We believe in clarity. In assessments tailored to the real-world threats facing your properties, your people, and your brand.

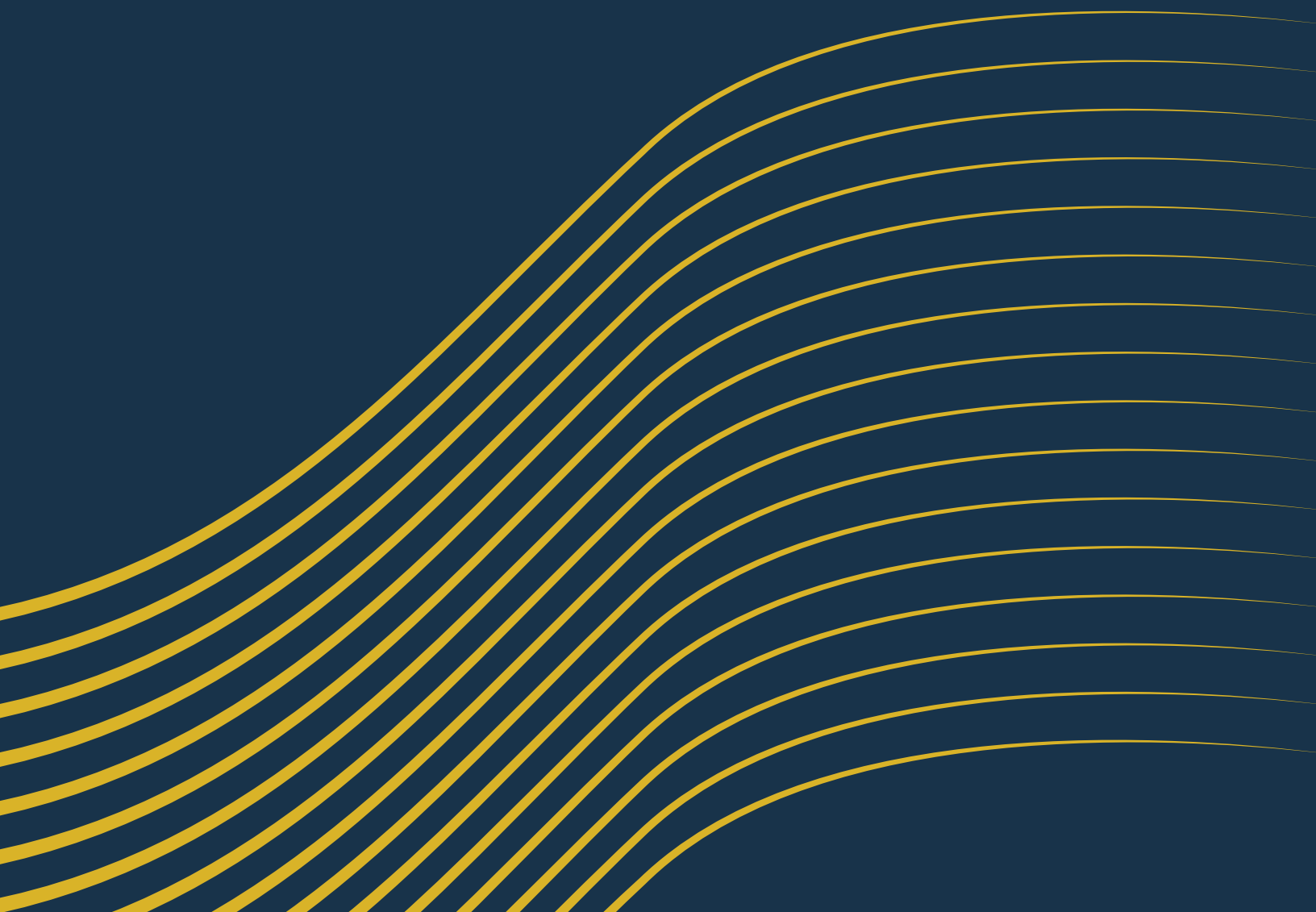
## **Request a Strategic Risk & Vendor Assessment**

Our team delivers high-impact consulting and operational intelligence for organizations ready to modernize, de-risk, and future-proof their security strategy.

### **Whether you're concerned about:**

- Foreign ownership exposure
- Vendor inconsistency across your portfolio
- Access control modernization
- Or simply building the business case for change

We can help.



**Corporate Headquarters** - 3300 Highlands Pkwy Suite 130 Smyrna GA, 30082  
ChesleyBrown.com | info@ChesleyBrown.com | (770) 436-3097