CSA

THE BUSINESS OF SECURITY™

HEALTHCARE SECURITY GOVERNANCE IMPERATIVE

Twelve Questions for Boards and Executive Leaders to Build Safer, More Accountable Health Systems

REPORT

We did not set out to write a governance report.

What we set out to do — what we have done, across decades of work in healthcare security, corporate security, law enforcement, and clinical operations — is help organizations protect the people inside them.

That work has taken us into emergency departments and executive suites, into facilities that had never written a security policy and systems that had spent millions on technology no one was governing. It has put us in front of boards that did not know what questions to ask, and security leaders who could not get a meeting with their own CFO.

Over time, a pattern became impossible to ignore. The organizations struggling most with physical security were not struggling because of bad people or bad intentions. They were struggling because of bad structure. Security was buried too low, funded too reactively, led without the executive competencies the role demands, and governed without the rigor applied to every other function the board considered essential. The same gaps appeared in system after system, regardless of size, geography, or resources. And the same improvements became possible when those gaps were addressed.

That pattern is what this report documents. The twelve questions it examines are not theoretical — they are the questions we have asked, and been asked, in real engagements with real organizations. The evidence it draws on reflects what we have seen work, and what we have seen fail. The voice throughout is our team's: practitioners who have led security functions at McKesson, Target, Walmart, Kaiser Permanente, and the FBI; who have built programs from the ground up and rebuilt them after crises; who have sat at board tables and on the front lines of the functions those boards are responsible for governing.

Our hope is that this report gives healthcare leaders — CEOs, CNOs, CMOs, board members, and the security professionals who serve them — a framework for the conversations that need to happen. Physical security in healthcare is at an inflection point. The regulatory environment is tightening. The financial and human cost of inaction is quantified and growing. And the governance model that would close the gap already exists in an adjacent domain: most healthcare boards have spent the last decade building exactly the oversight architecture for cybersecurity that physical security has been waiting for.

The path forward is clearer than most organizations realize. We wrote this report because we believe that clarity matters — and because the people working in healthcare deserve the protection that a well-governed security program provides.

INTRODUCTION

This report examines physical security governance in healthcare through twelve questions drawn from CSA's direct experience leading security transformations across major health systems. Each question is framed for C-suite leaders and board members — the people whose decisions determine whether physical security operates as a strategic capability or an operational afterthought.

The questions are organized to follow the logic of governance itself. The first four address the architecture: why physical security belongs on the board agenda, how the function should be structured, what the security leadership role actually requires, and who owns accountability when something goes wrong. The next three address the enterprise dimensions: consistency across a multi-facility system, technology governance, and investment discipline. The final five address program depth: building and retaining the right team, measuring what actually matters, breaking down the silos that undermine integrated safety, preparing for the crises that will come, and defining what security excellence looks like for the organization.

Each chapter stands alone. Readers may move directly to the questions most relevant to their current priorities. Those who read the report in sequence will find that the chapters build on each other — governance without structure is aspiration; structure without leadership is architecture without occupants; leadership without accountability is authority without consequence. The questions are connected because the challenges they address are connected.

A note on the evidence. The findings in this report draw on three sources: CSA's direct client experience across healthcare systems of varying size and complexity; the published standards and guidelines of the field's leading professional bodies, including ASIS International, the International Association for Healthcare Security and Safety, and the Joint Commission; and current data on the financial and human cost of workplace violence in healthcare, including the American Hospital Association's 2025 analysis estimating the total cost of violence to U.S. hospitals at $18.27 billion annually. Where the evidence points in a single direction, we have said so plainly. Where the path requires judgment, we have tried to equip the reader to exercise it.

The goal of this report is not to prescribe a single model. Healthcare organizations differ in size, structure, governance, and risk profile. What works at a 40-hospital integrated system will not translate unchanged to a single community hospital. What is universal is the governance discipline that effective security requires — and the questions that reveal whether that discipline is present. Those questions are the starting point for every conversation this report is designed to support.

EXECUTIVE SUMMARY

Physical security has always been a board-level responsibility. Patient safety, staff welfare, and the protection of organizational assets carry fiduciary weight, regulatory consequence, and reputational exposure. Yet in most healthcare systems, physical security has been managed operationally, funded reactively, and governed inconsistently — if governed at all.

That gap between principle and practice is no longer sustainable. In 2023, the total financial cost of violence to U.S. hospitals reached an estimated $18.27 billion — a figure the American Hospital Association describes as largely conservative. Healthcare workers are five times more likely to suffer workplace violence than workers in any other industry. The regulatory floor is rising: California, New York, and eight additional states have enacted healthcare-specific workplace violence protections, federal legislation is advancing, and the Joint Commission classifies every assault on hospital premises as a reviewable sentinel event. For boards, the question is no longer whether physical security belongs on the agenda. It is how quickly the distance between current state and actual need can be closed.

This report examines that distance through twelve questions drawn from CSA's direct experience leading security transformations across major healthcare systems. The questions are framed for C-suite leaders and board members. The answers, taken together, describe both the current state of physical security governance in healthcare and the path to a materially better one.

The governance architecture

The first four questions address the governance architecture that every other executive function takes for granted. Why is physical security on the board agenda now? Because the regulatory environment, financial exposure, and workforce consequences have converged to demand it — and because the governance model boards need already exists. Over the past decade, healthcare boards built sophisticated governance frameworks for cybersecurity: dedicated committees, regular risk reporting, defined accountability, and strategic investment. Physical security now faces the same set of drivers. The capability gap is not about building something new. It is about applying proven governance disciplines to a domain that has been waiting for them.

Is the security function structured for success? In most healthcare systems, security is buried within facilities management, plant operations, or nursing departments whose primary mission lies elsewhere. That organizational position is not a neutral administrative choice — it shapes what the function can accomplish, what resources it receives, and whether it has a voice in the conversations where risk decisions are made.

EXECUTIVE SUMMARY

Structure is a governance decision. The question is whether the current structure gives security the authority and cross-functional access to fulfill the role that regulators, accreditors, and industry standards already define for it.

Is the security leader set up to succeed? The ASIS International Chief Security Officer standard is clear: strategic, business, and interpersonal competencies are of greater importance than technical security skills. Business acumen has been described as the "nuclear element" of the role — the competency without which the others cannot be fully effective. Healthcare applies this principle to every other executive function. A Chief Financial Officer is not hired for bookkeeping skill; a Chief Nursing Officer is not selected on bedside experience alone. The security leader deserves the same standard — and the organization that sets that standard will find that a stronger leader at the top transforms the function at every level below.

Who is accountable when something goes wrong? The instinctive answer — the security department — is the wrong one. Management owns the risk. The security leader identifies it, assesses it, and recommends mitigation. The decision to accept, transfer, or address that risk belongs to operational leaders and, ultimately, to the board. When accountability is unclear, organizations create the conditions for exactly the failures they are trying to prevent. Building an accountability architecture — documented risk decisions, defined escalation paths, regular board reporting — is the governance foundation on which every other security improvement depends.

The enterprise challenge

The next three questions address the enterprise dimensions of security governance: consistency, technology, and investment. Multi-facility health systems are assembled through decades of acquisitions and organic growth. The result, in most cases, is not one security program but dozens of variations — different technologies, different procedures, different cultures, none of them reconciled into a coherent enterprise approach. When one large health system finally consolidated its security spending data, leadership discovered it was investing $11.5 million annually, not the $2–3 million assumed. An additional $21 million in technology assets sat unbooked on facility balance sheets. Enterprise consistency is not an operational afterthought. It is a governance requirement: when a board approves a security strategy, it is approving it for the entire organization.

Are we governing the technology we have? Healthcare organizations are spending millions on cameras, access control, and visitor management systems. The question most boards have never asked is whether any of it is working. Technology without governance, strategy, and operational integration produces investment without accountability. One health system invested $1.5 million in cameras with no one assigned to monitor them and no capacity to retain footage. Another installed $5,000 keypads with the access codes written on the keypads themselves. These are not technology failures. They are governance failures expressed through technology. The organizations that extract real value from security technology treat it the way they treat every other enterprise technology investment: with lifecycle management, defined operating protocols, and measurable outcomes.

EXECUTIVE SUMMARY

Are we investing wisely? Most healthcare organizations cannot answer that question — because they cannot answer the one before it: what are we actually spending? Security investment requires the same discipline applied to every other enterprise function. A security master plan that sequences investment against risk, links spending to measurable outcomes, and speaks the language of the CFO and board is not a luxury. It is the mechanism that transforms security from a cost to be controlled into a capability to be developed. The business case already exists in data the organization is already tracking: turnover rates, workers' compensation claims, staff satisfaction scores, and the $18.27 billion industry-wide cost of violence that prevention spending directly offsets.

Program depth

The final group of questions addresses the depth of the security program itself: the people who deliver it, the metrics that evaluate it, and the cross-functional integration that sustains it. Healthcare security faces a structural workforce challenge. The role demands empathy, de-escalation skill, sound judgment under pressure, and the ability to engage constructively with patients in crisis — qualities that entry-level wages and minimal development investment do not attract or retain. The organizations that have broken this cycle share a common insight: hire for character and clinical alignment, then teach security. Structured onboarding, simulation-based training, individual development plans, and genuine career pathways have reduced security officer turnover from 25–30 percent to under 10 percent at health systems that applied the same organizational development discipline to security that they routinely apply to clinical teams.

Healthcare has spent decades building sophisticated measurement systems for clinical quality. Physical security has no equivalent. Most security reports measure activity, not effectiveness — incident counts that tell leadership how busy the team is, not whether the organization is becoming safer. The organizations building mature security programs apply the same evidentiary standard to security reporting that boards already apply to clinical quality: categorization, trending, root cause analysis, leading and lagging indicators, and comparison to benchmarks. When security metrics appear alongside clinical quality and financial performance in board dashboards, they receive the same accountability and the same expectation of continuous improvement.

In most healthcare organizations, security, human resources, and clinical operations only interact when something has already gone wrong. The functions that most directly affect staff safety — security, HR, clinical leadership, compliance, and risk management — typically operate under separate reporting structures with limited visibility into each other's work. The model that works is not organizational convergence but deliberate alignment: shared governance, joint training, common incident reporting, and a standing multidisciplinary threat assessment team that evaluates behavioral concerns before they escalate. When security is integrated into the fabric of clinical operations — present in safety huddles, involved in root cause analysis, partnered with HR on workforce issues — the program improves continuously rather than reactively.

EXECUTIVE SUMMARY

Preparedness and excellence

Every healthcare organization has an emergency management plan. Most have conducted tabletop exercises. The gap between having a plan and having the capability to execute it under pressure is where most programs fail. Preparedness is not a document — it is a set of organizational capabilities that must be built, tested, and maintained. The organizations that are genuinely prepared are the ones whose last crisis exercise revealed something unexpected: a gap no one had anticipated, a protocol that dissolved under pressure, a communication pathway that failed. Preparedness, like clinical quality, requires investment, accountability, and the expectation of continuous improvement.

Security excellence in healthcare is not a destination. It is a governed process of continuous improvement — the same discipline that clinical leaders recognize from quality improvement, patient safety, and high-reliability organizing. It begins with a board decision: to hold physical security to the same governance, investment, and performance standards the organization already applies to every other function it considers essential. Clinical quality, patient experience, financial stewardship, regulatory compliance, and cybersecurity all operate under that standard. Physical security can and should meet it.

The starting point

The starting point is not a technology purchase, a staffing increase, or a policy revision. It is a leadership decision to ask the question that most healthcare executives have never put to their security leader: where are we going, how will we get there, and how will we know when we've arrived?

The frameworks exist. The evidence base is established. The expertise is available. The organizations that close the governance gap in physical security will be better positioned to protect their people, satisfy their regulators, and demonstrate the standard of care that patients, staff, and communities rightly expect.

CSA

THE BUSINESS OF SECURITY™

QUESTION 1 *of 12*

WHY IS PHYSICAL SECURITY ON OUR BOARD AGENDA NOW?

CSA HEALTHCARE SECURITY GOVERNANCE REPORT

WHY IS PHYSICAL SECURITY ON OUR BOARD AGENDA NOW?

Physical security has always been a board-level responsibility. Patient safety, staff welfare, and the protection of organizational assets are governance concerns by definition — they carry fiduciary weight, regulatory consequence, and reputational exposure. Yet for many healthcare systems, physical security has not received the strategic attention that its importance warrants. It has been managed operationally and funded reactively, governed inconsistently if governed at all.

That gap between principle and practice is no longer sustainable. Expanding regulation, escalating workplace violence, and hard lessons from cybersecurity governance are converging to place physical security firmly on the boardroom agenda. The question for healthcare leaders is not whether it belongs there, but how quickly the distance between current state and actual need can be closed.

Organizations that invest strategically in physical security — not as a cost to be minimized but as a capability to be governed — see measurable returns. A well-integrated security program reduces disruption to clinical operations, lowers workers' compensation exposure, supports staff retention, and contributes to the stable operating environment that every other strategic initiative depends on. The case for board attention therefore is not only about mitigating risk. It is about enabling the organization to function at its best.

The regulatory landscape

Healthcare security operates within an increasingly defined regulatory environment. The Joint Commission's environment of care standards require hospitals to maintain programs that address safety and security risks. Its sentinel event framework goes further: Every instance of assault, sexual abuse, or homicide on hospital premises is classified as a reviewable event, triggering mandatory root-cause investigation and corrective action subject to Joint Commission review. In 2024, 65 workplace violence-related sentinel events were reported — a figure widely believed to be a significant under-reporting given that submission is voluntary.

The Centers for Medicare and Medicaid Services tie security-related requirements to Conditions of Participation, the standards that determine eligibility for federal reimbursement. Non-compliance puts Medicare and Medicaid revenue at risk — a consequence boards understand immediately. OSHA's General Duty Clause adds a further layer of employer obligation, requiring workplaces free from recognized hazards likely to cause serious harm.

At the state level, legislative action has accelerated markedly. California's SB 553, effective 2024, established the first general industry workplace violence prevention standard. Nine additional states — New York, Connecticut, Minnesota, Illinois, Oregon, Washington, Maine, Maryland, and New Jersey — have enacted or strengthened healthcare-specific protections. At the federal level, the bipartisan Save Healthcare Workers Act (H.R. 3178/S. 1600), introduced in May 2025 with AHA support, would make assaulting an on-duty hospital worker a federal crime punishable by up to ten years' imprisonment. The trajectory is clear: the regulatory floor is rising, and organizations that treat compliance as their ceiling will find themselves exposed.

WHY IS PHYSICAL SECURITY ON OUR BOARD AGENDA NOW?

What the data tells us

The scale of this challenge is quantified with a precision that demands board-level attention. In June 2025, the AHA published The Burden of Violence to U.S. Hospitals, prepared by the University of Washington's Harborview Injury Prevention and Research Center. The headline finding: the total financial cost of violence to U.S. hospitals in 2023 was an estimated $18.27 billion.

$18.27 Billion.

— FOR EVERY —

$1 spent on prevention, $4 is spent responding.

Total financial cost of violence to U.S. hospitals in 2023. Of $3.62B in prevention spending and $14.65B in post-event costs, the 4:1 ratio reflects a system structured to react, not prevent. — AHA, The Burden of Violence to U.S. Hospitals (2025)

That imbalance is not a reflection of how much organizations care about their people. It is a reflection of how security investment has historically been structured: reactively, in response to incidents, rather than strategically, in pursuit of prevention. What's more, the report's authors noted that their estimates were "largely conservative," suggesting the actual burden is higher still.

Bureau of Labor Statistics data reinforces the picture. Healthcare workers are five times more likely to suffer workplace violence injuries than workers in other industries, with nurses, nursing assistants, and emergency department staff bearing disproportionate risk. The AHA report estimated $541 million in staffing-related costs from the non-physical effects of violence alone — the absenteeism, lost productivity, and increased turnover that follow exposure to violent incidents. In an industry already navigating a workforce crisis, these are not secondary concerns.

The inverse is equally important. Organizations that shift from reactive spending to governed, prevention-oriented investment redirect resources from the costliest part of the cycle toward the most effective. The business case is not about spending more on security. It is about spending differently — and measuring the return in reduced incident rates, lower compensation claims, improved retention, and uninterrupted clinical operations.

WHY IS PHYSICAL SECURITY ON OUR BOARD AGENDA NOW?

"Every board regularly discusses cyber security issues now. Almost none make an equivalent investment of time in physical security."

Ken Senser, CSA Chief Strategy Officer • Former Walmart Chief Security Officer

The governance gap that boards already know how to close

That observation identifies both the problem and its solution. Over the past decade, boards have built sophisticated governance structures for cybersecurity: dedicated committees, regular risk reporting, defined accountability, and strategic investment frameworks. They did this because regulatory pressure, high-profile incidents, and litigation risk made cyber a board-level concern. Physical security now faces the same set of drivers — but most healthcare boards have not yet extended their governance frameworks to match.

The good news is that the model already exists. The governance architecture boards have constructed for cybersecurity translates directly to physical security. The capability gap is not about inventing something new. It is about applying proven governance disciplines to a domain that has been waiting for them.

Where security sits shapes what security does

Brad Brekke, CSA's Chief Business Officer and former Vice President of Assets Protection and Corporate Security at Target Corporation, frames the board's exposure directly: "If boards understood their exposure on physical security the way they understand it on cyber, this conversation would be very different."

Part of the reason that conversation has been slow to develop is structural. In many healthcare systems, physical security reports through facilities management, plant operations, nursing, environmental services, or other functions whose primary mission is not security. When security is subordinated to a department with different priorities, it is inevitably shaped by those priorities. It becomes an operational line item rather than a strategic capability — resourced to respond to incidents rather than to prevent them and rarely represented in the conversations where risk decisions are made.

"Most healthcare systems don't have a security strategy. They have a collection of reactions."

Jeremy Baumann, CSA Chief Executive Officer

That distinction matters. A collection of reactions, however well-intentioned, cannot deliver the consistency or accountability that governance requires. Reactions are backward-looking by definition. Strategy is forward-looking — it anticipates risk, allocates resources against priorities, and creates the framework within which operational decisions can be made, measured, and improved. The question of where security sits, who it reports to, and what it is empowered to do is ultimately a question about how the organization governs risk.

The question for your board

The regulatory environment is tightening — the data is unambiguous. And the governance model that boards need already exists in an adjacent domain. The gap between where physical security sits today and where it belongs is closable — and the organizations that close it first will be better positioned to protect their people, satisfy their regulators, and demonstrate the governance that stakeholders rightly expect.

The question is straightforward: does your board receive regular reporting on physical security risk with the same rigor it applies to financial performance, clinical quality, and cybersecurity? If not, that gap is the most important conversation your leadership team isn't having yet.

REFERENCES

1. American Hospital Association. (2025). The Burden of Violence to U.S. Hospitals: A Comprehensive Assessment of Financial Costs and Other Impacts of Workplace and Community Violence. Prepared by Harborview Injury Prevention & Research Center, University of Washington School of Medicine.
2. Bureau of Labor Statistics. (2020). Workplace Violence in Healthcare, 2018. U.S. Department of Labor.
3. The Joint Commission. (2025). Sentinel Event Data: 2024 Annual Review.
4. The Joint Commission. (2025). Sentinel Event Policy (SE). Classifies assault, sexual abuse/assault, and homicide of patients, staff, practitioners, trainees, visitors, or vendors on hospital premises as reviewable sentinel events.
5. The Joint Commission. Environment of Care Standards (EC.02.01.01).
6. Centers for Medicare & Medicaid Services. Conditions of Participation for Hospitals (42 CFR §482).
7. Occupational Safety and Health Act of 1970, Section 5(a)(1) (General Duty Clause).
8. California Senate Bill 553 (SB 553). Effective July 1, 2024.
9. Save Healthcare Workers Act. H.R. 3178/S. 1600, 119th Congress. Introduced May 5, 2025.
10. Additional state healthcare workplace violence legislation: New York (Labor Law §27-b), Connecticut (PA 21-174), Minnesota (Minn. Stat. §144.566), Illinois (Health Care Violence Prevention Act, 210 ILCS 160), Oregon (ORS 654.414), Washington (WAC 296-800-140), Maine (26 MRSA §806), Maryland (Md. Code, Health-General §19-353), New Jersey (N.J.S.A. 26:2H-5.19).

CSA

THE BUSINESS OF SECURITY™

QUESTION 2 *of 12*

IS OUR SECURITY FUNCTION STRUCTURED FOR SUCCESS?

CSA HEALTHCARE SECURITY GOVERNANCE REPORT

IS OUR SECURITY FUNCTION STRUCTURED FOR SUCCESS?

Physical security warrants board oversight. The critical question is structural: is the security function itself designed to deliver what governance requires?

In most healthcare systems, the answer exposes a fundamental contradiction. Boards acknowledge that staff safety, patient protection, and regulatory compliance depend on effective security — yet the function responsible for delivering those outcomes is often buried within facilities management, plant operations, or nursing departments whose primary mission lies elsewhere. The organizational position of security is not a neutral administrative choice. It shapes what the function can accomplish, what leadership expects from it, and whether it operates as a strategic capability or a cost to be managed.

Organizations that treat this as a reporting-line question alone miss the larger point. Structure is a governance decision. It determines whether security has the authority, visibility, and cross-functional access to fulfill the role that regulators, accreditors, and industry standards already define for it.

Where security sits today

The common models are familiar. Security reports to a Vice President of Facilities, a Chief Operating Officer, a Chief Nursing Officer, or in some cases a risk or compliance executive. Each arrangement carries trade-offs, but the deeper issue is not which box security occupies on the org chart — it is whether that position enables or constrains strategic capability.

"Sometimes security is buried too low in the hierarchy — more as a cost center versus a strategic partner," observes John Chilson, CSA Senior Advisor and veteran healthcare executive. With 30+ years of experience in healthcare leadership — including interim security leadership for a Level I Trauma Center and senior HR leadership across complex health systems — Chilson has seen firsthand how organizational placement shapes security effectiveness. When security is subordinated to a department with competing priorities, it is inevitably shaped by those priorities. Budget requests are weighed against facilities maintenance. Staffing decisions are influenced by operational headcount targets. And security leadership is rarely in the room when enterprise risk decisions are made.

Tim Leroux, CSA Senior Advisor and former senior leader at one of the nation's largest integrated health systems, frames the consequence directly: "Healthcare security is arguably the least mature function in any hospital system." That assessment is not a reflection of the people doing the work. It is a reflection of where organizations have placed the function — and what they have resourced it to become.

> "Healthcare security is arguably the least mature function in any hospital system."
>
> ***Tim Leroux, CSA Senior Advisor • Former Senior Healthcare Leader***

IS OUR SECURITY FUNCTION STRUCTURED FOR SUCCESS?

What the industry already requires

The argument for restructuring security governance is not new, nor is it coming solely from security professionals. The industry's own standards bodies, accreditors, and professional associations have already defined what effective security governance should look like. The gap is between what these frameworks require and how most organizations actually operate.

The Joint Commission's Environment of Care standards (EC.01.01.01) require hospitals to maintain a written plan for managing the security of everyone who enters the facility. The standards further require designated individuals to manage risk, coordinate risk reduction activities, collect deficiency information, and report results to leadership. The Leadership Chapter establishes explicit reporting relationships between organizational leadership and those responsible for the environment of care. These are not suggestions — they are conditions of accreditation. Yet in many systems, security's representation in this governance structure is nominal: a seat at the Environment of Care committee that functions as a compliance exercise rather than a strategic forum.

ASIS International's Enterprise Security Risk Management Guideline, published in 2019, goes further. The ESRM framework rests on four foundational pillars: holistic risk management, stakeholder partnership, transparency, and governance. It defines governance as aligned with overall organizational governance, with committees leading risk tolerance discussions and top-level decision-making. Critically, ESRM positions the security professional not as an enforcer but as a trusted advisor — a strategic partner who works with asset owners to identify and prioritize risks. It assigns four distinct roles of responsibility: asset owners, security professionals, stakeholders, and top management. That distribution of accountability is precisely what most healthcare security structures lack.

The International Association for Healthcare Security and Safety reinforces this in its Healthcare Security Industry Guidelines, now in its 13th edition. IAHSS calls for security programs built through collaborative planning and work by multi-disciplinary teams with risk-based processes tailored to organizational complexity. The standard envisions security as a function that integrates with clinical, operational, and administrative leadership — not one that operates in isolation beneath them.

The point is not that healthcare organizations should adopt any single framework wholesale. It is that the industry has already defined the governance architecture security requires — multi-disciplinary, risk-based, strategically positioned, and connected to senior leadership. Most healthcare systems are meeting only the compliance minimum of these standards, and many are not meeting that.

IS OUR SECURITY FUNCTION STRUCTURED FOR SUCCESS?

Governance first, structure second

What does it look like when an organization takes these principles seriously? Jeremy Baumann, CSA's Chief Executive Officer, describes the transformation at a major health system where governance was the first priority: "Governance was the first thing to tackle. We needed decision-makers from each silo at the table — not observers, but people with authority to make decisions and allocate resources."

Baumann argues that the specific reporting line matters less than whether the structure provides genuine access to the executive committee — not through a chain of intermediaries, but as a direct participant in the conversations where risk decisions are made. That distinction reframes the structural question: it is less about which department security reports to and more about whether the governance design gives security a voice at the leadership level.

> "What matters is access to the executive committee."
>
> ***Jeremy Baumann, CSA Chief Executive Officer***

That governance-first approach was tested almost immediately. When a mass shooting at a community clinic made national headlines, the governance group immediately pivoted the system's security priorities from just hospitals to add significant focus on ambulatory locations — a decision that required coordination across executive leadership system-wide. Without the governance structure already in place, that kind of strategic realignment would have taken months.

The contrast of governance without authority is instructive. At one of the nation's largest integrated health systems, a capable security team managed to publish only seven of thirty needed security policies over eighteen months. Attorneys debated language, committees deferred decisions, and the absence of clear governance authority meant that even foundational documents were treated as optional rather than essential. The capability existed. The structure did not support it.

Brad Brekke, CSA's Chief Business Officer and former Vice President of Assets Protection and Corporate Security at Target Corporation, identifies the root issue: "Governance is the critical function and lever. Start at the highest level, which pulls up the lower levels." When security governance begins at the enterprise level — with board visibility, defined committee representation, and documented decision rights — it creates the conditions for operational effectiveness at every level below. When it begins at the site level and attempts to build upward, it encounters the silos, competing priorities, and fragmented authority that define the current state in most healthcare systems.

IS OUR SECURITY FUNCTION STRUCTURED FOR SUCCESS?

The question for your board

The standards already exist. The Joint Commission requires security management plans with leadership oversight. ASIS defines governance as a foundational pillar of enterprise security. IAHSS calls for multi-disciplinary, risk-based program design. The question is not whether your organization should govern security strategically — the industry has already answered that. The question is whether your current structure enables it.

Does your security leader have direct access to the executive committee — not through a chain of intermediaries, but as a participant in the conversations where risk decisions are made? Does security have a seat on the governance committees that matter — risk, safety, operations — with the authority to influence decisions, not merely report on them? Or is security structured as a subordinate function within a department whose priorities lie elsewhere?

If the answer to that last question is yes, then the structure itself is the first thing that needs to change.

REFERENCES

1. The Joint Commission. Environment of Care Standards (EC.01.01.01): Written plan requirements for security management, risk coordination, and leadership reporting.
2. The Joint Commission. Environment of Care Standards (EC.04.01.01): Annual evaluation of environment of care management plans by governing body or designated leadership.
3. The Joint Commission. Leadership Chapter (LD.04.04.05): Reporting relationships between leadership and responsible entities for environment of care.
4. ASIS International. (2019). Enterprise Security Risk Management (ESRM) Guideline. Four foundational pillars: holistic risk management, stakeholder partnership, transparency, and governance. Available at: https://www.asisonline.org/publications--resources/standards--guidelines/esrm-guideline/
5. ASIS International. ESRM Maturity Model. Assessment framework for program strategy, governance, implementation, and alignment of security risk mitigation.
6. International Association for Healthcare Security and Safety. Healthcare Security Industry Guidelines, 13th Edition.
7. International Association for Healthcare Security and Safety. Security Design Guidelines for Healthcare Facilities, 4th Edition.

CSA

THE BUSINESS OF SECURITY™

QUESTION 3 *of 12*

IS OUR SECURITY LEADER SET UP TO SUCCEED?

CSA HEALTHCARE SECURITY GOVERNANCE REPORT

IS OUR SECURITY LEADER SET UP TO SUCCEED?

Effective governance of physical security depends on capable executive leadership. The question is whether the individual leading the function is positioned and prepared to operate as a strategic risk leader.

In most healthcare systems, the opportunity often lies in a structural gap. Security leaders are frequently hired for operational strength and incident management experience. Those skills are essential, but they are not sufficient for board engagement, enterprise alignment, and regulatory strategy. When the industry defines security leadership tactically, it should not be surprised when strategic impact remains constrained.

What the role demands

Bob Pocica, CSA Practice Area Lead, Corporate Security and former Senior Vice President and Chief Security Officer at McKesson Corporation, frames the problem directly: "Many CSOs know lights, locks, and alarms but can't build a business plan. If you can't talk to your CFO with a business plan, you're never going to get any money."

That observation is not unique to healthcare, but it is especially consequential there. Healthcare security leaders operate in environments of extraordinary complexity — regulatory requirements from the Joint Commission, CMS, and OSHA; clinical workflows that cannot be interrupted; patient populations that include the vulnerable, the volatile, and the cognitively impaired; and a workforce that experiences violence at five times the rate of the general workforce. Managing that environment requires more than technical proficiency in access control and surveillance. It requires someone who can articulate risk in financial terms, build cross-functional relationships, and translate security requirements into language that resonates with clinical and administrative leadership.

Healthcare already understands this principle in every other executive function. No system would hire a Chief Financial Officer whose only qualification was bookkeeping, or a Chief Nursing Officer based solely on bedside clinical skill. The expectation that leadership roles require leadership competencies — strategic thinking, organizational navigation, financial fluency, stakeholder management — is well established across every executive function. Security has historically been the exception, where organizations routinely promote based on operational tenure rather than executive capability.

Jeremy Baumann, CSA's Chief Executive Officer, reduces the requirement to its essence: "Business skills, business skills, and business skills." The repetition is deliberate. In Baumann's experience leading healthcare security transformations, the leaders who succeed are not necessarily those with the deepest security expertise. They are the ones who understand how the organization makes decisions, how budgets are built and defended, and how to present a strategic case to executives who have no background in security.

> "You may already be a security expert, but you don't know how to be an executive."
>
> ***Bob Pocica, CSA Practice Area Lead, Corporate Security • Former SVP & CSO, McKesson Corporation***

IS OUR SECURITY FUNCTION STRUCTURED FOR SUCCESS?

What the role actually requires

The ASIS International Chief Security Officer Guideline, first published in 2004 and subsequently adopted as an ANSI-approved national standard, provides the most widely referenced competency framework for senior security leadership. Its central finding is striking: the strategic, business, and interpersonal abilities of a security leader are of greater importance than technical security skills, many of which are available through internal subject matter experts or external consultants.

The guideline identifies five core competency areas:

- Leadership and management — people development, change management, and stakeholder relationships
- Analyzing the business — the ability to evaluate security's place in the wider organization
- Risk management — translating security requirements into business language
- Business acumen — strategy, financial matters, and operational understanding
- Emotional intelligence — self-awareness and interpersonal skill for navigating complex organizational dynamics

Subsequent analysis has described business acumen as the "nuclear element" of the CSO role — the competency without which the others cannot be fully effective.

That framework was designed for corporate environments broadly, but it maps directly onto the challenges of healthcare security leadership. A security leader who cannot analyze the business will not connect security investments to patient safety outcomes. A leader without emotional intelligence will not build the clinical trust that effective security requires. A leader without business acumen will present security as a cost to be minimized rather than a capability to be developed.

The profile that works

If technical expertise alone is insufficient, what does the right profile look like? The answer from CSA's practitioners is consistent — and perhaps counterintuitive.

Baumann describes a decision at a major health system that illustrates the principle. When the security director role opened, the system hired not from within security but from human resources — a leader with no security experience whatsoever. That person transformed the function. The reason was not that security expertise was irrelevant, but that the organization's greater need was for someone who could build teams, manage change, develop people, and navigate cross-functional relationships. The new leader brought credibility with clinical stakeholders that a career security professional would have spent years building. He professionalized hiring, introduced structured development pathways, and rebuilt trust between security and the departments it served. Technical security knowledge was taught and sourced from subject matter

experts within the team. Executive leadership capability — the competency the function had lacked — walked in the door on day one.

Brad Brekke, CSA's Chief Business Officer and former Vice President of Assets Protection and Corporate Security at Target Corporation, frames the investment principle: "Start high, which pulls up the lower levels." Brekke's argument is that organizations should invest in fewer, better-compensated security leaders rather than spreading budget across a large number of lower-level positions. A strong leader at the top attracts better talent below, raises expectations across the team, and creates the conditions for the kind of professional development that retains high performers.

The contrast is visible in how organizations recruit at every level. Jen Moberg, CSA Senior Advisor and Vice President of Emergency Services, identifies the baseline problem: "Security hires are often first jobs — 'this is my neighbor's kid.'" David Flynn, CSA Chief Administrative Officer, puts the structural cause plainly: organizations expect a highly capable professional but budget for a $17-an-hour entry-level position. When the entry point to the profession signals low expectations and low investment, the leadership pipeline reflects those expectations. There is no development pathway from an underpaid frontline role to an executive position that requires business acumen, financial fluency, and strategic capability. The gap between the two is not a career ladder — it is a canyon.

One large health system's leadership search illustrates how the trajectory can change. The organization evolved from promoting an internal candidate whose previous role was in frontline security operations, to conducting a national executive search that ultimately attracted a former senior FBI executive. The difference was not just in the individuals — it was in what the organization signaled about how seriously it took the function.

The question for your board

The competency framework exists. The ASIS standard defines what an effective security leader looks like. The experience of organizations that have invested in the right leadership profile demonstrates what becomes possible when security is led by someone who can operate at the executive level. The question for healthcare boards is whether they have applied the same rigor to selecting and developing their security leader that they apply to every other executive function.

"If you're not comfortable with that leader presenting to your executive committee and board, you don't have the right leader."

Jeremy Baumann, CSA Chief Executive Officer

IS OUR SECURITY FUNCTION STRUCTURED FOR SUCCESS?

The test is not whether your security leader can manage guards and cameras. It is whether that leader can present a strategic security plan to the board, defend a budget request to the CFO, collaborate with the Chief Nursing Officer on workplace violence prevention, and sit credibly at the executive committee table. Baumann offers one final diagnostic: in his experience, healthcare executives almost never ask their security leader for a strategy. That silence reveals as much about the organization's expectations as it does about the leader's capabilities.

REFERENCES

1. ASIS International. (2004). Chief Security Officer (CSO) Guideline (GDL CSO 06 2004). Competency framework for senior security leadership, including five core areas: leadership and management, analyzing the business, risk management, business acumen, and emotional intelligence.
2. ASIS International. Chief Security Officer (CSO) Organizational Standard (ASIS CSO.1). ANSI-approved national standard defining the senior security executive role, functions, and competencies.
3. ASIS International. (2023). "From CSO to SSE: Expanding Leadership Roles in Security." Security Management. Analysis of business acumen as the "nuclear element" of the CSO role.
4. Bureau of Labor Statistics. (2022). Survey of Occupational Injuries and Illnesses: Healthcare workers experience workplace violence at five times the rate of the general workforce.

CSA

THE BUSINESS OF SECURITY™

QUESTION 4 *of 12*

WHO IS ACCOUNTABLE WHEN SOMETHING GOES WRONG?

CSA HEALTHCARE SECURITY GOVERNANCE REPORT

WHO IS ACCOUNTABLE WHEN SOMETHING GOES WRONG?

Physical security requires board-level attention, governance structures designed for strategic impact, and leadership with executive competencies. Each of those principles raises a question that most healthcare organizations have not clearly answered: when a security incident occurs, who is accountable?

The instinctive answer — the security department — is the wrong one. And the consequences of that misunderstanding extend well beyond incident response. When accountability for security risk is unclear, organizations create the conditions for exactly the failures they are trying to prevent.

The misconception

Bob Pocica, CSA Practice Area Lead, Corporate Security and former Senior Vice President and Chief Security Officer at McKesson Corporation, identifies the foundational error: "Management owns the risk. The CSO provides insight, guidance, and mitigation." That distinction is not semantic. It defines whether security operates as a strategic advisory function or as a department that absorbs blame when things go wrong.

In Pocica's framework, the security leader's role is to identify risk, assess it, recommend mitigation, and communicate clearly to the leaders who own the assets and operations at stake. The decision to accept, mitigate, or transfer that risk belongs to the operational leaders and, ultimately, to the board. Pocica is explicit about how he ensured that distinction held: "I confirm this in an email, not just a conversation." The paper trail is not bureaucracy — it is the mechanism that ensures risk decisions are visible, documented, and owned by the people with the authority to make them.

> "Management owns the risk. The CSO provides insight, guidance, and mitigation."
>
> ***Bob Pocica, CSA Practice Area Lead, Corporate Security • Former SVP & CSO, McKesson Corporation***

Healthcare already applies this principle to other forms of risk. Clinical liability is not owned by the quality department — it is owned by the clinicians, departments, and executives who deliver care, with quality providing oversight, measurement, and guidance. Financial compliance is not owned by the audit function — it is owned by the leaders who authorize transactions and manage budgets. Security risk should follow the same model: distributed ownership with centralized advisory capability.

WHO IS ACCOUNTABLE WHEN SOMETHING GOES WRONG?

What governance already requires

The regulatory framework for healthcare accountability has been strengthened significantly. The HHS Office of Inspector General's General Compliance Program Guidance, updated in November 2023, outlines seven elements of an effective compliance program and is explicit about board responsibility. The guidance states that governing boards should be knowledgeable about the content and operation of the compliance program, should meet with the compliance officer at least quarterly, and should receive annual reports on the program's effectiveness in addressing identified risks. The board has a fiduciary duty to ensure that information and reporting systems exist to allow informed judgments about compliance and risk.

The accountability gap becomes especially visible when compared to cybersecurity. In July 2023, the SEC adopted rules requiring public companies to disclose material cybersecurity incidents within four business days of determining materiality and to describe the board's oversight of cyber risk in annual filings. That framework establishes mandatory, board-level accountability for one form of security risk — with defined timelines, disclosure requirements, and governance expectations. No comparable framework exists for physical security. A healthcare organization that experiences a workplace violence incident resulting in serious injury or death faces no equivalent obligation to disclose the event, describe its governance of the risk, or demonstrate that the board was informed and exercising oversight.

That compliance framework applies broadly, but the accountability architecture it describes — board oversight, quarterly engagement, documented risk assessment, clear reporting relationships — is precisely what physical security governance lacks in most healthcare organizations. Compliance officers report to the board. Chief Medical Officers report to the board. Chief Information Security Officers increasingly report to the board on cyber risk. Physical security leaders, in most systems, do not.

Brad Brekke, CSA's Chief Business Officer and former Vice President of Assets Protection and Corporate Security at Target Corporation, frames the exposure in terms any board member understands: "Are you running the organization like a car without seatbelts?" The analogy is apt. An organization that has not defined who owns security risk, how that risk is escalated, and what decisions require board-level visibility is operating without the mechanisms that would protect it when — not if — an incident occurs.

When accountability fails

The consequences of unclear accountability are visible in patterns that recur across healthcare systems. Jeremy Baumann, CSA's Chief Executive Officer, describes the structural version of the problem at a major health system where security reported too far down the organizational hierarchy. Information was filtered before it reached leadership — shaped not by what the organization needed to know but by the priorities and agenda of the intermediary. Critical risk information that should have reached the executive committee was softened, delayed, or reframed. The result was not a failure of the security function but a failure of the accountability structure: the information existed, but the reporting pathway prevented it from reaching the people who needed to act on it.

WHO IS ACCOUNTABLE WHEN SOMETHING GOES WRONG?

Jen Moberg, CSA Senior Advisor and Vice President of Emergency Services, identifies a subtler but equally damaging pattern. In her experience, security is rarely invited to participate in root cause analysis after safety events — treated as a separate venue rather than an integrated part of the investigation. When security is excluded from the processes that examine what went wrong, the organization loses the ability to identify whether structural failures, rather than individual failures, contributed to the event. Accountability without investigation is blame assignment. Investigation without security participation is incomplete.

> "Are you running the organization like a car without seatbelts?"
>
> ***Brad Brekke, CSA Chief Business Officer • Former VP of Assets Protection & Corporate Security, Target***

Building accountability structures

Effective accountability requires architecture, not aspiration. At McKesson, Pocica established a Senior Risk Advisory Board with clear escalation paths, documented risk acceptance protocols, and defined decision rights at each organizational level. When a risk was identified and a recommendation made, the response was tracked: accepted, modified, or declined — with the declination documented and owned by the leader who made the decision. That structure ensured that accountability was distributed to the people with the authority to act, not concentrated on the person who identified the problem.

Pocica adds a dimension that distinguishes genuine advisory accountability from passive documentation. When he believed a risk decision was wrong, he went back — a second, third, fourth time. The obligation of the security leader does not end with a single recommendation and a documented refusal. A risk that is real on Monday is still real on Friday. The professional responsibility is to persist until the risk is genuinely addressed or the organization has made an informed, eyes-open decision to accept it. Documentation without advocacy is compliance theater. The accountability model works only when the security leader treats the advisory role as a genuine obligation, not a procedural box to check.

For healthcare organizations, building that architecture means defining accountability at three levels: the board, which oversees security governance and receives regular risk reporting; the executive committee, which makes risk decisions and allocates resources; and operational leadership, which owns the implementation of security measures within their areas of responsibility. The security function advises all three levels, provides the risk assessment that informs decisions, and maintains the documentation that ensures accountability is traceable.

WHO IS ACCOUNTABLE WHEN SOMETHING GOES WRONG?

The question for your board

When the next security incident occurs — and in healthcare, it is a matter of when, not if — will your organization be able to demonstrate that risk was identified, communicated to the appropriate decision-makers, and either mitigated or consciously accepted? Can you show who was informed, what they decided, and why? If the answer to those questions depends entirely on the security department's records, then the organization has not distributed accountability — it has delegated it downward to a function without the authority to act on it.

The HHS-OIG guidance is clear: governing boards have a fiduciary duty to ensure that reporting systems exist for informed risk judgments. The SEC has established that principle for cybersecurity. The question is whether physical security is part of that system — or whether it remains the one enterprise risk that the board has never formally agreed to own.

REFERENCES

1. U.S. Department of Health and Human Services, Office of Inspector General. (2023). General Compliance Program Guidance (GCPG). Seven elements of an effective compliance program, board oversight requirements, quarterly engagement with compliance officer, annual risk assessment.
2. U.S. Securities and Exchange Commission. (2023). Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (Release Nos. 33-11216; 34-97989). Adopted July 26, 2023. Requires material incident disclosure within four business days and annual board oversight reporting.
3. U.S. Sentencing Commission. Organizational Sentencing Guidelines, §8B2.1. Governing authority requirement to be knowledgeable about compliance program content and operation.
4. ASIS International. (2019). Enterprise Security Risk Management (ESRM) Guideline. Four roles of responsibility: asset owners, security professionals, stakeholders, and top management.
5. The Joint Commission. Environment of Care Standards (EC.01.01.01): Leadership reporting requirements for security management activities.

CSA

THE BUSINESS OF SECURITY™

QUESTION 5 *of 12*

ARE WE CONSISTENT ACROSS THE ENTERPRISE?

CSA HEALTHCARE SECURITY GOVERNANCE REPORT

ARE WE CONSISTENT ACROSS THE ENTERPRISE?

Governance, structure, leadership, and accountability all assume that decisions made at the enterprise level translate into consistent practice across the organization. In most healthcare systems, they do not.

Multi-facility health systems are assembled through decades of acquisitions, mergers, and organic growth. Each hospital, clinic, and ambulatory site brings its own security history — different technologies, different procedures, different cultures, and often different leaders who built their programs in isolation. The result is not one security program but dozens of variations, each shaped by local decisions that were never reconciled into a coherent enterprise approach.

What fragmentation looks like

Jeremy Baumann, CSA's Chief Executive Officer, describes what he found at the outset of a major health system engagement: nine different video management systems, six different access control platforms, and no aggregate visibility into what the organization was spending on security technology. Each facility had made its own purchasing decisions over years of independent operation. The systems did not communicate with each other. Data could not be consolidated. And no one at the enterprise level had a complete picture of the organization's security posture.

The financial consequences of that fragmentation were striking. When the organization finally consolidated its security spending data, leadership discovered it was investing $11.5 million annually in physical security — not the $2–3 million they had assumed. An additional $21 million in security technology assets sat unbooked on facility balance sheets. The gap between what leadership believed it was spending and what it was actually spending was not a rounding error — it was the direct cost of operating without enterprise visibility. An organization that cannot see what it spends cannot evaluate whether it is spending effectively.

David Flynn, CSA Chief Administrative Officer, identifies the operational symptom that signals deeper fragmentation: "'We call John' is a red flag." When a security program depends on one person's knowledge, relationships, or institutional memory to function, it is not a program — it is a personality-dependent operation. If 'John' retires, transfers, or is unavailable during a crisis, the organization discovers that what it thought was a system was actually an individual.

> "We call John' is a red flag — single-person dependency indicates fragmentation."
>
> ***David Flynn, CSA Chief Administrative Officer***

Baumann traces the root cause directly: "Poor organizational structure — fiefdoms — governance lacking." When individual facilities control their own security budgets, hiring, and technology decisions without enterprise oversight, fragmentation is not a failure of execution. It is the predictable outcome of a governance structure that never required consistency in the first place.

ARE WE CONSISTENT ACROSS THE ENTERPRISE?

The policy development challenge

Fragmentation is most visible in technology, but its most consequential expression is in policy. Tim Leroux, CSA Senior Advisor and former Senior Healthcare Leader, describes the difficulty of establishing enterprise-wide security standards even in a system that recognized the need. Over eighteen months, a capable security team managed to publish only seven of the thirty policies required. Attorneys debated language. Committees deferred decisions. Stakeholders with competing priorities delayed approvals. The absence of clear governance authority meant that even foundational documents — the policies that should define what security looks like across the organization — were treated as optional rather than essential.

That experience illustrates a pattern that extends beyond any single organization. When security lacks governance authority and leadership competencies, enterprise consistency becomes impossible regardless of intent. Policies without enforcement authority are suggestions. Standards without governance backing are aspirations. The problem is not that organizations do not recognize the need for consistency — it is that their structures do not support achieving it.

Jen Moberg, CSA Senior Advisor and Vice President of Emergency Services, adds a timing reality that leadership must understand: even when enterprise policies are approved, it typically takes six to twelve months before frontline staff experience the change. Implementation at scale requires training, communication, technology deployment, and cultural adaptation across every site. Organizations that underestimate that timeline mistake policy publication for program change.

Framework for consistency

Consistency does not mean rigidity. A Level I Trauma Center in an urban environment faces different risks than a rural ambulatory clinic, and the security response should reflect those differences. The goal is not to impose identical operations at every site but to establish a common framework — shared standards, consistent technology platforms, unified policies, and enterprise-level oversight — within which local adaptation is both expected and governed.

Baumann describes the model that worked: system-wide leaders responsible for technology standards and program design, with site-level execution that operates within those standards. That structure ensures that when a new facility is acquired or a new site opens, it is integrated into the enterprise security program rather than allowed to develop its own. Technology platforms are consolidated. Policies apply system-wide. Data flows to a central point where enterprise risk can be assessed.

> "Poor organizational structure — fiefdoms — governance lacking."
>
> ***Jeremy Baumann, CSA Chief Executive Officer***

ARE WE CONSISTENT ACROSS THE ENTERPRISE?

Technology is the most tangible lever for consistency. When every facility operates on the same access control and video management platform, data can be consolidated, incidents can be compared across sites, and leadership can make informed decisions about where risk is concentrated. When each facility operates on its own platform, the enterprise is blind to patterns that only emerge at scale.

The proof that healthcare organizations can achieve enterprise consistency already exists within their own walls. Ken Senser, CSA's Chief Strategy Officer, describes arriving at a major health system and finding a fully mature cybersecurity program — NIST-aligned, HIPAA-compliant, regularly audited, with clear enterprise standards applied uniformly across every facility. Alongside it, the physical security program had none of that: no enterprise standards, no consistent technology, no unified governance. Same organization, same board, same leadership team — but dramatically different maturity levels. The point is not that cybersecurity is better managed. It is that the organization has already demonstrated it can build and sustain enterprise consistency when it treats a function as a governance priority. Physical security has simply not yet been given that treatment.

The question for your board

If a serious security incident occurred at one of your facilities tomorrow, could you demonstrate that the same policies, standards, and governance apply across every site in the system? Could you show that the security program at the facility in question reflects enterprise standards rather than local improvisation? Or would the investigation reveal what most multi-facility health systems already know but have not yet addressed — that the answer depends entirely on which facility you ask about?

Enterprise consistency is not an operational afterthought. It is a governance requirement. When the board approves a security strategy, it is approving it for the entire organization. If that strategy is implemented unevenly — rigorously at some sites, loosely at others, not at all in acquired facilities that were never integrated — then the board's governance is aspirational rather than actual. And when something goes wrong, the gap between what the board approved and what actually existed will be the first thing anyone examines.

ARE WE CONSISTENT ACROSS THE ENTERPRISE?

REFERENCES

1. The Joint Commission. Environment of Care Standards (EC.01.01.01): Written plan requirements for security management across all facilities within a healthcare organization.
2. ASIS International. (2019). Enterprise Security Risk Management (ESRM) Guideline. Holistic, enterprise-wide approach to security governance and risk management.
3. International Association for Healthcare Security and Safety. Healthcare Security Industry Guidelines, 13th Edition. Multi-disciplinary, risk-based program design standards.
4. The Joint Commission. Environment of Care Standards (EC.04.01.01): Annual evaluation of environment of care management plans by governing body or designated leadership.
5. National Institute of Standards and Technology. Cybersecurity Framework (CSF). Enterprise-wide standards for risk management referenced as a model for consistent security governance.

THE BUSINESS OF SECURITY™

QUESTION 6 *of 12*

HOW SHOULD TECHNOLOGY ENABLE OUR SECURITY PROGRAM?

CSA HEALTHCARE SECURITY GOVERNANCE REPORT

HOW SHOULD TECHNOLOGY ENABLE OUR SECURITY PROGRAM?

Healthcare organizations are spending millions of dollars on security technology. Cameras line hallways. Access control systems protect entrances. Visitor management platforms screen arrivals. The question that most boards have never asked is whether any of it is working — or whether the technology is creating an expensive illusion of security rather than the reality.

Technology is essential to modern security operations. But technology without governance, strategy, and operational integration produces investment without accountability, capability without consistency, and cost without measurable outcomes.

When technology becomes theater

Jeremy Baumann, CSA's Chief Executive Officer, keeps a photograph of a wall of 176 monitors — eight rows of twenty-two screens — at a healthcare facility's security operations center. One or two people were responsible for watching all of them. No human being can meaningfully monitor 176 video feeds simultaneously. The wall existed not because it improved security outcomes but because it looked like security. It was, in Baumann's assessment, theater.

That example is dramatic but not unusual. Baumann describes a pattern he encounters repeatedly: organizations that have invested $1.5 million in cameras with no one assigned to monitor them and no storage capacity to retain footage for investigation. The cameras exist. They record nothing useful. At another facility, $5,000 keypads were installed on secured doors in an elderly care unit — with the access codes written on the keypads themselves. The technology was purchased, installed, and immediately rendered meaningless by an operational failure that no one was responsible for preventing.

These are not technology failures. They are governance failures expressed through technology. When an organization purchases security systems without defining how they will be operated, maintained, monitored, and integrated into the broader security program, the investment produces hardware, not security.

"Technology doesn't get tired, doesn't unionize, doesn't call in sick. But it has to be governed."

Jeremy Baumann, CSA Chief Executive Officer

ARE WE CONSISTENT ACROSS THE ENTERPRISE?

The right investment framework

The principle is straightforward: where technology can accomplish the same security objective at lower cost, higher consistency, or greater scale than staffing alone, it should. But the transition from a people-intensive model to a technology-enabled model is neither simple nor fast.

Brad Brekke, CSA's Chief Business Officer and former Vice President of Assets Protection and Corporate Security at Target Corporation, describes a transformation that took twenty years. Target's security function evolved from approximately 70–80 percent staffing and 20–30 percent technology to the inverse: 70–80 percent technology-enabled and 20–30 percent staffing. That evolution was not a technology project — it was a business transformation that required new competencies, new operating models, and sustained investment in both systems and people. The technology did not replace the workforce. It changed what the workforce did.

Tim Leroux, CSA Senior Advisor and former Senior Healthcare Leader, offers an important counterweight: "Technology is not the panacea that vendors sell it as." Leroux's experience in a system with more resources and integration capability than most demonstrates that even well-funded technology investments require operational maturity to produce outcomes. Systems that lack governance structures and clear accountability will not extract value from technology regardless of how much they spend.

What strategic technology investment looks like

Baumann provides a detailed example of technology investment done right. At a major financial services company, he led the consolidation of eleven security operation centers into two centralized Global Security Operations Centers. The capital investment was $7.2 million. The annual operating expense reduction was $2.1 million — a payback period of less than four years, with compounding savings every year thereafter.

The key insight was operational, not technological. The previous model assumed that security dispatchers needed intimate knowledge of each facility to be effective. The consolidation proved that assumption wrong: dispatchers needed standard protocols and reliable technology, while the patrol officers on-site provided the local knowledge. Centralizing dispatch did not reduce security capability — it improved consistency, reduced response variability, and created data that could be analyzed at the enterprise level.

For healthcare, that model translates directly. Multi-facility health systems operating independent security command centers at each hospital are replicating the fragmentation that undermines enterprise consistency. Centralized monitoring with standardized protocols and local response teams can deliver better outcomes at lower cost — but only when the technology investment is accompanied by the governance, training, and operational design that make centralization work.

ARE WE CONSISTENT ACROSS THE ENTERPRISE?

The lifecycle management gap

Even organizations that invest wisely in security technology often fail at lifecycle management. Bob Pocica, CSA Practice Area Lead, Corporate Security and former Senior Vice President and Chief Security Officer at McKesson Corporation, describes a pattern common across industries: analog cameras that have not been updated in a decade, half of them no longer functioning. Organizations that depreciate security technology assets over twenty to thirty years when the effective life of those systems is five to seven years. The result is a technology inventory that looks substantial on paper but delivers diminishing returns as systems age, fail, and become incompatible with modern platforms.

Jen Moberg, CSA Senior Advisor and Vice President of Emergency Services, identifies a related gap in emerging technology. Weapons detection systems — one of the most visible technology investments in healthcare security today — are producing uneven results. In Moberg's experience, too many edged weapons are getting through screening, including knives of five inches or more. The technology exists, but its effectiveness depends on calibration, staffing of screening points, and integration with response protocols. A weapons detection system that misses weapons is worse than no system at all — it creates false confidence.

> "Technology is not the panacea that vendors sell it as."
>
> ***Tim Leroux, CSA Senior Advisor • Former Senior Healthcare Leader***

The question for your board

The question is not how much your organization is spending on security technology. It is whether that technology is governed, operated, maintained, and integrated into a coherent security program — or whether it is a collection of independent purchases that no one has connected into a functioning system. Technology that is not monitored is decoration. Technology that is not maintained is a depreciating liability. Technology that is not integrated into operational protocols is an expensive expression of hope.

The organizations that extract real value from security technology are the ones that treat it as a business capability requiring governance, investment planning, lifecycle management, and measurable outcomes — exactly the way they treat every other enterprise technology investment. Ask whether your organization applies the same rigor to its security technology portfolio that it applies to its clinical systems, its electronic health record, or its financial platforms. If the answer is no, the technology is not the problem.

ARE WE CONSISTENT ACROSS THE ENTERPRISE?

REFERENCES

1. ASIS International. (2019). Enterprise Security Risk Management (ESRM) Guideline. Technology as an enabler within a governance-led security framework.
2. International Association for Healthcare Security and Safety. Healthcare Security Industry Guidelines, 13th Edition. Technology integration standards for healthcare security programs.
3. The Joint Commission. Environment of Care Standards (EC.02.01.01): Security systems maintenance and testing requirements for healthcare facilities.
4. ASIS International. (2012). Security Management Standard: Physical Asset Protection (PAP). Lifecycle management framework for security technology systems.

CSA

THE BUSINESS OF SECURITY™

QUESTION 7 *of 12*

ARE WE INVESTING WISELY IN SECURITY?

CSA HEALTHCARE SECURITY GOVERNANCE REPORT

ARE WE INVESTING WISELY IN SECURITY?

Healthcare organizations invest millions in security — staffing, technology, contracts, training. But most cannot answer a basic question: is the investment producing results? And many cannot answer an even more fundamental one: what are we actually spending?

For most healthcare systems, security spending is scattered across facility budgets, capital accounts, and departmental line items with no consolidated view. And the outcomes that spending produces are rarely measured against the kind of business case that any other enterprise investment would require.

The visibility problem

Fragmentation creates financial blindness. When one large health system finally consolidated its security spending data, the gap between what leadership assumed it was spending and what it was actually spending was nearly fourfold — with tens of millions in additional technology assets untracked on facility balance sheets. That is not an accounting error. It is the predictable outcome of a governance structure in which no one is responsible for seeing the full picture.

The problem extends beyond total spend visibility. Healthcare security budgets are overwhelmingly people-intensive. Industry benchmarks from the International Association for Healthcare Security and Safety indicate that 73 percent of healthcare security budgets are dedicated to staffing. When nearly three-quarters of the investment goes to personnel, and the remaining quarter is distributed across facilities without enterprise coordination, the organization has no mechanism to evaluate whether its total investment is sized appropriately, allocated effectively, or producing the outcomes that justify the cost.

> "Would you build a multimillion-dollar house without architectural drawings?"
>
> ***Jeremy Baumann, CSA Chief Executive Officer***

The business case framework

Jeremy Baumann, CSA's Chief Executive Officer, frames the investment discipline with an analogy that resonates with any executive: "Would you build a multimillion-dollar house without architectural drawings?" The question answers itself. Yet most healthcare organizations are making multimillion-dollar security investments without a strategic plan, a prioritized roadmap, or a business case that leadership can evaluate the way it evaluates any other capital request.

The European Union Agency for Cybersecurity's Return on Security Investment methodology provides a parallel framework. The calculation is straightforward: take the annualized cost of a risk without mitigation,

subtract the residual cost after mitigation and the cost of the mitigation itself, and evaluate whether the investment produces a positive return. That framework — already standard practice in cybersecurity planning — has no reason not to apply to physical security. A workplace violence prevention program that reduces incidents, lowers turnover, decreases workers' compensation claims, and avoids regulatory penalties produces a quantifiable return, just as a cybersecurity investment that prevents a breach does.

Brad Brekke, CSA's Chief Business Officer and former Vice President of Assets Protection and Corporate Security at Target Corporation, describes articulating security ROI as "more an art than a science." The key is aligning security metrics to what the organization already measures rather than inventing a parallel measurement system. At one major health system, Brekke linked visitor management not to security incident rates but to employee satisfaction scores and staff retention — metrics leadership already tracked and valued. The investment became visible in data the board was already reviewing. The business case succeeded because it spoke the organization's language, not security's.

Quantifying security value

The data to build these business cases already exists. Healthcare workplace violence costs an estimated $18.27 billion annually across the industry. Research indicates that 19.2 percent of nurses exposed to workplace violence leave the profession entirely. At a replacement cost of approximately $61,000 per registered nurse, the turnover cost alone provides a compelling basis for investment in prevention.

David Flynn, CSA Chief Administrative Officer, identifies additional financial levers that security leaders rarely quantify. Labor disputes increasingly cite workplace safety as a bargaining issue — strike demands reference security failures, and unions use safety data in contract negotiations. The attrition costs from violence exposure extend beyond direct replacement to include training, institutional knowledge loss, and the impact on team morale and patient care quality. Post-traumatic stress among healthcare workers exposed to violence creates ongoing costs in absenteeism, reduced productivity, and long-term disability claims.

None of these costs are invisible. They are simply uncounted — because the organization has never assigned anyone the responsibility to count them. When security spending has no business case, leadership evaluates it as a cost to be controlled rather than an investment to be optimized. That framing guarantees underinvestment in prevention and overinvestment in reactive response.

The security master plan

The IAHSS Healthcare Security Industry Guidelines recommend the development of multi-year security master plans — strategic documents that define the organization's security objectives, prioritize investments based on risk, and establish measurable milestones over a three-to-five-year horizon. Baumann describes the approach he implemented at one health system: a comprehensive business plan that addressed every identified security gap in a risk-prioritized sequence, with clear cost projections and expected outcomes for each phase.

ARE WE INVESTING WISELY IN SECURITY?

The discipline of a security master plan is not just about identifying gaps — it is about sequencing investment against risk. Baumann describes the prioritization logic: travel security for a dispersed workforce might represent significant risk exposure but require only $60,000 in annual investment to address. Enterprise-wide technology consolidation might carry a $26 million price tag. Both are legitimate needs. Without a strategic plan that evaluates risk severity against cost, organizations default to addressing whatever is most visible or most recently demanded — which is rarely what matters most.

That kind of strategic planning requires executive capabilities — a security leader who can build a business plan, present it to the CFO, and defend the investment logic against competing priorities. It also requires accountability structures so that approved investments are tracked, implemented, and evaluated against the outcomes they were designed to produce.

Bob Pocica, CSA Practice Area Lead, Corporate Security and former Senior Vice President and Chief Security Officer at McKesson Corporation, describes a practical advantage of those governance structures. At McKesson, his participation on the Senior Risk Advisory Board meant that major security investments were effectively presold to key decision-makers before they reached formal budget review. The CFO, General Counsel, and Chief Compliance Officer had already seen the risk data and understood the rationale. Budget conversations became confirmations rather than introductions — because the investment case had been built through the governance process itself.

> "Strike demands cite safety. Attrition is expensive. The costs are there — no one is counting them."
>
> ***David Flynn, CSA Chief Administrative Officer***

The question for your board

If your Chief Financial Officer asked tomorrow for the total cost of physical security across the enterprise — staffing, technology, contracts, maintenance, training, and incident-related costs — could your organization produce that number? And if it could, would it be accompanied by a business case that demonstrates what the investment is producing in reduced incidents, lower turnover, decreased liability, and avoided regulatory penalties?

Every other enterprise function is expected to justify its investment. Clinical programs demonstrate outcomes. IT departments present total cost of ownership. Compliance functions quantify risk reduction. Security should meet the same standard — not because it is under scrutiny, but because a disciplined approach to investment planning is the only way to ensure that the organization is spending enough, spending wisely, and spending in the places where it will matter most.

ARE WE INVESTING WISELY IN SECURITY?

REFERENCES

1. International Association for Healthcare Security and Safety. Healthcare Security Industry Guidelines, 13th Edition. Multi-year security master plan development and staffing benchmarks (73% personnel allocation).
2. European Union Agency for Cybersecurity (ENISA). (2012). Introduction to Return on Security Investment. ROSI methodology: (ALE − mALE − Cost) / Cost framework for security investment evaluation.
3. American Hospital Association. (2025). The Burden of Violence to U.S. Hospitals: A Comprehensive Assessment of Financial Costs and Other Impacts of Workplace and Community Violence. Prepared by Harborview Injury Prevention & Research Center, University of Washington School of Medicine.
4. NSI Nursing Solutions, Inc. (2024). National Health Care Retention & RN Staffing Report. Average cost of turnover for a registered nurse: approximately $61,000.
5. Bureau of Labor Statistics. (2022). Survey of Occupational Injuries and Illnesses. Healthcare workplace violence rates and workforce impact data.

CSA

THE BUSINESS OF SECURITY™

QUESTION 8 *of 12*

HOW DO WE BUILD AND RETAIN A HIGH-PERFORMING SECURITY TEAM?

CSA HEALTHCARE SECURITY GOVERNANCE REPORT

HOW DO WE BUILD AND RETAIN A HIGH-PERFORMING SECURITY TEAM?

When CSA Senior Advisor John Chilson arrived at a major integrated health system, he found a security team on the verge of collapse. Morale had deteriorated to the point where officers were actively pursuing unionization. The root cause was not compensation or scheduling — it was neglect.

> "What was loud and clear when I came in — no one was given the right training. No one felt invested in."
>
> ***John Chilson, CSA Senior Advisor • Senior Healthcare Leader***

The officers were not lazy or disengaged by nature. They had simply never been given the tools, development, or recognition that would make them want to stay. Through structured development, accountability, genuine listening, and partnership with CSA, the team was transformed. Turnover dropped from 25–30 percent to under 10 percent. The officers who had been ready to unionize became advocates for the program.

That transformation did not require a larger budget or a technology upgrade. It required treating security staff with the same organizational development discipline that healthcare systems routinely apply to clinical teams.

The talent challenge

Healthcare security faces a structural workforce problem that most clinical executives have not fully examined. The role demands empathy, de-escalation skills, physical stamina, sound judgment under pressure, and the ability to engage constructively with patients in crisis. The Bureau of Labor Statistics reports the median annual wage for security guards nationally at approximately $36,000 — with healthcare settings typically ranging from $28,000 to $50,500 depending on facility size and location. As David Flynn, CSA's Chief Administrative Officer, observes, the industry is asking for a "$17-an-hour Chuck Norris" — expecting expertise and composure at entry-level wages.

The talent pool reflects that mismatch. Jen Moberg, CSA Senior Advisor and Vice President of Emergency Services, notes that "security hires are often first jobs — 'this is my neighbor's kid.'" That is not inherently a problem — but it becomes one when the organization provides no structured onboarding, no clinical context, and no career pathway. The result is a cycle of underinvestment and high turnover that organizations accept as inevitable rather than recognizing as a design failure.

HOW DO WE BUILD AND RETAIN A HIGH-PERFORMING SECURITY TEAM?

Hiring for the mission

Organizations that have broken this cycle share a common insight: hire for character and clinical alignment, then teach security. Jeremy Baumann, CSA's Chief Executive Officer, describes the approach: "Go after raw talent with the right general experience — I can teach security." The qualities that make an effective healthcare security officer — empathy, composure, communication — are not skills that can be trained into someone who lacks them.

This reframes security as a patient care role, which changes who you recruit and how you evaluate them. Moberg's approach at her health system involved cross-functional panel interviews with clinical stakeholder input — the most successful hiring model she has seen. Chilson built structured behavioral interviews grounded in the organization's mission, vision, and values, using two-tier hiring panels that set clear expectations about attendance, commitment, and professional conduct from the first conversation.

The critical point for boards is that hiring is a program design decision, not an administrative task. When security recruitment mirrors the intentionality applied to clinical hiring — structured interviews, cross-functional input, values-based assessment — the quality of the workforce changes fundamentally.

Training as a discipline

Chilson is emphatic that training must be a line of discipline within the security structure — not an afterthought, not an annual compliance exercise, and not something squeezed into the margins of operational schedules.

> "You need to have a simulation center — spend half a day on actual scenarios. You put officers through that and evaluate."
>
> ***John Chilson, CSA Senior Advisor • Senior Healthcare Leader***

His model includes simulation centers for scenario-based learning, competency checklists aligned to role requirements, annual refreshers on de-escalation and crisis response, and field training officers who mentor new hires through their first months. The clinical parallel is deliberate: healthcare validates clinical competency through simulation labs, skills checkoffs, and supervised practice. Security teams operating in clinical environments deserve the same rigor.

Moberg reinforces this from the clinical operations perspective: "The most impactful de-escalation training is role-playing, not webinars." The distinction matters. When security officers and clinical staff train together on de-escalation, they build shared language, mutual respect, and the kind of trust that makes real-time collaboration possible during a crisis.

HOW DO WE BUILD AND RETAIN A HIGH-PERFORMING SECURITY TEAM?

A major health system engagement illustrates what structured training investment looks like at scale: the organization went from zero formal training infrastructure to a dedicated Training Program Manager, building systematic competency development across a protective force that expanded from 54 to 174 FTE with a full rank structure and professional development pathway.

Retention and development

Recruitment and training create capability. Retention and development sustain it. Chilson's approach centers on Individual Development Plans — personalized growth pathways that give officers visibility into their future within the organization.

> "Individual development plans are golden. They give you fair warning — and they give the officer a roadmap."
>
> ***John Chilson, CSA Senior Advisor • Senior Healthcare Leader***

His retention framework includes role rotation to combat disengagement and burnout, regular one-to-one meetings that focus on growth rather than just performance, open-door leadership that builds psychological safety, and recognition tailored to the individual. As Chilson notes, "not everyone wants the party in the break room — sometimes a personal note is key."

The counterpart to development is accountability. Baumann frames the balance directly: "You either change people or you change people." Performance management is not the opposite of development investment — it is the essential counterpart. Organizations that invest in training, create clear expectations, and then hold people accountable find that the officers who thrive are the ones who wanted to grow all along.

This is the same talent management discipline that clinical leaders apply to nursing workforce retention. Healthcare systems have spent a decade refining nurse recruitment, residency programs, preceptor models, and career ladders. Security teams operating within those same organizations deserve equivalent investment — and the return on that investment, as the transformation story demonstrates, can be remarkably swift.

The question for your board

What is the turnover rate in your security department, and how does it compare to your clinical staff? What is your training investment per officer? Does your organization have a structured development pathway for security professionals — or is it cycling through entry-level hires and accepting the costs of that churn as inevitable?

HOW DO WE BUILD AND RETAIN A HIGH-PERFORMING SECURITY TEAM?

Organizations that track these metrics often discover the answers point to the same structural investments that transformed clinical workforce retention: intentional hiring, competency-based training, career development, and leadership that treats every team member as someone worth investing in.

REFERENCES

1. Bureau of Labor Statistics. Occupational Employment and Wage Statistics, Security Guards (SOC 33-9032), May 2024.
2. International Association for Healthcare Security and Safety. Healthcare Security Industry Guidelines and Benchmarking Data.
3. OSHA. Guidelines for Preventing Workplace Violence for Healthcare and Social Service Workers, OSHA 3148-06R, 2016.
4. UC Berkeley Labor Center. Demographic and Job Characteristics of NYC's Security Guard Workforce, 2025.
5. ASIS International. Chief Security Officer Guideline, ASIS GDL CSO-2004.
6. NSI Nursing Solutions, Inc. (2024). National Health Care Retention & RN Staffing Report.

CSA

THE BUSINESS OF SECURITY™

QUESTION 9 *of 12*

ARE WE MEASURING WHAT ACTUALLY MATTERS?

CSA HEALTHCARE SECURITY GOVERNANCE REPORT

HOW DO WE BUILD AND RETAIN A HIGH-PERFORMING SECURITY TEAM?

Healthcare has spent decades building sophisticated measurement systems for clinical quality. From core measures and patient satisfaction scores to readmission rates and infection benchmarks, clinical leaders have developed a shared language for defining what "good" looks like and holding their organizations accountable for achieving it.

Physical security has no equivalent. Tim Leroux, CSA Senior Advisor and former Senior Healthcare Leader, frames the challenge directly.

> "Healthcare security is arguably the least mature function in the enterprise — we don't know how to keep score."
>
> ***Tim Leroux, CSA Senior Advisor • Former Senior Healthcare Leader***

The problem is not that security leaders lack data. Most organizations collect incident reports, response times, and basic activity counts. The problem is that the industry has not reached consensus on what to measure, how to categorize it, or what language to use when reporting it. Leroux identifies the root cause: "You can't have quality without metrics." Without agreed-upon measurement frameworks, security leaders cannot demonstrate program effectiveness, justify investment, or benchmark against peers — and boards cannot evaluate whether their security program is performing or merely existing.

Beyond incident counts

The default metrics in most healthcare security programs — total incidents, response times, arrest counts — measure activity, not effectiveness. They tell leadership how busy the security team is, not whether the organization is becoming safer.

David Flynn, CSA's Chief Administrative Officer, illustrates the problem with a single statistic: "57 assaults could be 57 different situations." Without proper categorization — by type, severity, location, contributing factors, and patient acuity — a headline number tells leadership almost nothing actionable. An emergency department assault involving a patient in psychiatric crisis and a verbal threat in a waiting room are fundamentally different events with different root causes and different prevention strategies. Treating them as equivalent in a board report obscures rather than illuminates.

Leroux introduces a useful framework: the balance between reactive and proactive activity. His benchmark is a 60/40 split — 60 percent of security team time spent on proactive measures such as rounding, training, relationship building, and threat assessment, with 40 percent on reactive response. As he notes, "Proactive is how you build a program." An organization whose security team spends 90 percent of its time responding to incidents is not measuring a high-performing program — it is documenting a reactive one.

HOW DO WE BUILD AND RETAIN A HIGH-PERFORMING SECURITY TEAM?

What clinical staff would tell you

One of the most underused measurement tools in healthcare security sits inside a system that clinical leaders already trust: the staff engagement survey.

Jen Moberg, CSA Senior Advisor and Vice President of Emergency Services, advocates for direct feedback from the workforce security serves. Her approach includes specific survey questions: "Do you see security rounding? When you call, is response timely? Do you feel safe?" These questions measure something that incident counts cannot: whether the people the program is designed to protect experience it as effective.

Leroux formalized this through twice-yearly customer perception surveys at his health system, specifically designed to capture clinical staff feedback on security visibility, responsiveness, and professionalism. He also recommends leveraging the annual employee engagement survey: "Leverage the annual engagement survey — it's usually around safety." Most health systems already ask staff about workplace safety; the insight is in ensuring security leadership has access to those results and uses them as program performance data.

This matters because, as Leroux observes, "feelings and perceptions can be more important than actual security." A program that reduces incidents by 20 percent but leaves clinical staff feeling unprotected has not achieved its objective. Perception data complements operational data — and for a board evaluating program effectiveness, both are essential.

Metrics that drive action

The goal of security measurement is not reporting for its own sake — it is generating information that drives better decisions. Moberg, who has supported CEOs in evaluating security program performance, describes the kind of dashboard that enables executive oversight: retention rates within the security team, workplace violence events categorized by type and severity, response time trends, root cause analysis themes, and patient complaints related to safety or security interactions.

The distinction between leading and lagging indicators is critical. Most security reports focus on lagging indicators — incidents that have already occurred. Leading indicators — training completion rates, proactive rounding frequency, threat assessment volume, staff survey scores — provide the forward-looking intelligence that allows leadership to intervene before problems escalate. A board that only reviews incident counts is driving by looking in the rearview mirror.

IAHSS benchmarking data provides a valuable external reference point, enabling organizations to compare their staffing ratios, budget allocation, and incident rates against peer institutions. However, benchmarking is most powerful when combined with internal trending — tracking your own organization's trajectory over time against clearly defined program objectives. An organization that falls below the IAHSS median on staffing but shows consistent improvement in proactive metrics and staff satisfaction may be outperforming a peer that staffs above the median but cannot demonstrate program outcomes.

HOW DO WE BUILD AND RETAIN A HIGH-PERFORMING SECURITY TEAM?

"Strike demands cite safety. Attrition is expensive. The costs are there — if you're not measuring them, someone else will."

David Flynn, CSA Chief Administrative Officer

The organizations with the most mature measurement approaches integrate security data into existing enterprise reporting structures. When security metrics appear alongside clinical quality, patient experience, and financial performance in board-level dashboards, they receive the same scrutiny, the same accountability, and the same expectation of continuous improvement that clinical programs have long accepted as standard.

The question for your board

If your chief nursing officer presented a quality report that consisted of a single number — total patient incidents — the board would ask for categorization, trending, root cause analysis, and comparison to benchmarks. Does your security reporting meet the same standard?

The organizations that measure security with the same discipline they apply to clinical quality are the ones building programs that demonstrably improve. The starting point is not a new technology platform or a consultancy engagement — it is the decision to hold security performance to the same evidentiary standard the board already applies to every other function it oversees.

REFERENCES

1. International Association for Healthcare Security and Safety. Healthcare Security Industry Benchmarking Data, 2024.
2. Joint Commission. Environment of Care Standards, EC.01.01.01 and EC.02.01.01.
3. CMS. Conditions of Participation: Patient Rights, 42 CFR § 482.13.
4. OSHA. Guidelines for Preventing Workplace Violence for Healthcare and Social Service Workers, OSHA 3148-06R, 2016.
5. ASIS International. Enterprise Security Risk Management Guideline, ASIS ESRM-2019.
6. Bureau of Labor Statistics. Survey of Occupational Injuries and Illnesses (SOII), Healthcare and Social Assistance, 2023.

CSA

THE BUSINESS OF SECURITY™

QUESTION 10 *of 12*

WHY ARE SECURITY, HR, AND CLINICAL TEAMS STILL WORKING IN SILOS?

CSA HEALTHCARE SECURITY GOVERNANCE REPORT

WHY ARE SECURITY, HR, AND CLINICAL TEAMS STILL WORKING IN SILOS?

In most healthcare organizations, physical security, human resources, and clinical operations only interact when something has already gone wrong. A workplace violence incident triggers a joint investigation. A threatening patient prompts a hastily assembled threat assessment. A regulatory citation forces departments that rarely communicate to sit in the same room. The pattern is reactive, episodic, and in desperate need of improvement.

The functions that most directly affect staff safety — security, HR, clinical leadership, compliance, and risk management — typically operate under separate reporting structures, with different metrics, different priorities, and limited visibility into each other's work. The result is not a coordinated safety program but a collection of disparate efforts that intersect only in crisis.

The convergence debate

The security industry has debated "convergence" — the organizational merger of physical security, cybersecurity, and related functions — for decades. Bob Pocica, CSA Practice Area Lead, Corporate Security and former Senior Vice President and Chief Security Officer at McKesson Corporation, offers a practitioner's perspective: "I've been hearing about convergence for 35–40 years. I think it's oversold."

The data supports his skepticism. ASIS Foundation research found that only 24 percent of organizations globally have fully converged their physical and cybersecurity functions. Among those that have, 96 percent report positive outcomes — but the vast majority have not attempted it. In healthcare specifically, convergence rates are among the lowest of any major industry.

The reason is not resistance to collaboration. It is that full organizational merger often creates as many problems as it solves. As Pocica explains, "Convergence does not make sense — one gets prioritized over another." When physical and cybersecurity are placed under a single leader, the function with the larger budget and louder boardroom voice typically dominates. In healthcare, that means cybersecurity — leaving physical security further marginalized rather than elevated.

> "They need to be aligned, not converged."
>
> ***Bob Pocica, CSA Practice Area Lead, Corporate Security***

WHY ARE SECURITY, HR, AND CLINICAL TEAMS STILL WORKING IN SILOS?

Alignment over merger

The distinction Pocica draws is critical for boards evaluating their organizational design. Alignment means that security, HR, clinical operations, compliance, and risk management share information, coordinate response, and report into a common governance structure — without requiring a single reporting line. Ken Senser, CSA's Chief Strategy Officer and former Chief Security Officer at Walmart, describes a practical model of integration under an enterprise risk committee. That committee brings functions together for shared situational awareness and coordinated decision-making — without forcing an organizational chart redesign that healthcare's matrix structures would resist.

CISA's framework for critical infrastructure protection reinforces this approach, advocating cooperative partnerships between IT, facilities management, physical security, and cybersecurity rather than organizational consolidation. The goal is not to merge departments but to ensure that the information each function holds is available to every other function that needs it — before an incident, not after.

The clinical interface

The most consequential silo in healthcare security is not between physical and cybersecurity. It is between security and clinical operations.

Clinical teams conduct daily safety huddles, rapid-cycle improvement meetings, and multidisciplinary rounding as standard practice. These are the mechanisms through which clinical staff identify emerging risks, coordinate responses, and close the loop on patient and staff safety concerns. Yet as Jen Moberg, CSA Senior Advisor and Vice President of Emergency Services, observes: "Security gets forgotten about. They're not invited to root cause analysis or tiered huddles." The result is that clinical staff develop their own ad hoc approaches to safety concerns — approaches that may conflict with or undermine the security program's protocols.

> "Security gets forgotten about. They're not invited to root cause analysis or tiered huddles."
>
> ***Jen Moberg, CSA Senior Advisor and Vice President of Emergency Services***

Moberg's experience with the Certified Professional in Patient Safety credential reinforces the structural nature of this gap: the certification included nothing on workplace violence, staff safety, or interdisciplinary security collaboration. Patient safety and staff safety are treated as separate disciplines, governed by separate standards, despite the fact that the threats to both frequently originate from the same sources and occur in the same clinical environments.

WHY ARE SECURITY, HR, AND CLINICAL TEAMS STILL WORKING IN SILOS?

Tim Leroux, CSA Senior Advisor and former Senior Healthcare Leader, identifies the governance mechanism that should bridge this gap: enterprise risk management. "ERM should be the unifying umbrella," he observes — but in practice, every department conducts its own risk assessments with its own methodology, producing fragmented risk pictures that leadership cannot synthesize into a coherent enterprise view.

Making integration work

The organizations that have achieved effective cross-functional alignment share common structural features. David Flynn, CSA's Chief Administrative Officer, describes the threat assessment team model: a standing multidisciplinary group that includes HR, legal, clinical leadership, and security, with defined protocols for case referral, risk evaluation, and coordinated intervention. The Association of Threat Assessment Professionals recommends this multidisciplinary approach as the standard of practice, and the Joint Commission's Environment of Care standards require organizations to address security risks through processes that inherently demand cross-functional coordination. The model ensures that behavioral concerns identified by any function are evaluated by all relevant functions before they escalate.

John Chilson, CSA Senior Advisor, reinforces this from the HR perspective. His experience at a major integrated health system demonstrated that the most effective security improvements came when HR and security operated as genuine partners — with shared participation in investigations, joint accountability for outcomes, and collaborative approaches to workforce issues that have security implications. The alternative — security and HR operating in parallel, communicating only when forced — leaves gaps that incidents exploit.

Joint training represents another practical integration mechanism. When clinical staff and security officers train together on de-escalation, they build the shared language, mutual understanding, and interpersonal trust that make real-time collaboration possible during a crisis. An emergency department nurse and a security officer who have never trained together will improvise their response. Those who have practiced together will execute a coordinated one.

The organizations with the most mature integration also implement shared reporting: a single incident reporting system accessible to security, HR, clinical risk, and compliance, ensuring that patterns visible only through cross-functional analysis are identified before they produce a serious event.

WHY ARE SECURITY, HR, AND CLINICAL TEAMS STILL WORKING IN SILOS?

The question for your board

When a workplace violence incident occurs in your emergency department, how many separate reporting systems does the information enter? How many departments conduct their own investigation? And does any single governance body see the complete picture — the security response, the HR follow-up, the clinical impact, the regulatory implications, and the root cause — in one place?

Organizations that can answer "yes" to that last question are the ones whose security programs improve continuously. Those that cannot are managing the same risks through fragmented lenses — and wondering why the same problems keep recurring.

REFERENCES

1. ASIS Foundation / AlertEnterprise. The State of Security Convergence in the United States, Europe, and India, 2020.
2. CISA. Cybersecurity and Physical Security Convergence: Action Guide for Critical Infrastructure, 2021.
3. ASIS International. Enterprise Security Risk Management Guideline, ASIS ESRM-2019.
4. Joint Commission. Environment of Care Standards, EC.01.01.01 and EC.02.01.01.
5. OSHA. Guidelines for Preventing Workplace Violence for Healthcare and Social Service Workers, OSHA 3148-06R, 2016.
6. Security Industry Association. Security Convergence 2024: Organizational Drivers and Approaches.

CSA

THE BUSINESS OF SECURITY™

QUESTION 11 *of 12*

ARE WE TRULY PREPARED FOR THE NEXT CRISIS?

CSA HEALTHCARE SECURITY GOVERNANCE REPORT

ARE WE TRULY PREPARED FOR THE NEXT CRISIS?

Every healthcare organization has an emergency management plan. Most have conducted tabletop exercises. Many have invested in mass notification systems, lockdown infrastructure, and crisis communication protocols. But when Bob Pocica, CSA Practice Area Lead, Corporate Security and former Senior Vice President and Chief Security Officer at McKesson Corporation, assesses the state of crisis preparedness in healthcare, his conclusion is direct.

"You can't be secure on hope and luck."

Bob Pocica, CSA Practice Area Lead, Corporate Security

The gap between having a plan and having the capability to execute it under pressure is where most healthcare security programs fail. Emergency plans that have never been stress-tested against realistic scenarios, leadership teams that have never practiced crisis decision-making, and communication systems that have never been activated outside a scheduled drill create an illusion of preparedness that dissolves on contact with a real event.

The compliance trap

Healthcare organizations face extensive regulatory requirements for emergency preparedness. CMS Conditions of Participation mandate emergency plans, communication protocols, training, and testing. Joint Commission Environment of Care standards require organizations to address security risks and demonstrate readiness. State and federal regulations impose additional requirements for specific threat types.

The risk is that compliance becomes the objective, rather than the baseline. An organization that has checked every regulatory box — completed the required drills, filed the required documentation, updated the required plans — may still be fundamentally unprepared for a crisis that does not conform to the scenarios it has practiced. Pocica's assessment of typical hospitals is blunt: reactive rather than proactive, with no planned approach to emerging threats and a persistent skills gap in the security leadership expected to manage crisis response.

The distinction matters because the threats healthcare organizations face are evolving faster than compliance requirements can track. Active assailant events, targeted violence against specific clinicians, coordinated protests, sophisticated theft operations, and infrastructure attacks all require response capabilities that basic regulatory compliance does not build.

ARE WE TRULY PREPARED FOR THE NEXT CRISIS?

Building from crisis

The most effective crisis preparedness programs are often built in the aftermath of a crisis that exposed critical gaps. Ken Senser, CSA's Chief Strategy Officer, experienced this firsthand. As Assistant Director of the FBI's Security Division, he was recruited to rebuild the Bureau's security apparatus following the Robert Hanssen espionage case — a breach that revealed systemic failures in the FBI's internal security. The transformation required not incremental improvement but a fundamental rethinking of how the organization identified, assessed, and responded to insider threats. The discipline Senser built at the FBI — intelligence-led, risk-informed, and integrated across the enterprise — is the same discipline healthcare organizations need, ideally before a crisis forces the conversation.

Jeremy Baumann, CSA's Chief Executive Officer, describes how external crises can accelerate internal governance reform. When a mass shooting occurred at a clinic across the street from one of his client health systems, the organization's governance group reprioritized its entire security agenda within nine days. Over 200 clinics in the system had no meaningful security infrastructure. The event that forced action was not internal — but the vulnerability it exposed was.

> "The question is not whether you will face a crisis — the question is whether your organization will recognize the warning signs and act before it becomes one."
>
> ***Ken Senser, CSA Chief Strategy Officer***

Crisis response capability

Preparedness is not a document. It is a set of organizational capabilities that must be built, tested, and maintained. David Flynn, CSA's Chief Administrative Officer, describes the threat assessment infrastructure that effective organizations deploy: a tiered model with local assessment capability at each facility, regional coordination for complex cases, and enterprise-level oversight for the most serious threats. This structure ensures that behavioral warning signs — whether identified by clinical staff, HR, or security — are evaluated through a consistent methodology and escalated appropriately.

Senser emphasizes the intelligence dimension: the most effective security programs identify threats before they materialize, using behavioral indicators, environmental scanning, and information-sharing partnerships with law enforcement and peer institutions. An organization that relies solely on reactive response — waiting for the incident to occur before activating its plan — has already conceded the most important phase of crisis management.

Jen Moberg, CSA Senior Advisor and Vice President of Emergency Services, identifies a critical gap in most organizations' crisis response cycle: the debrief. "We don't take time to do this," she observes. Clinical operations routinely conduct after-action reviews following adverse events. Security incidents — even

significant ones — are frequently handled without structured debriefing, root cause analysis, or systematic learning. The result is that the same response failures recur because the organization never institutionalized the lessons from the last event.

Organizational resilience

Crisis preparedness in its most mature form extends beyond security response to organizational resilience — the capacity to absorb disruption, maintain critical functions, and recover effectively. The ASIS Organizational Resilience Standard provides a framework that integrates security, preparedness, and business continuity into a unified discipline rather than treating each as a separate compliance requirement.

For healthcare organizations, resilience includes dimensions that other industries do not face. Patient care cannot be suspended during a crisis. Clinical staff who have experienced a violent incident need immediate psychological support and may need extended recovery time. Regulatory reporting obligations activate within hours. Community trust — the foundation of a hospital's relationship with the population it serves — can be damaged in ways that take years to rebuild. Moberg emphasizes the importance of closed-loop communication and defined escalation pathways: every person involved in a crisis response needs to know who is making decisions, what information is being communicated, and when the situation has been resolved.

The organizations that demonstrate genuine resilience treat every incident — including near-misses — as an opportunity to strengthen the system. They invest in realistic scenario-based exercises that test decision-making under pressure, not just procedural compliance. They build recovery plans that address the human impact of crises, not just the operational restoration. And they hold their crisis response capabilities to the same continuous improvement standard they apply to clinical quality.

The question for your board

When did your organization last conduct a crisis exercise that genuinely surprised the leadership team — that revealed a gap no one had anticipated? If the answer is never, or if the exercises consistently confirm that everything is working, the organization is testing its documentation rather than its capability.

The organizations that are truly prepared for the next crisis are the ones that have been uncomfortable during their last exercise. They are the ones whose leaders can describe what they learned, what they changed, and how they verified the change worked. Preparedness is not a state. It is a discipline — and like every discipline in healthcare, it requires investment, accountability, and the expectation of continuous improvement.

ARE WE TRULY PREPARED FOR THE NEXT CRISIS?

REFERENCES

1. CMS. Emergency Preparedness Requirements for Medicare and Medicaid Participating Providers and Suppliers, 42 CFR Parts 403, 416, 418, et al.
2. Joint Commission. Emergency Management Standards, EM.01.01.01 through EM.04.01.01.
3. ASIS International. Organizational Resilience Standard, ASIS SPC.1-2009.
4. ASIS International / Everbridge. Active Assailant Preparedness Survey, 2024.
5. OSHA. Guidelines for Preventing Workplace Violence for Healthcare and Social Service Workers, OSHA 3148-06R, 2016.
6. FEMA. Healthcare Coalition Response Plan Guidance, 2022.

THE BUSINESS OF SECURITY™

QUESTION 12 *of 12*

WHAT DOES SECURITY EXCELLENCE LOOK LIKE FOR US?

CSA HEALTHCARE SECURITY GOVERNANCE REPORT

WHAT DOES SECURITY EXCELLENCE LOOK LIKE FOR US?

Most healthcare systems do not have a security strategy. They have a collection of responses — to incidents, to regulatory requirements, to budget cycles, to the most recent crisis. The result is a function that operates tactically within an organization that governs everything else strategically.

Jeremy Baumann, CSA's Chief Executive Officer, identifies this as the foundational gap: "Healthcare executives never ask their security leader for a strategy." They ask for incident reports, staffing plans, and technology proposals. They rarely ask the question that every other enterprise function is expected to answer: where are we going, how will we get there, and how will we know when we've arrived?

The absence of that question is not an oversight. It reflects an assumption — that security is an operational function to be managed rather than a strategic capability to be developed. That assumption is wrong. The consequences of leaving it unchallenged are measurable, and the path to a different model is well understood.

What excellence looks like

Security excellence in healthcare is not a destination. It is a governed process of continuous improvement — the same discipline that clinical leaders recognize from quality improvement, patient safety, and high-reliability organizing. Ken Senser, CSA's Chief Strategy Officer and former Chief Security Officer at Walmart, describes what it looks like in practice: a function that is intelligence-led, enterprise-integrated, and accountable to the board for outcomes rather than activity. It starts, he says, with a charter from the board — "short, succinct, clear" — that defines the security function's mandate and the standard it is expected to meet.

Brad Brekke, CSA's Chief Business Officer and former Vice President of Assets Protection and Corporate Security at Target Corporation, adds a complementary dimension: security that creates measurable business value, not just risk reduction. When security investments demonstrably lower turnover, reduce liability exposure, improve staff satisfaction, and protect the organization's reputation, the function earns its place in enterprise strategy. When it cannot demonstrate those outcomes, it remains a cost to be controlled.

> "Most healthcare systems don't have a security strategy. They have a collection of reactions."
>
> ***Jeremy Baumann, CSA Chief Executive Officer***

WHAT DOES SECURITY EXCELLENCE LOOK LIKE FOR US?

The integrated framework

A mature healthcare security program is not built on any single initiative. It is built on an integrated framework of five pillars.

Governance ensures that physical security receives the same board-level oversight, reporting cadence, and strategic attention as cybersecurity, clinical quality, and financial performance. Executive accountability establishes clear ownership of security risk at the leadership level, with documented decision-making and defined responsibility for outcomes. Enterprise consistency means that standards, policies, and capabilities are coordinated across every facility and setting — not reinvented at each site. Program maturity requires structured investment in people, technology, training, and measurement — the same organizational development discipline healthcare applies to every other critical function. And business outcomes mean that security investment is evaluated against the same return-on-investment logic applied to clinical programs, capital expenditures, and technology deployments.

These are not five separate initiatives. They are one integrated approach — and the organizations that achieve security excellence are the ones that pursue all five simultaneously, governed by a strategic plan that sequences investment against risk and measures progress against defined milestones.

The clinical alignment test

The simplest test of security program maturity is whether it operates with the same governance discipline the organization applies to clinical care. Senser frames the security function's purpose in clinical terms: "The purpose of security is to facilitate healing." When security enables clinicians to focus on patient care without fear for their own safety, it is fulfilling its mission. When security protocols impede care delivery, create adversarial relationships with clinical staff, or operate without clinical input, the program has lost alignment with the organization it serves.

Jen Moberg, CSA Senior Advisor and Vice President of Emergency Services, describes the aspiration: "Security in the fabric of every meeting — a culture of care and security together." That integration only happens through sustained engagement — joint training, shared governance, common goals, and the kind of daily collaboration that makes security a trusted partner in the clinical mission rather than an external function called only in crisis.

The case for independent assessment

Healthcare organizations routinely engage independent reviewers for clinical quality, financial audit, regulatory compliance, and information security. The logic is straightforward: internal teams, regardless of competence, benefit from external perspective. Institutional familiarity can obscure gaps that an independent assessment would identify. Relationships built over years can make it difficult to deliver candid evaluations.

WHAT DOES SECURITY EXCELLENCE LOOK LIKE FOR US?

The same logic applies to physical security. John Chilson, CSA Senior Advisor, frames it from the perspective of an organizational leader who has seen both sides of the equation.

> "Don't go back to the same old process. Utilize an independent organization to come in and give an independent view, without the attachment or relationships that might bias one to overlook things."
>
> ***John Chilson, CSA Senior Advisor***

The value of independent assessment is not that internal teams are inadequate. It is that the combination of internal knowledge and external perspective produces better outcomes than either alone. The organizations that have achieved the most significant security transformations have consistently partnered with advisors who bring enterprise-level experience, cross-industry benchmarks, and the ability to deliver candid assessments to boards and executive teams.

The starting point

Defining security excellence is itself a form of self-assessment. It requires an honest evaluation of where the program operates today, and a clear articulation of where the demands of modern healthcare require it to operate.

The starting point is not a technology purchase, a staffing increase, or a policy revision. It is a decision: to hold physical security to the same governance, investment, and performance standards the organization already applies to every other function it considers essential. Clinical quality, patient experience, financial stewardship, regulatory compliance, and cybersecurity all operate under that standard. Physical security can and should meet it.

The path forward is clearer than most organizations realize. The frameworks exist. The evidence base is established. The expertise is available. The question is whether leadership will ask for a strategy — and then hold the organization accountable for executing it.

WHAT DOES SECURITY EXCELLENCE LOOK LIKE FOR US?

REFERENCES

1. ASIS International. Enterprise Security Risk Management Guideline, ASIS ESRM-2019.
2. ASIS International. Chief Security Officer Guideline, ASIS GDL CSO-2004.
3. International Association for Healthcare Security and Safety. Healthcare Security Industry Guidelines, 13th Edition.
4. Joint Commission. Environment of Care Standards and Leadership Standards, 2024.
5. American Hospital Association. (2025). The Burden of Violence to U.S. Hospitals: A Comprehensive Assessment of Financial Costs and Other Impacts of Workplace and Community Violence. Prepared by Harborview Injury Prevention & Research Center, University of Washington School of Medicine.
6. CMS. Conditions of Participation: Patient Rights, 42 CFR § 482.13.

THE BUSINESS OF SECURITY™

CONCLUSIONS AND RECOMMENDATIONS

CSA HEALTHCARE SECURITY GOVERNANCE REPORT

ARE WE TRULY PREPARED FOR THE NEXT CRISIS?

The twelve questions examined in this report do not describe twelve separate problems. They describe one: physical security governance in healthcare has not kept pace with the demands placed on it. The regulatory environment has intensified. The financial and human cost of inaction is quantified. The governance disciplines that would close the gap are well understood and already deployed, in the same organizations, for cybersecurity, clinical quality, and financial performance. The question is whether healthcare leadership will extend that discipline to physical security — deliberately, systematically, and before the next crisis makes the decision for them.

The conclusions that follow are organized around five areas where action is most consequential. The recommendations that accompany them are framed for the leaders best positioned to act: the board, the executive committee, and the security leader. They are sequenced by priority, not alphabetically — because in governance, sequence matters. An organization that begins with measurement before it has established accountability will measure the wrong things. One that invests in technology before it has governance will purchase hardware, not security.

Governance is the precondition for everything else

No security improvement sustains without governance to support it. Technology without governance produces theater. Investment without governance produces spending without accountability. Leadership without governance produces capability without authority. Every organization that has achieved a material improvement in physical security effectiveness has begun in the same place: establishing clear board-level oversight, defined reporting structures, and explicit decision rights. Every organization that has failed to sustain improvement has done so because governance was treated as infrastructure rather than foundation — assumed rather than built.

The governance model healthcare needs for physical security is not hypothetical. Most boards have already built it for cybersecurity: dedicated committee oversight, regular risk reporting with defined metrics, documented accountability, and strategic investment frameworks that connect spending to outcomes. That architecture translates directly. The capability gap is not about inventing something new. It is about extending existing governance discipline to a domain that has been waiting for it.

For the board: establish a formal reporting cadence for physical security risk, equivalent in frequency and rigor to cybersecurity reporting. Define which security risks require board-level visibility and decision, and which are delegated to the executive committee. Assign a board committee — risk, audit, or a dedicated safety committee — with explicit oversight responsibility. Receive and review an annual security program assessment, including independent evaluation where internal perspective is insufficient. Ask whether the organization has a security strategy — not a security plan, but a strategy: where the program is going, how it will get there, and how progress will be measured.

CONCLUSIONS AND RECOMMENDATIONS

For the executive committee: establish an enterprise security governance committee with representation from security, HR, clinical operations, legal, compliance, risk management, and facilities. Give that committee authority to make decisions and allocate resources, not merely to exchange information. Ensure that the security leader has direct access to the executive committee — not through intermediaries — for risk escalation and strategic discussion. Document the organization's risk tolerance for physical security, the same way it documents risk tolerance for financial and compliance risks.

Structure and leadership capability are governance decisions

Where security sits in the organizational hierarchy and who leads it are not administrative choices. They are governance decisions that determine what the function can accomplish. A security leader buried within facilities management, without access to the executive committee and without the business competencies to engage clinical and financial leadership as a peer, cannot govern security at the level the organization requires. The structure produces the outcome.

The ASIS International Chief Security Officer standard is unambiguous: strategic, business, and interpersonal competencies are of greater importance than technical security skills. Business acumen is the competency without which the others cannot be fully effective. Healthcare applies this logic to every other executive role. The same standard applied to security leadership selection, development, and evaluation will produce a materially different caliber of leader — and a materially different security program.

For the board: evaluate whether the security leader's organizational position provides genuine access to executive leadership, or whether that access is filtered through intermediaries with different priorities. Ask whether you would be comfortable with your security leader presenting a strategic security plan to this committee. If not, the question is whether the leader needs development — or whether the organization has never asked for a strategy and therefore never built the leadership capability to deliver one.

For the executive committee: apply the same competency framework to security leadership selection and evaluation that you apply to other executive roles. Define the reporting structure that gives security the authority, visibility, and cross-functional access the role requires. Invest in the development of security leadership capability — business acumen, financial fluency, stakeholder management — with the same intentionality applied to clinical and operational leadership development.

Accountability must be distributed and documented

The most consequential misunderstanding in healthcare security governance is the belief that the security department owns security risk. It does not. Management owns the risk. The security leader identifies it, assesses it, and recommends mitigation. The decision to accept, transfer, or address that risk belongs to the operational leaders and, ultimately, to the board. When that distinction is unclear, organizations concentrate accountability in the function with the least authority to act on it — and create the conditions for exactly the failures they are trying to prevent.

CONCLUSIONS AND RECOMMENDATIONS

Effective accountability requires architecture: documented risk decisions, defined escalation paths, and a reporting structure that ensures critical risk information reaches the people with the authority to act on it without being filtered, softened, or delayed. It also requires persistence. A security leader who raises a risk once and accepts a declination without follow-up has not fulfilled the advisory obligation. The risk that is real on Monday is still real on Friday. Advocacy is part of the role.

For the board: confirm that a formal risk escalation pathway exists for physical security — that critical risk information reaches the board directly, not only through the chain of operational leadership. Ensure that risk acceptance decisions are documented and attributable to the leaders who made them. Review whether physical security is included in the organization's enterprise risk management framework, or whether it operates as a parallel, disconnected process.

For the security leader: establish a Senior Risk Advisory structure with defined escalation protocols and documented decision rights at each organizational level. Confirm every significant risk communication in writing. Track risk recommendations through to resolution: accepted, modified, or formally declined — with declinations owned by the leader with the authority to make them. Treat the advisory role as a genuine professional obligation, not a procedural step.

Enterprise consistency is a governance requirement, not an operational afterthought

When a board approves a security strategy, it approves it for the entire organization. If that strategy is implemented rigorously at some facilities and loosely at others — or not at all at recently acquired sites — the board's governance is aspirational rather than actual. Enterprise consistency is not about imposing identical operations at every location. It is about establishing a common framework — shared standards, consistent technology platforms, unified policies, and enterprise oversight — within which appropriate local variation is both expected and governed.

The financial case for consistency is as compelling as the governance case. Multi-facility systems that have consolidated security spending data routinely discover that actual investment is two to four times what leadership assumed, with significant technology assets untracked and unmanaged. Consolidation creates visibility. Visibility enables accountability. Accountability enables improvement. Organizations that have achieved enterprise consistency in physical security have done so the same way they achieved it in cybersecurity: by treating the function as a governance priority and building the structures that governance requires.

For the executive committee: commission a comprehensive inventory of security spending, technology, staffing, and policy compliance across every facility. Treat the results as the baseline against which enterprise consistency will be measured. Establish system-wide standards for technology platforms, policy frameworks, and program design, with a defined integration process for acquired facilities. Appoint enterprise-level security leadership with the authority and scope to drive consistency across the system, not just at flagship locations.

CONCLUSIONS AND RECOMMENDATIONS

Program maturity requires the same investment discipline applied to clinical quality

Healthcare has built sophisticated systems for clinical quality improvement: defined metrics, agreed measurement frameworks, independent benchmarking, structured accountability, and the expectation of continuous improvement. Physical security has none of that infrastructure at scale. Most security programs measure activity, not effectiveness. Most security teams are hired without the development investment that would allow them to grow. Most security technology is purchased without the governance that would allow it to perform. And most security investments are made without a business case that leadership can evaluate the way it evaluates any other capital request.

Closing this gap does not require resources that healthcare organizations do not have. It requires applying resources already committed to security more deliberately: with a strategic plan that sequences investment against risk, metrics that measure outcomes rather than activity, talent practices that treat security officers as professionals worth developing, and technology governance that connects hardware to operational protocols and measurable results.

For the board: require that security investment be presented with the same business case discipline applied to clinical programs and capital expenditures. Establish a baseline for security program measurement — staffing ratios, incident categorization, staff perception data, response time trends — and review progress against it annually. Treat security officer development, turnover, and training investment as program quality indicators, the same way nursing workforce metrics are treated as indicators of clinical program quality.

For the security leader: develop a multi-year security master plan that prioritizes investment against risk, defines measurable milestones, and translates security requirements into the financial language that CFOs and boards use to evaluate competing priorities. Build a measurement framework that includes both leading indicators — training completion, proactive rounding rates, threat assessment volume — and lagging indicators such as incident trends, staff satisfaction, and turnover. Make the business case in data the organization is already tracking.

The standard to meet

The standard against which physical security governance should be measured is not a security standard. It is the governance standard the organization already applies to every other function it considers essential. Clinical quality is governed with rigor because the board decided it should be. Financial stewardship is governed with rigor because the board decided it should be. Cybersecurity is governed with rigor because the board decided it should be. The same decision, applied to physical security, will produce the same result.

CONCLUSIONS AND RECOMMENDATIONS

The organizations that have made that decision — that have restructured security governance, elevated security leadership, invested in program maturity, and built the accountability architecture that sustains improvement — are better positioned to protect their people, satisfy their regulators, and deliver the stable operating environment that every other strategic initiative depends on. The path to that position is clearer than most organizations realize. The frameworks exist. The evidence base is established. The expertise is available.

What is required is the decision to begin — and the governance to ensure that what begins, continues.

THE BUSINESS OF SECURITY™

BIBLIOGRAPHY

CSA HEALTHCARE SECURITY GOVERNANCE REPORT

BIBLIOGRAPHY

The following references are cited across the chapters of this report. Sources are grouped by organization or body to aid navigation. Where a source appears in multiple chapters, it is listed once here.

American Hospital Association

American Hospital Association. (2025). The Burden of Violence to U.S. Hospitals: A Comprehensive Assessment of Financial Costs and Other Impacts of Workplace and Community Violence. Prepared by Harborview Injury Prevention & Research Center, University of Washington School of Medicine.

ASIS International

ASIS International. (2004). Chief Security Officer (CSO) Guideline (GDL CSO 06 2004). Competency framework for senior security leadership, including five core areas: leadership and management, analyzing the business, risk management, business acumen, and emotional intelligence.

ASIS International. Chief Security Officer (CSO) Organizational Standard (ASIS CSO.1). ANSI-approved national standard defining the senior security executive role, functions, and competencies.

ASIS International. (2012). Security Management Standard: Physical Asset Protection (PAP). Lifecycle management framework for security technology systems.

ASIS International. (2019). Enterprise Security Risk Management (ESRM) Guideline. Four foundational pillars: holistic risk management, stakeholder partnership, transparency, and governance. Four roles of responsibility: asset owners, security professionals, stakeholders, and top management.

ASIS International. ESRM Maturity Model. Assessment framework for program strategy, governance, implementation, and alignment of security risk mitigation.

ASIS International. Organizational Resilience Standard, ASIS SPC.1-2009.

ASIS International. (2023). "From CSO to SSE: Expanding Leadership Roles in Security." Security Management. Analysis of business acumen as the "nuclear element" of the CSO role.

ASIS Foundation / AlertEnterprise. (2020). The State of Security Convergence in the United States, Europe, and India.

ASIS International / Everbridge. (2024). Active Assailant Preparedness Survey.

Bureau of Labor Statistics

Bureau of Labor Statistics. (2020). Workplace Violence in Healthcare, 2018. U.S. Department of Labor.

Bureau of Labor Statistics. (2022). Survey of Occupational Injuries and Illnesses. Healthcare workers experience workplace violence at five times the rate of the general workforce.

Bureau of Labor Statistics. (2023). Survey of Occupational Injuries and Illnesses (SOII), Healthcare and Social Assistance.

Bureau of Labor Statistics. Occupational Employment and Wage Statistics, Security Guards (SOC 33-9032), May 2024.

Centers for Medicare & Medicaid Services

Centers for Medicare & Medicaid Services. Conditions of Participation for Hospitals (42 CFR §482).

Centers for Medicare & Medicaid Services. Conditions of Participation: Patient Rights, 42 CFR § 482.13.

Centers for Medicare & Medicaid Services. Emergency Preparedness Requirements for Medicare and Medicaid Participating Providers and Suppliers, 42 CFR Parts 403, 416, 418, et al.

Cybersecurity and Infrastructure Security Agency (CISA)

CISA. (2021). Cybersecurity and Physical Security Convergence: Action Guide for Critical Infrastructure.

BIBLIOGRAPHY

European Union Agency for Cybersecurity (ENISA)

European Union Agency for Cybersecurity (ENISA). (2012). Introduction to Return on Security Investment. ROSI methodology: (ALE − mALE − Cost) / Cost framework for security investment evaluation.

Federal Emergency Management Agency (FEMA)

FEMA. (2022). Healthcare Coalition Response Plan Guidance.

HHS Office of Inspector General

U.S. Department of Health and Human Services, Office of Inspector General. (2023). General Compliance Program Guidance (GCPG). Seven elements of an effective compliance program, board oversight requirements, quarterly engagement with compliance officer, annual risk assessment.

International Association for Healthcare Security and Safety (IAHSS)

International Association for Healthcare Security and Safety. Healthcare Security Industry Guidelines, 13th Edition. Multi-disciplinary, risk-based program design standards; multi-year security master plan development; staffing benchmarks (73 percent personnel allocation); technology integration standards.

International Association for Healthcare Security and Safety. Healthcare Security Industry Benchmarking Data, 2024.

International Association for Healthcare Security and Safety. Security Design Guidelines for Healthcare Facilities, 4th Edition.

The Joint Commission

The Joint Commission. Environment of Care Standards (EC.01.01.01): Written plan requirements for security management, risk coordination, and leadership reporting across all facilities.

The Joint Commission. Environment of Care Standards (EC.02.01.01): Security systems maintenance, testing requirements, and technology integration standards for healthcare facilities.

The Joint Commission. Environment of Care Standards (EC.04.01.01): Annual evaluation of environment of care management plans by governing body or designated leadership.

The Joint Commission. Leadership Chapter (LD.04.04.05): Reporting relationships between leadership and responsible entities for environment of care.

The Joint Commission. Emergency Management Standards, EM.01.01.01 through EM.04.01.01.

The Joint Commission. (2025). Sentinel Event Data: 2024 Annual Review.

The Joint Commission. (2025). Sentinel Event Policy (SE). Classifies assault, sexual abuse/assault, and homicide of patients, staff, practitioners, trainees, visitors, or vendors on hospital premises as reviewable sentinel events.

National Institute of Standards and Technology (NIST)

National Institute of Standards and Technology. Cybersecurity Framework (CSF). Enterprise-wide standards for risk management referenced as a model for consistent security governance.

NSI Nursing Solutions

NSI Nursing Solutions, Inc. (2024). National Health Care Retention & RN Staffing Report. Average cost of turnover for a registered nurse: approximately $61,000.

Occupational Safety and Health Administration (OSHA)

Occupational Safety and Health Act of 1970, Section 5(a)(1) (General Duty Clause).

OSHA. (2016). Guidelines for Preventing Workplace Violence for Healthcare and Social Service Workers, OSHA 3148-06R.

BIBLIOGRAPHY

U.S. Securities and Exchange Commission

U.S. Securities and Exchange Commission. (2023). Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (Release Nos. 33-11216; 34-97989). Adopted July 26, 2023. Requires material incident disclosure within four business days and annual board oversight reporting.

U.S. Sentencing Commission

U.S. Sentencing Commission. Organizational Sentencing Guidelines, §8B2.1. Governing authority requirement to be knowledgeable about compliance program content and operation.

Legislation

California Senate Bill 553 (SB 553). Effective July 1, 2024. First general industry workplace violence prevention standard in the United States.

Save Healthcare Workers Act. H.R. 3178/S. 1600, 119th Congress. Introduced May 5, 2025. Would make assaulting an on-duty hospital worker a federal crime punishable by up to ten years' imprisonment.

Additional state healthcare workplace violence legislation: New York (Labor Law §27-b), Connecticut (PA 21-174), Minnesota (Minn. Stat. §144.566), Illinois (Health Care Violence Prevention Act, 210 ILCS 160), Oregon (ORS 654.414), Washington (WAC 296-800-140), Maine (26 MRSA §806), Maryland (Md. Code, Health-General §19-353), New Jersey (N.J.S.A. 26:2H-5.19).

Other sources

Security Industry Association. (2024). Security Convergence 2024: Organizational Drivers and Approaches.

UC Berkeley Labor Center. (2025). Demographic and Job Characteristics of NYC's Security Guard Workforce.

THE BUSINESS OF SECURITY™

ABOUT CSA

ABOUT CSA

The findings in this report reflect the combined experience of the Corporate Security Advisors team — practitioners who have led security transformations at the highest levels of healthcare, corporate, law enforcement, and clinical operations. Their backgrounds are the evidence base from which this report draws.

Jeremy Baumann, CPP

Founder and Chief Executive Officer

Jeremy Baumann founded Corporate Security Advisors with a singular focus: helping healthcare organizations build security programs that operate at the strategic level the industry demands. A Certified Protection Professional with decades of experience leading security transformations across major health systems, Baumann has built and rebuilt security governance structures at organizations ranging from single-facility hospitals to multi-system enterprises with hundreds of locations. His engagements have addressed every dimension of the security governance challenge — structure, leadership, technology, investment, and measurement — and his practitioner perspective on what separates programs that improve from those that stall informs every chapter of this report. Baumann is a frequent speaker on healthcare security governance and a recognized voice in the field on the relationship between executive leadership and security program effectiveness.

Brad Brekke

Founder and Chief Business Officer

Brad Brekke brings to CSA a career built at the intersection of enterprise security and business strategy. As Vice President of Assets Protection and Corporate Security at Target Corporation, he led one of the most sophisticated retail security operations in the country — overseeing a multi-decade transformation from a people-intensive model to a technology-enabled enterprise security program operating at national scale. That experience, and the investment discipline it required, shapes Brekke's approach to healthcare security: the business case for security investment must be built in the language that CFOs and boards already use, and the return must be measurable in outcomes the organization already tracks. At CSA, Brekke leads the firm's business development and client engagement strategy, bringing the rigorous investment and governance discipline of enterprise corporate security to healthcare systems at every stage of program maturity.

Ken Senser

Chief Strategy Officer

Ken Senser's career spans the highest levels of security leadership. In enterprise he served as Chief Security Officer at Walmart, and in federal law enforcement he served as Assistant Director of the FBI's Security Division. He was recruited to rebuild the Bureau's internal security apparatus following the Robert Hanssen espionage case — one of the most consequential security failures in FBI history. The transformation required not incremental improvement but a fundamental rethinking of how the organization identified, assessed, and responded to insider threats. The discipline Senser built at the FBI — intelligence-led, risk-informed, and integrated across the enterprise — is the same discipline he brings to healthcare security strategy. At CSA, Senser leads the firm's strategic direction, with particular focus on crisis preparedness, intelligence-led security, and the board-level governance frameworks that define security excellence. His view that effective security begins with a clear charter from the board — short, succinct, and accountable — anchors CSA's approach to governance design.

ABOUT CSA

David Flynn, MBA

Chief Administrative Officer

David Flynn oversees the operational and administrative infrastructure of Corporate Security Advisors, bringing an MBA-grounded business perspective to the operational dimensions of security program management. His experience spans the financial, workforce, and organizational dynamics of security investment — including the labor relations implications of workplace violence, the hidden costs of security workforce underinvestment, and the structural causes of the talent pipeline problem that most healthcare security programs have not yet addressed. Flynn's insight that organizations routinely expect a highly capable security professional while budgeting for an entry-level position — and that the costs of that mismatch are measurable in turnover, liability, and operational disruption — reflects the financial lens he brings to every engagement. His observation that 'we call John' is a red flag for single-person dependency has become a diagnostic touchstone for evaluating enterprise security program fragmentation.

Bob Pocica

Practice Area Lead, Corporate Security

Bob Pocica brings to CSA the perspective of a practitioner who has led security at the enterprise level of one of the largest and most complex organizations in healthcare. As Senior Vice President and Chief Security Officer at McKesson Corporation, he built and managed an enterprise security function with responsibility across a sprawling, multi-sector organization. His framework for security accountability — management owns the risk, the CSO provides insight, guidance, and mitigation — has become a defining principle of CSA's advisory approach, and his experience establishing Senior Risk Advisory Boards with documented escalation protocols and formal decision rights reflects the governance architecture that distinguishes mature security programs from reactive ones. Pocica's direct practitioner voice, including his assessment that too many security leaders know lights, locks, and alarms but lack the business fluency to operate at the executive level, is among the most frequently cited perspectives in this report.

John Chilson, MA-HR

Senior Advisor

John Chilson brings more than thirty years of healthcare leadership experience to his advisory role at CSA, with a career that has spanned senior human resources leadership across complex health systems and interim security leadership at a Level I Trauma Center. That combination — deep HR expertise and direct security operational experience — gives Chilson a distinctive perspective on the workforce dimensions of security program transformation. His work rebuilding a security team on the verge of collapse — reducing turnover from 25–30 percent to under 10 percent through structured development, individual accountability, and genuine investment in officer growth — demonstrates what becomes possible when healthcare organizations apply the same organizational development discipline to security that they apply to clinical teams. Chilson's emphasis on simulation-based training, behaviorally grounded hiring, and individual development plans as the foundation of high-performing security teams shapes CSA's approach to security workforce strategy.

ABOUT CSA

Tim Leroux

Senior Advisor

Tim Leroux brings to CSA the experience of a security leader who built and sustained a mature security program at one of the nation's largest and most complex integrated health systems. As Director of Security Governance and Quality Improvement at Kaiser Permanente, Leroux developed the measurement frameworks, governance structures, and cross-functional integration models that distinguish a high-performing security program from a reactive one. His observation that healthcare security is arguably the least mature function in the enterprise — and his corollary that you cannot have quality without metrics — reflects both the scale of the challenge and the clarity of the path forward. Leroux's framework for balancing proactive and reactive security activity, his advocacy for customer perception surveys as a core program measurement tool, and his experience navigating the policy development and governance challenges of enterprise-scale security programs inform CSA's approach to measurement, maturity assessment, and program design.

Jen Moberg

Senior Advisor

Jen Moberg occupies a distinctive position in the CSA advisory team: she brings the perspective of a clinical operations leader who has worked at the intersection of emergency services and security for her entire career, and who continues to serve as Vice President of Emergency Services alongside her advisory role. That dual vantage point — security as seen from the clinical side of the wall, and emergency operations as understood by someone who has built and led them at scale — gives Moberg an unusually grounded view of where the gaps between security and clinical operations actually cost organizations. Her experience with cross-functional hiring panels, joint security and clinical training, and the integration of security into clinical safety huddles and root cause analysis processes reflects the operational reality that security program effectiveness ultimately depends on whether clinical staff experience security as a trusted partner or an external function called only in crisis. Moberg's work on crisis response, de-escalation, and closed-loop communication in emergency situations shapes CSA's advisory approach to preparedness and clinical integration.

About Corporate Security Advisors

Corporate Security Advisors is the American Hospital Association's first Preferred Physical Security Advisory Services Provider. CSA works with healthcare organizations across the country to build security programs that operate at the strategic level the industry demands — governed by boards, led by executives with the competencies the role requires, consistent across the enterprise, and measured against outcomes that matter. CSA's advisory services span governance design, security program assessment, leadership development, technology strategy, investment planning, and crisis preparedness. Every engagement draws on the direct practitioner experience of a team that has led security transformations at the highest levels of healthcare, corporate security, federal law enforcement, and clinical operations.

For more information, visit corporatesecurityadvisors.com.

THE ART OF STRATEGY

THOSE WHO ARE VICTORIOUS PLAN EFFECTIVELY AND CHANGE DECISIVELY. THEY ARE LIKE A GREAT RIVER THAT MAINTAINS ITS COURSE BUT ADJUSTS ITS FLOW... THEY HAVE FORM BUT ARE FORMLESS. THEY ARE SKILLED IN BOTH PLANNING AND ADAPTING AND NEED NOT FEAR THE RESULT OF A THOUSAND BATTLES: FOR THEY WIN IN ADVANCE, DEFEATING THOSE THAT HAVE ALREADY LOST.

SUN TZU

CHINESE WARRIOR, PHILOSOPHER, ~500 B.C.

CSA THE BUSINESS OF SECURITY ™

Learn more at: corporatesecurityadvisors.com