GMR SECURITY CONSULTING GROUP

PROTECT WHAT MATTERS MOST

EXECUTIVE BRIEFING

TOP PHYSICAL SECURITY TRENDS LEADING INTO 2027

A strategic outlook for corporate security leaders, enterprise executives and boards of directors.

November 2026

GMRSECURITY.COM

certified WBENC WOMEN'S BUSINESS ENTERPRISE

© 2026 GMR 410, LLC. All rights reserved.

Executive Summary

As organizations begin planning for 2027, security leaders face a complex operating environment: evolving threats to executives, heightened geopolitical uncertainty, technology convergence, increasingly sophisticated cyber-physical attacks, and greater expectations for measurable risk reduction.

The central executive challenge is no longer simply whether an organization has security controls in place. It is whether those controls are **intelligence-informed, risk-based, integrated, measurable, and resilient under adverse conditions.**

For large enterprises, particularly those operating in financial services, energy, healthcare, and other highly regulated sectors, GMR Security Consulting Group has identified the following eight trends.

1. **Executive targeting and workplace violence** are driving a reassessment of personnel protection.
2. **AI-enabled security and analytics** are changing detection, investigation, and operational decision-making.
3. **Cyber-physical convergence** is exposing vulnerabilities across connected security systems.
4. **Enterprise Security Risk Management (ESRM) and governance** are becoming central to demonstrating security program effectiveness.
5. **Geopolitical instability and targeted disruption** are influencing facility protection and business continuity.
6. **Integrated security operations** are replacing fragmented technology and operating models.
7. **Supply chain, third-party, and insider risks** are demanding broader visibility.
8. **Security performance measurement and resilience** are becoming critical executive accountability priorities.

The strategic implication is clear: organizations should move away from disconnected, compliance-driven security programs toward an integrated, intelligence-led model that connects people, facilities, technology, and business operations.

© GMR 410, LLC

1. Executive Targeting and Workplace Violence

Priority: Critical | Time Horizon: Immediate

The protection of senior executives, employees, and other high-profile individuals has become a more prominent corporate governance concern.

The emerging issue is not simply the physical threat to a CEO. It is the convergence of personal grievances, online exposure, public visibility, workplace conflict, and digital reconnaissance that can precede a physical incident.

A September 2026 analysis of S&P 500 disclosures found that the proportion of companies reporting personal security arrangements for their CEOs increased from 35% to 54% year over year. Approximately 47% also provided personal security to at least one additional named executive officer. Protection programs are increasingly incorporating digital privacy, residential assessments, and cyber-related safeguards. Harvard Law School

The EY 2026 physical security and crisis management survey also identified a significant readiness gap: only 12% of surveyed organizations said they felt prepared to detect a targeted attack against an executive or employee.

What Is Changing

- Executive protection is expanding beyond the CEO to other executives, board members, and individuals whose roles or visibility create elevated exposure.
- Residential security and off-site activities are receiving greater attention.
- Online threats, doxxing, personal information exposure, and hostile communications are increasingly relevant to physical protection.
- Workplace violence prevention requires closer collaboration among Corporate Security, HR, Legal, and behavioral threat assessment teams.
- Executive travel, public appearances, corporate events, and predictable routines require risk-based planning.

Executive Implications

Traditional executive protection programs may be too narrowly focused on transportation, protective agents, and physical security at corporate offices.

The stronger approach is a **risk-based executive protection program** integrating protective intelligence, threat assessment, residential security, digital exposure reduction, travel security, and incident response.

© GMR 410, LLC



A risk-based executive protection program integrates six protective components rather than focusing only on transportation and office security.

Recommended Actions for Q4 2026

1. Conduct individualized threat assessments for the CEO, board members, and other executives based on exposure, role, geography, and credible threats.
2. Assess residential security, executive travel, public appearances, and personal information exposure.
3. Establish a multidisciplinary threat management process involving Security, HR, Legal, and relevant business leaders.
4. Test escalation procedures for a credible threat against an executive or employee.
5. Establish clear criteria for increasing or decreasing protective measures as threat conditions change.

Board-level Question: Is the organization protecting executives based on documented risk, or primarily on organizational hierarchy and historical practice?

© GMR 410, LLC

2. AI-Enabled Physical Security and Intelligent Analytics

Priority: High | Time Horizon: Immediate to 12 Months

Artificial intelligence is moving from experimentation into operational security applications.

The opportunity is not merely to automate surveillance. It is to help security teams recognize meaningful events sooner, prioritize alarms, identify patterns, and make better-informed decisions.

The 2026 physical security industry research from Genetec found that interest in adopting AI among surveyed end users had more than doubled year over year. However, 70% expressed concerns about AI design and implementation, particularly data usage and transparency.

Where AI Is Creating the Most Strategic Value

Application	Potential Business Value	Executive Consideration
Video analytics	Identify unusual activity and events requiring attention	Validate accuracy and false-positive rates
Alarm prioritization	Help operators focus on higher-risk events	Ensure critical alarms are not suppressed
Investigative analytics	Reduce the time required to review video and incident records	Preserve evidence integrity and auditability
Risk intelligence	Identify patterns across incidents, locations, and external threats	Validate data quality and analytical assumptions
Access control analytics	Identify anomalous access patterns and potential misuse	Integrate with identity governance
Security operations support	Summarize incidents and help operators follow response procedures	Require human verification for consequential decisions

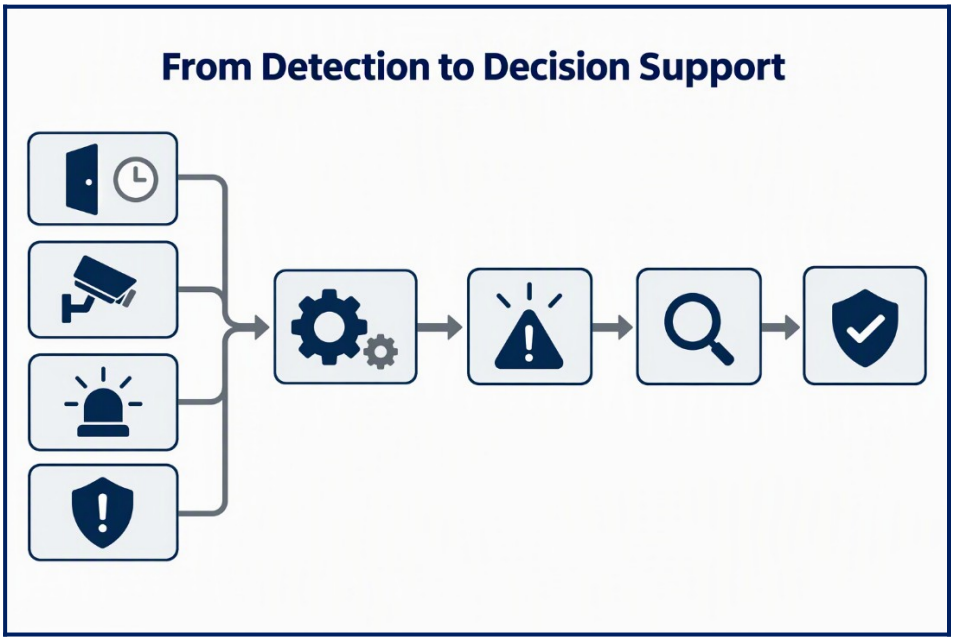
The Trend to Watch: From Detection to Decision Support

Organizations are moving toward systems that correlate multiple data sources rather than treating each camera, access reader, alarm, and incident as a separate event.

© GMR 410, LLC

For example, an after-hours access-control event might be correlated with video, alarm activation, and an existing threat notification to help an operator assess the situation more quickly.

This is a potential capability, not a guarantee of detection. Its effectiveness depends on system integration, data quality, configuration, and operator training.



Correlating access-control, video, alarm, and threat data (left to right) produces a prioritized alert for human verification before any response decision.

Key Risks

- False positives and missed detections.
- Biased or unreliable analytical outputs.
- Privacy, retention, and surveillance concerns.
- Overreliance on automated recommendations.
- Vendor claims that exceed demonstrated performance.
- AI-generated impersonation or manipulated media affecting security decisions.

© GMR 410, LLC

Recommended Actions for Q4 2026

1. Identify three to five high-value AI use cases tied to documented security risks.
2. Establish AI governance covering approved applications, data access, privacy, validation, and human oversight.
3. Require vendors to demonstrate performance against realistic operational scenarios.
4. Measure performance against a baseline before and after deployment.
5. Retain human authority for consequential security decisions.

Board-level Question: Can the company demonstrate that our AI investments reduce risk or improve operational effectiveness, rather than simply add technology?

---

3. Cyber-Physical Security Convergence

Priority: Critical | Time Horizon: Immediate

The traditional separation between physical security and cybersecurity is becoming increasingly difficult to defend.

Modern security environments rely on connected access control, video management, intrusion detection, building management, cloud platforms, remote maintenance, and centralized monitoring.

These connections create operational efficiencies, but they also introduce new pathways through which a digital compromise could affect physical protection or business continuity.

In April 2026, the Cybersecurity and Infrastructure Security Agency (CISA) and partner agencies published guidance on adapting Zero Trust principles to operational technology. The guidance emphasizes asset visibility, identity and access management, supply chain risk, segmentation, and the unique operational and safety constraints of OT environments.

In July 2026, CISA and international partners also issued guidance on isolating critical operational technology and enabling systems during a crisis.

© GMR 410, LLC

Why This Matters

Consider a hypothetical attack against a large financial institution.

An attacker compromises a third-party account used to maintain physical security systems. The attacker then attempts to disrupt monitoring, interfere with access-control operations, or exploit remote access to connected infrastructure.

The incident may begin as a cybersecurity problem but quickly becomes a physical security and business continuity issue.

The same principle applies to healthcare facilities, manufacturing sites, energy infrastructure, and data centers.

Executive Priorities

A. Establish joint ownership. Physical Security, IT, Information Security, Facilities, and OT teams should share responsibility for protecting connected security infrastructure.

B. Identify critical dependencies. Maintain an inventory of security systems, network connections, privileged accounts, remote-access pathways, and vendor dependencies.

C. Reduce unnecessary connectivity. Use appropriate network segmentation, secure authentication, least-privilege access, and controlled remote maintenance.

D. Prepare for degraded operations. Determine how facilities will maintain essential protective functions when networks, cloud services, or centralized monitoring are unavailable.

E. Test recovery. Exercise the loss of video monitoring, access-control services, communications, and critical building systems.

Recommended Action

Conduct a cyber-physical resilience assessment that examines not only whether systems can be compromised, but also how the organization would continue operating if essential security technology became unavailable.

Board-level Question: If the physical security technology were compromised or disconnected tomorrow, could we maintain safe and secure operations?

© GMR 410, LLC

4. ESRM, Governance, and Executive Accountability

Priority: Critical | Time Horizon: Q4 2026 Through 2027

Enterprise Security Risk Management (ESRM) is increasingly important because organizations need to demonstrate that security decisions are tied to business risks, assigned ownership, and measurable outcomes.

The challenge is not a shortage of security policies or technology. It is ensuring that the right people make the right decisions at the right time, with clear accountability for accepting and managing risk.

EY's May 2026 research found that 87% of surveyed organizations reported increased board oversight of physical security and executive protection over the preceding 12–18 months. Yet the research also identified fragmented responsibility across functions and gaps in crisis preparedness.

What Mature Security Governance Looks Like

A mature program connects five elements:

1. **Risk ownership:** Business leaders understand and own the risks associated with their facilities, people, and operations.
2. **Security standards:** Enterprise requirements establish minimum protective measures while allowing for site-specific risk.
3. **Decision rights:** Leaders know who can approve exceptions, accept residual risk, and authorize emergency actions.
4. **Performance measurement:** Management can evaluate control effectiveness, risk exposure, and program maturity.
5. **Assurance:** Testing, assessments, and corrective actions demonstrate whether the program is working as intended.

The Shift from Compliance to Performance

Compliance is necessary, but compliance alone does not demonstrate that a security program is effective.

A facility may satisfy a technical standard and still have material vulnerabilities because of staffing limitations, poor procedures, weak emergency coordination, or changes in its threat environment.

© GMR 410, LLC

Security leaders should therefore assess both control implementation and the residual risk remaining after controls are applied.

Recommended Actions for Q4 2026

- Refresh the enterprise physical security risk register.
- Map critical risks to accountable business owners.
- Establish an enterprise security governance committee with defined decision rights.
- Standardize facility risk assessments and minimum-security requirements.
- Implement a documented exception and risk-acceptance process.
- Report material risks, control deficiencies, and overdue corrective actions to executive leadership.
- Establish an annual assurance plan for critical security controls.

Board-level question: Can management demonstrate which physical security risks remain outside tolerance, who owns them, and what is being done to reduce them?

---

5. Geopolitical Risk, Targeted Disruption, and Critical Infrastructure

Priority: High to Critical | Time Horizon: Immediate Through 2027

Physical security planning increasingly needs to account for the relationship between geopolitical events, domestic tensions, public sentiment, and threats against corporate facilities.

Organizations may face exposure because of their industry, business decisions, government relationships, public profile, geographic footprint, or association with controversial issues.

The threat environment is not uniform. A financial institution, energy company, healthcare provider, and technology company will have different exposure profiles. The objective is to identify which external developments could create a credible threat to a specific organization.

The 2026 EY survey highlights growing attention to data centers, infrastructure sabotage, drone-related scenarios, executive targeting, and global uncertainty.

© GMR 410, LLC

Trends Security Leaders Should Monitor

1. Targeted protests and grievance-driven activity

Corporate locations may become focal points for protests, intimidation, vandalism, or disruption. Security teams should distinguish lawful demonstrations from credible indicators of violence or targeted criminal activity.

2. Threats to critical facilities

Energy infrastructure, data centers, healthcare facilities, financial institutions, and logistics networks may face threats that extend beyond conventional property crime.

3. Drone-related security concerns

Unmanned aircraft can create safety, surveillance, and operational concerns around sensitive facilities. Organizations should evaluate site-specific exposure, applicable aviation rules, and lawful detection and response options.

4. Geopolitical spillover

International developments can affect domestic operations through protests, threats against personnel, disruptions to supply chains, and risks to employees traveling or working abroad.

Recommended Actions

- Refresh threat assessments for high-consequence and high-visibility locations.
- Develop a process for translating geopolitical and open-source intelligence into site-specific risk decisions.
- Evaluate perimeter protection, surveillance, incident reporting, and emergency procedures.
- Establish escalation criteria for credible threats, targeted protests, and potential disruptions.
- Coordinate with Legal, Communications, Government Affairs, and Business Continuity.
- Exercise scenarios involving simultaneous threats at multiple locations.

Executive Takeaway: Geopolitical intelligence is valuable only when it informs specific protective measures, operational decisions, and contingency plans.

© GMR 410, LLC

6. Integrated Security Operations and Technology Modernization

Priority: High | Time Horizon: 6–18 Months

A major industry trend is the movement away from fragmented security technology toward integrated platforms, common operating procedures, and more coordinated decision-making.

Many large enterprises still operate separate systems for video surveillance, access control, intrusion detection, visitor management, guard operations, threat intelligence, and executive protection.

These systems may each work adequately in isolation but fail to provide a coherent operational picture.

The 2026 industry research from Genetec identifies stronger integration, deployment flexibility, AI, and closer collaboration between physical security and IT as important developments.

What the Next-Generation Operating Model Looks Like

An integrated security operations model connects:

- Video management and analytics.
- Access control and identity systems.
- Intrusion detection and alarm management.
- Global Security Operations Center (GSOC) capabilities.
- Threat intelligence and case management.
- Executive protection and travel risk.
- Regional security operations and contract guard services.
- Emergency management and business continuity.

The objective is not necessarily to purchase one platform that does everything.

Instead, the goal is to create a **common operating picture, consistent workflows, and reliable information exchange across systems and teams.**

© GMR 410, LLC

Three Modernization Priorities

A. Standardize before integrating.

Establish common definitions for incidents, alarms, facility criticality, escalation, and reporting before connecting systems across the enterprise.

B. Prioritize interoperability.

Use open interfaces and documented integration requirements where practical. Avoid creating unnecessary dependence on a single vendor or technology stack.

C. Modernize based on risk.

Prioritize facilities where obsolete technology, operational importance, incident history, or threat exposure creates the greatest potential consequence.

Recommended Actions

For 2027, develop a multi-year security technology roadmap that includes:

1. An enterprise inventory of security technologies and their dependencies.
2. A current-state maturity assessment.
3. A target architecture and integration strategy.
4. A prioritized modernization plan.
5. Cybersecurity, privacy, and vendor risk requirements.
6. Defined operational benefits and performance measures.
7. A lifecycle replacement and maintenance strategy.

Executive Takeaway: Technology integration should improve the organization's ability to detect, assess, communicate, and respond to incidents, not simply create a more sophisticated technical environment.

---

7. Third-Party Risk, Insider Threats, and Supply Chain Security

Priority: High | Time Horizon: Q4 2026 Through 2027

Enterprise security risk extends beyond employees and company-owned facilities.

© GMR 410, LLC

Contractors, maintenance providers, security integrators, logistics partners, temporary workers, and other third parties can create vulnerabilities through their access to people, buildings, systems, and sensitive operations.

The challenge is particularly significant for organizations with large facility portfolios, distributed operations, and complex vendor ecosystems.

Research published in February 2026 by McGrathNicol highlighted the need for a more coordinated approach to physical security, personnel security, and supply chain exposure.

Three Areas Requiring Greater Attention

Third-party access

Organizations should understand who can access critical facilities, which privileges they possess, when access is authorized, and how promptly those privileges are removed.

Insider risk

Insider risk management should consider malicious activity, coercion, conflicts of interest, policy violations, and inadvertent actions that could compromise people, assets, or operations.

Vendor and technology dependencies

A security technology provider or maintenance contractor may have privileged access to systems that protect multiple facilities.

The organization should understand these dependencies and establish controls appropriate to the potential consequences of a compromise.

Recommended Actions

- Review third-party access to critical facilities and security systems.
- Validate the authorization and periodic recertification of privileged access.
- Coordinate behavioral threat assessment with HR and Legal under appropriate privacy and employment safeguards.
- Include physical security requirements in vendor onboarding and contract management.
- Assess the security implications of vendor remote access and subcontractor relationships.
- Establish rapid access revocation and offboarding procedures.

© GMR 410, LLC

- Exercise incidents involving compromised contractor credentials or insider-enabled access.

Executive Takeaway: Your security perimeter increasingly includes people and organizations that your company does not directly employ or control.

---

8. Security Metrics, Workforce Effectiveness, and Organizational Resilience

Priority: High | Time Horizon: Immediate Through 2027

Security leaders are under increasing pressure to demonstrate the value of security investments while managing staffing challenges, operational complexity, and competing budget priorities.

The opportunity is to move beyond activity-based reporting toward measures that demonstrate risk reduction, control effectiveness, operational readiness, and business resilience.

The 2026 World Security Report from AlliedUniversal identifies workforce recruitment and retention as continuing challenges for security organizations, even as technology investment and the strategic importance of security increase.

The Problem with Traditional Security Reporting

A dashboard showing the number of cameras installed, guards deployed, alarms investigated, or training sessions completed may be useful operationally.

However, those numbers do not necessarily demonstrate that the organization is safer.

For example, a high number of incidents closed does not establish whether incidents were prevented, response times improved, or underlying vulnerabilities were corrected.

Recommended Executive Scorecard

Measurement Category	Example KPI	Executive Value
Risk exposure	Percentage of critical facilities with current risk assessments	Shows visibility into enterprise risk

© GMR 410, LLC

Measurement Category	Example KPI	Executive Value
Control effectiveness	Percentage of critical controls that pass testing	Demonstrates whether controls work
Remediation	Percentage of high-risk findings remediated within target time	Measures risk reduction
Incident response	Time from verified detection to appropriate escalation	Measures operational responsiveness
Threat management	Percentage of high-priority threats assessed within required time	Measures threat-management discipline
Workforce readiness	Percentage of critical posts meeting staffing and qualification requirements	Identifies operational coverage gaps
Crisis preparedness	Percentage of critical facilities completing required exercises	Measures preparedness
Technology resilience	Percentage of critical security systems meeting availability and recovery requirements	Measures continuity of protection
Financial stewardship	Cost and risk reduction associated with priority security initiatives	Supports investment decisions
Governance	Percentage of material security risks with documented owners and treatment plans	Measures accountability

These are suggested measures, not universal benchmarks. Targets should be established using the organization's risk appetite, operating environment, baseline performance, and applicable requirements.

The Workforce Dimension

Automation can improve the efficiency of security operations, but it does not eliminate the need for trained personnel who can interpret information, exercise judgment, communicate clearly, and respond appropriately.

© GMR 410, LLC

Security leaders should assess whether their workforce has the skills needed for integrated operations, technology-enabled investigations, threat assessment, crisis management, and risk-based decision-making.

Recommended Actions

- Establish an executive security scorecard.
- Link significant investments to documented risks and measurable outcomes.
- Develop competency requirements for critical security roles.
- Review staffing resilience, succession planning, and training.
- Conduct realistic exercises and track corrective actions.
- Report material residual risks and remediation progress to leadership.

Executive Takeaway: A mature security program should be able to demonstrate not just what it does, but how effectively it reduces risk and supports business continuity.

---

9. The Cross-Cutting Issue: Crisis Management and Enterprise Resilience

Although resilience appears throughout the eight trends, it deserves separate consideration because it is where weaknesses in governance, technology, intelligence, and operations often become visible.

Organizations can have strong individual security controls and still struggle when an incident crosses organizational boundaries.

A credible threat against an executive might require coordinated decisions by Corporate Security, HR, Legal, Communications, executive leadership, and law enforcement.

A cyberattack affecting access-control systems could require IT, Facilities, Security Operations, and business continuity teams to coordinate while maintaining safe operations.

A disruptive event at one location could require the GSOC to coordinate information and protective measures across multiple regions.

EY's May 2026 research identified fragmented crisis decision-making and limited preparedness for some high-consequence scenarios. Its findings reinforce the need to test

© GMR 410, LLC

not just response procedures, but also decision authority and cross-functional coordination.

What Organizations Should Do Differently

Move beyond tabletop exercises that simply review a plan. Use realistic exercises to test:

- Decision-making under time pressure.
- Escalation and notification procedures.
- Coordination between corporate and regional teams.
- Communications failures and unavailable technology.
- Executive protection during an emerging threat.
- Continuity of essential security functions.
- Recovery, investigation, and post-incident accountability.

Each exercise should produce documented findings, accountable owners, deadlines, and follow-up validation.

Executive Takeaway: Resilience is demonstrated by the organization's ability to maintain essential functions, make sound decisions, and recover—not merely by the existence of a crisis management plan.

---

10. Executive Priority Matrix: Where to Invest Attention

For a large enterprise entering 2027, prioritize initiatives according to potential consequences, existing control maturity, and the organization's specific threat exposure.

The following is a recommended planning framework, not a claim that every organization faces identical risks.

Strategic Priority	Next 30 Days	Next 90 days	2027 Objective
Executive protection	Review executive threat exposure and existing protective measures	Close material gaps in residential, travel, and digital protection	Establish a risk-based, continuously reviewed program
Workplace	Review threat reporting	Test coordination	Establish an integrated

© GMR 410, LLC

Strategic Priority	Next 30 Days	Next 90 days	2027 Objective
violence	and escalation procedures	among Security, HR, and Legal	threat management capability
Cyber-physical security	Identify critical connected systems and dependencies	Assess remote access, segmentation, and degraded operations	Implement a cyber-physical resilience program
Security governance	Review the enterprise risk register and risk ownership	Establish executive reporting and risk acceptance procedures	Embed security into enterprise risk governance
AI and analytics	Inventory existing AI applications and proposed use cases	Validate priority use cases and establish governance	Scale proven applications with measurable benefits
Technology integration	Assess the current technology architecture	Define the target architecture and prioritized roadmap	Modernize critical systems through risk-based investment
Third-party risk	Review privileged vendor access and critical dependencies	Address high-risk access and contract deficiencies	Integrate third-party security into enterprise risk management
Performance and resilience	Establish baseline metrics and review exercise history	Test critical scenarios and remediate priority findings	Demonstrate sustained improvement in risk reduction and readiness

Three Principles for Prioritization

First, address material exposures before pursuing broad technology transformation. An organization with significant gaps in executive protection, access governance, or crisis readiness should not allow an ambitious technology roadmap to displace urgent risk reduction.

Second, distinguish enterprise-wide standards from site-specific controls. A high-consequence facility may warrant different protective measures from a low-risk administrative office.

Third, treat risk acceptance as a management decision. Security should advise on risk and recommend treatment, while designated business owners should accept residual risk within established governance and authority limits.

© GMR 410, LLC

11. Sector-Specific Considerations

Although the trends are broadly applicable, their implications vary by industry.

Sector	Physical Security Priorities	Key Executive Consideration
Financial Services	Executive protection, branch and office security, insider risk, cyber-physical resilience, vendor access	Protect people and critical services while maintaining operational continuity
Energy and Utilities	Critical infrastructure protection, OT dependencies, perimeter security, remote sites, sabotage preparedness	Maintain safe operations when security or enabling systems are disrupted
Healthcare	Workplace violence, emergency department security, access management, insider risk, emergency preparedness	Protect patients and staff without impeding essential care
Technology and Data Centers	Perimeter protection, access governance, insider risk, drone-related concerns, infrastructure resilience	Protect high-consequence assets and maintain service availability
Manufacturing and Logistics	Site access, cargo and supply chain security, contractor management, operational continuity	Prevent disruptions across interconnected facilities and supply networks
Corporate Headquarters	Executive protection, threat assessment, visitor management, workplace violence, crisis coordination	Integrate employee safety, executive protection, and business continuity

The correct investment profile should reflect each organization's risk assessment, operating model, geographic exposure, and legal obligations.

---

12. What Should Be on the Board's Agenda Before Year-End?

The Chief Security Officer should present a concise briefing organized around five questions.

1. What has materially changed in our threat environment?

© GMR 410, LLC

Identify significant changes in threats to executives, employees, facilities, and operations. Distinguish credible, organization-specific risks from general media attention.

2. Where are we most exposed?

Present the highest-consequence risks, critical control deficiencies, and locations where existing safeguards do not adequately reduce risk.

3. How prepared are we to respond?

Explain what recent exercises and assessments reveal about decision-making, escalation, coordination, and recovery.

4. What investments are required?

Present a prioritized plan distinguishing immediate remediation, strategic modernization, workforce requirements, and longer-term capability development.

5. How will we demonstrate improvement?

Define the measures that management will use to assess risk reduction, control effectiveness, remediation progress, and operational resilience.

A useful board presentation should make clear which risks are within tolerance, which require treatment, which need executive decisions, and which require formal acceptance of residual risk.

---

13. Recommended Strategic Outlook for 2027

GMR Security Consulting Group's assessment is that five capabilities will distinguish more mature physical security programs from those that remain primarily reactive.

1. Integrated protective intelligence

The ability to connect external threat information, internal incident data, executive exposure, and facility risk assessments to inform protective decisions.

2. Risk-based enterprise governance

A defined framework that establishes accountability, risk ownership, minimum standards, exception management, and executive oversight.

3. Cyber-physical resilience

© GMR 410, LLC

The ability to protect connected systems and sustain essential security functions during technology disruptions or cyber incidents.

4. Measurable security performance

A consistent way to demonstrate that investments and controls reduce exposure, improve readiness, and support operational continuity.

5. Adaptive operating models

The ability to adjust protective measures, staffing, technology, and response procedures as the threat environment changes.

These capabilities reinforce one another. Intelligence without governance may not produce action. Technology without trained operators may not improve outcomes. Controls without testing may create false confidence. And a risk assessment without accountable owners may not lead to meaningful remediation.

The strategic objective should therefore be to build an operating model in which these capabilities work together.

Final Executive Assessment

As organizations plan their security budgets for 2027, the most important development is the continued evolution of physical security from a facility-focused protective function into an enterprise capability responsible for managing interconnected risks to people, assets, information, and operations.

The latest industry research supports several important conclusions:

- Board attention and investment are increasing, but preparedness and accountability remain inconsistent.
- Executive protection is expanding beyond traditional physical measures to include digital exposure and broader personal risk.
- AI adoption and integrated security technology are advancing, while governance, privacy, and operational validation remain important considerations.

© GMR 410, LLC

- Cyber-physical dependencies require organizations to plan for disruption and preserve essential functions, not simply prevent unauthorized access.

GMR Security's Top Three Recommendations for Chief Security Officers

1. Conduct an enterprise-wide physical security risk and readiness review before year-end. Focus on executive targeting, workplace violence, critical facilities, cyber-physical dependencies, and crisis response.

2. Establish a measurable security governance framework for 2027. Assign risk owners, standardize reporting, define risk acceptance authority, and link investments to documented business risks.

3. Prioritize resilience over technology acquisition alone. Invest in integrated intelligence, interoperable systems, trained personnel, and realistic exercises that demonstrate the organization's ability to respond and recover.

The ultimate measure of a mature physical security program is not how much technology it deploys, how many guards it employs, or how many policies it publishes.

It is whether the organization understands its most significant risks, makes informed decisions about those risks, and can demonstrate that its people, facilities, and critical operations remain protected when conditions deteriorate.

That is the standard physical security leaders should be working toward as they enter 2027.

About GMR Security Consulting Group

GMR Security Consulting Group (legal name GMR 410, LLC) delivers independent, proven and expert-driven physical security consulting tailored to the specific needs of each client. We are a trusted team of experienced professionals providing strategic solutions and operational support to help you protect what matters most. We believe robust security should be accessible, proactive, and transparent, because serving our clients is at the heart of everything we do. Our services range from risk assessments to program development, embedded services, and executive recruiting.

Founded in 2019, GMR Security Consulting Group is headquartered in Heath, Texas and serves clients globally across high-risk sectors including finance, healthcare, education, and critical infrastructure.

© GMR 410, LLC

Why GMR Security Consulting Group?

Industry-Leading Expertise: Our credentialed professionals bring decades of experience, delivering proactive strategies that mitigate risks before threats emerge.

Independent and Unbiased: As a vendor-neutral firm, our recommendations are based solely on what is best for our clients, never influenced by product affiliations.

Client-Centric Approach: We tailor every engagement to your unique risks and goals, building long-term partnerships that evolve with your organization.

Collaborative Partnership: We work as an extension of your team, educating stakeholders, managing projects, and delivering clear, actionable security solutions.

Contact Us

www.gmrsecurity.com

contact@gmrsecurity.com

(504) 228-4829

© GMR 410, LLC