Navigating Physical Security in the Wake of M&A

A strategic approach for security leaders

siteowl®

TABLE OF CONTENTS

01 Introduction

02 The new landscape of security post-M&A

03 Identifying risks and setting the strategy

04 Integrating systems and cultures

05 Building resilience and operational efficiency

06 Conclusion

INTRODUCTION

Welcome to the SiteOwl Guide to Navigating Physical Security Post-M&A.

If you're steering the ship through the choppy waters of a merger or acquisition, this guide's your compass. Mergers and acquisitions shake up organizations—there's no sugarcoating it. But while everyone's busy aligning business operations and strategies, physical security tends to slide down the priority list. Here's where we step in. We're here to shine a light on how M&A activities can be a challenge to navigate for physical security teams and to arm you with actionable strategies to keep your guard up during these times of organizational change.

Who is this e-book for?

- **Security Leader or Executive**
  At the helm of your organization's security strategy, looking to steer your team through the integration of new assets and cultures.

- **IT and Security Operations Manager**
  On the front lines, ensuring that the day-to-day security operations run smoothly, even as the ground shifts under your feet.

- **Facility Manager**
  Tasked with the safety and security of more square footage than ever before, seeking smart ways to expand your reach.

- **Risk Management Professional**
  With an eye for potential pitfalls and a knack for planning, you're the one looking to mitigate risks before they turn into realities.

What is covered?

Navigating the complexities of mergers and acquisitions (M&A) is no small feat—especially when it comes to ensuring your physical security strategy is sound. This eBook is is designed to cover essential ground to safeguard your organization's future.

Here's what we are unpacking:

Chapter 1	**The new landscape of security post-M&A** We start by painting the big picture: How does M&A activity affect your physical security strategy? Understand the challenges and opportunities that arise from expanding your operational footprint.
Chapter 2	**Identifying risks and setting the strategy** With change comes risk. This chapter focuses on identifying potential security vulnerabilities early in the M&A process and setting a proactive strategy to address them. Learn how to conduct effective risk assessments and prioritize your actions.
Chapter 3	**Integrating systems and cultures** Integration is more than just a technical challenge; it's about harmonizing different security cultures. Discover strategies for merging disparate security systems and protocols, and learn how to foster a unified security culture across your newly expanded organization.
Chapter 4	**Building resilience and operational efficiency** Resilience is key to navigating the post-M&A landscape. Explore how to build operational resilience through effective security management practices, leveraging technology to enhance efficiency and responsiveness.
Conclusion	**Charting your path forward** We wrap up with a look ahead, focusing on how to maintain momentum and continuously improve your security posture. Learn how to leverage the lessons from your M&A experience to prepare for future challenges and opportunities.

Each chapter is packed with insights, actionable advice, and real-world strategies designed to empower security leaders like you to navigate the M&A process with confidence.

CHAPTER 1

The new landscape of security post-M&A

When companies merge or get acquired, the result deeply reshapes the physical security landscape, one where physical security can easily be compromised. This transformation goes beyond mere operational adjustments. It's about knitting together disparate systems into a unified security blanket that covers the newly formed entity in its entirety. This often involves navigating fragmented systems, diminished visibility, and the need for real-time situational awareness across vast geographical areas.

Physical security is often relegated to the backseat in the M&A process, overshadowed by financial and operational priorities. Yet, overlooking the integration of security measures can have far-reaching consequences.

> *Mergers and acquisitions (M&A) '...leave critical security systems vulnerable', making the joining of different entities a complex challenge for maintaining a secure environment."*
>
> *- Security InfoWatch*

1.1 Visibility: The first casualty

One of the most immediate effects of M&A activity on physical security is the sudden blur in visibility. As the organizational landscape expands, so does the challenge of maintaining a clear, unified view of all physical assets and threats across new and diverse locations.

Key visibility challenges:

- **Fragmented oversight**

  Monitoring sprawling estates from a single vantage point becomes a Herculean task, introducing delays and potential security oversights.

- **Varying security standards**

  The merger of two entities often brings together mismatched security priorities and investments, leaving gaps that need bridging.

- **Increased footprint**

  More physical locations, buildings, and access points significantly expand the attack surface that needs protecting.

- **Managing access & credentials**

  Keeping track of who has access to which facilities, merging badge or key systems, and handling employee offboarding becomes exponentially more complex.

- **Incident response confusion**

  Without a unified incident response framework, the expanded entity may struggle with slow reaction times and miscommunication during critical moments.

- **Increasing costs**

  Security upgrades post-M&A can lead to unexpected financial burdens.

1.2 Why M&A is particularly challenging for physical security

M&A activities present a unique puzzle for physical security, where the pieces don't always fit neatly together. Proactive planning becomes non-negotiable here, encompassing thorough risk assessments, the formulation of an integrated security strategy, and the exploration of technological solutions to bridge any gaps.

A cautionary tale underscores the importance of this proactive stance:

A company, post-acquisition, faced a sudden revelation—their new assets required an immediate security overhaul, costing upwards of $2 million upfront and an additional $3 million annually for operations.

Source: Security InfoWatch (M&A Security Risk)

This example underscores the critical importance of integrating security considerations into the merger and acquisition process to avoid unforeseen expenses and ensure the seamless integration of security practices.

Next, we'll share some strategic frameworks and innovative solutions to overcome the hurdles posed by M&As, focusing on ensuring seamless security integration and maintaining a robust security posture.

CHAPTER 2

Identifying risks and setting the strategy

Mergers and acquisitions (M&A) offer organizations the potential for expanded market reach, diverse products, and greater financial power. However, successfully integrating physical security strategies during an M&A presents serious challenges.

While security professionals often focus on immediate risks like inconsistent standards and access control, they can overlook critical aspects of lifecycle management. These include:

Visibility
Tracking and understanding the full scope of security assets across all merged entities.

Inventory
Maintaining accurate records of all physical security devices.

Vendor management
Streamlining relationships and contracts with numerous security service providers.

Documentation
Ensuring crucial security policies, procedures, and records are centralized and accessible.

Addressing these lifecycle management issues is essential for a smooth and secure M&A transition.

2.1 Identifying and mitigating potential security risks early

Mergers and acquisitions, while potentially transformative, significantly increase an organization's physical security risk profile. Being proactive from the very beginning is key to a smooth transition and maintaining robust security for the newly formed entity.

Don't let physical security become an afterthought! In the early stages of an M&A, conduct a thorough assessment of both companies' security posture. This is essential for:

- **Uncovering hidden vulnerabilities**

  Existing security weaknesses might not be immediately obvious. Deep due diligence can prevent unpleasant surprises later.

- **Cost-effective mitigation**

  Early planning allows for informed budgeting and avoids costly emergency fixes post-merger.

- **Maintaining business continuity**

  Addressing immediate risks minimizes disruptions and ensures the protection of sensitive data throughout the process.

INSIGHT # 1

Physical Security System Lifecycle Assessment

SiteOwl's Physical Security System Lifecycle Assessment is a straightforward and actionable tool designed to help security directors identify potential risks and areas for improvement in their security systems.

The assessment will help you gain insights into:

- The current state of your physical security system lifecycle practices.
- Strategies for optimizing resource utilization.
- Areas where security operations can be improved.
- More efficient collaboration with integrators.
- Ways to reduce costs and increase efficiencies.
- Opportunities for risk reduction.

Completing the Security System Lifecycle Assessment

- The current state of your physical security system lifecycle practices.
- Strategies for optimizing resource utilization.
- Areas where security operations can be improved.

2.2 The power of lifecycle management

Thorough security assessments are a non-negotiable part of finalizing any M&A deal. However, a common blind spot for many companies is the lifecycle management of their security systems. It's easy to get caught up in the immediate assessment of access control, surveillance, and policies, but this narrow view leaves organizations vulnerable long-term.

What does lifecycle management in this context mean? It involves:

Centralized visibility

Gaining a complete and up-to-date understanding of your entire physical security infrastructure, spanning locations and systems.

Streamlined maintenance and updates

Proactively planning for maintenance, tracking warranties, and ensuring timely upgrades to protect against vulnerabilities.

Data-driven decision-making

Leveraging insights from asset health, usage patterns, and historical data to inform budgeting, upgrades, and replacements.

2.3 Security integration challenges

Security integration challenges are widespread, significantly impacting industries from healthcare to finance. These challenges are set to grow as physical security complexities increase, particularly with mergers and acquisitions (M&A) expected to rise by 50% in the upcoming years. This surge will broaden the physical footprint and the range of assets needing safeguarding, underlining the need for advanced, scalable physical security solutions.

Consider the challenges presented by a merger or acquisition scenario, which brings together two companies with vastly different security systems:

Scenario:

A major manufacturer with modern, integrated physical security infrastructure acquires a smaller competitor relying on outdated access control (key locks, old badge readers), minimal surveillance, and aging intrusion detection systems across multiple facilities.

Consequences:

- **Vulnerabilities and blindspots**
  Inconsistent security leaves facilities open to intrusion and theft and limits awareness of incidents across the combined entity.

- **Operational challenges**
  Managing multiple disparate systems complicates access control, hinders timely incident response, and makes it difficult to generate a consolidated view of security incidents.

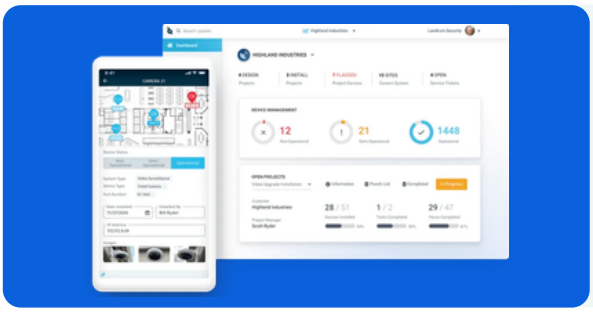
- **Maintenance headaches**
  Unpredictable failures of outdated systems, difficulty sourcing parts, and reliance on reactive repairs drive up costs and cause operational disruptions.

- **Compliance risks**
  Outdated systems may violate industry regulations or specific security requirements for handling sensitive materials.

- **Inefficient upgrades**
  Without clear lifecycle data on the acquired systems, it's difficult to prioritize which needs immediate replacement vs. those with usable life, leading to potential misallocation of funds.

Aligning physical security post-M&A: The SiteOwl advantage

Mergers and acquisitions often result in a fragmented physical security infrastructure, with varying systems and protocols struggling to communicate and operate cohesively. This disjointed landscape complicates security management, elevates risk, and can lead to inefficiencies and increased costs. SiteOwl offers a seamless solution to this challenge, providing a unified platform for integrating disparate security systems into a coherent, manageable framework.

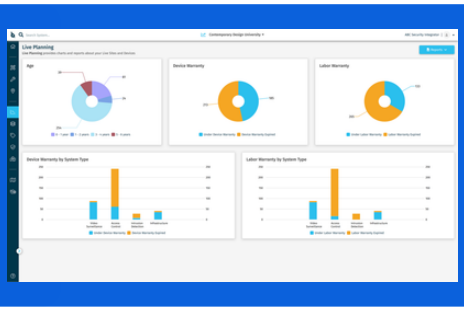


Centralized asset management

SiteOwl can create a digital inventory of all physical security systems across the entire portfolio, regardless of brand or age. This includes details about installation dates, warranties, and maintenance histories.

Proactive maintenance planning

SiteOwl's tools enable teams to schedule preventive maintenance, set alerts for upcoming component replacements, and track the overall lifecycle of their security devices.



Compliance support

SiteOwl can generate audit-ready reports and track compliance history for different systems, helping avoid costly fines and potential risks.

CHAPTER 3

Integrating systems and cultures

Mergers and acquisitions (M&As) are not just financial decisions but strategic moves that can redefine an organization's future. As such, building operational resilience during these transitions, especially from a physical security standpoint, becomes paramount.

Below are three challenges that highlight why building operational resilience with a focus on physical security is crucial during these strategic moves:

Challenge #1

Increased vulnerability during transition

A large, multi-campus university system faced the challenge of managing a complex mix of security systems across its sites. With some campuses built recently and others with legacy infrastructure, they needed a way to future-proof their approach without constantly replacing systems wholesale.

Here's an example to understand how:

Mid-size company acquisition

Company A

Uses a mix of cloud-based access control and older, on-premise security systems with less reliable maintenance.

Company B

Relies primarily on local security staff at their facilities for monitoring and response.

Challenges

Integrating security systems may take time. If access control changes aren't implemented immediately, outdated systems could remain vulnerable, and gaps in physical monitoring become a risk during the transition period

INSIGHT # 2

Proactive threat monitoring mitigates risk

SiteOwl provides a unified view of security assets across all locations, even with disparate systems. This centralized visibility minimizes security blind spots. Streamlined device ticketing, real-time project status updates, and comprehensive system-wide audits help quickly identify and address outdated systems, inconsistencies in security practices, and potential vulnerabilities before they become critical risk points.

Challenge #2

Merging systems create gaps

Imagine two companies, each with their own set of security cameras, access control systems, and protocols. Merging these can be a logistical nightmare. Incompatible technologies and inconsistent security standards create risks until a unified system is established. These gaps are prime opportunities for security breaches and disruptions.

Here's an example to understand how:

Large enterprise merger

Company A

Highly centralized security operations with a sophisticated Security Operations Center (SOC) and established incident response protocols.

Company B

Operates a more decentralized security model with localized monitoring across their facilities and less-formalized procedures.

Challenges

Determining whether to maintain a centralized or hybrid security management model, standardizing protocols, and consolidating tools and data feeds across two potentially very different operational structures.

INSIGHT # 3

Facilitating a hybrid security management model

SiteOwl's flexible architecture supports both centralized and decentralized security operations, allowing for a seamless blend of Company A's SOC capabilities and Company B's local monitoring strengths. This hybrid approach ensures that the merged entity benefits from robust oversight and rapid local response, creating a security framework that is greater than the sum of its parts.

Challenge #3

Expanded threat landscape

A merged organization suddenly has more locations to protect. New facilities may have unknown security weaknesses, and the combined entity might be safeguarding assets it never had to previously. This expanded threat landscape necessitates a robust and adaptable security approach.

Here's an example to understand how:

Specialty manufacturer merger

Company A

Primarily protects intellectual property and sensitive research data. Their security focus is on cyber threats and strict access controls within the facility.

Company B

Operates several manufacturing sites and warehouses, focused on securing physical assets and inventory, with less emphasis on data security.

Challenges

The merged company needs a comprehensive security strategy that protects IP and physical assets across multiple locations. Achieving this requires assessing new threats, scaling technology, and potentially adapting security protocols.

INSIGHT # 4

Scalable security for the evolving entity

SiteOwl's modular, cloud-based platform grows with your security needs. Easily integrate new facilities, add monitoring capabilities, and adapt to the unique threat landscape faced by the merged company. SiteOwl simplifies the process of extending powerful physical security to all locations, ensuring comprehensive protection from day one.

Navigate the M&A maze with a physical security playbook

Mergers and acquisitions (M&As) are transformative, but they also introduce significant physical security challenges. A well-structured Physical Security Playbook provides a clear roadmap for addressing these challenges.

"Many companies have disparate systems and protocols in place that make sharing information and access permissions between employees nearly impossible."

-PSIA

Why you need a physical security playbook:

- **Unify Standards**
  Establish consistent policies and procedures from the start, even if technology isn't fully integrated yet. This sets a clear baseline and reduces risk.

- **Plan for a Smooth Transition**
  Develop plans tailored to your merger, safeguarding sensitive assets and minimizing disruption throughout the change.

- **Proactive Threat Assessment**
  Analyze new locations and assets using provided templates, building protection against potential risks faced by the merged company.

- **Streamlined Integration**
  Workflows, checklists, and communication templates make merging systems and teams easier, maintaining strong security coverage.

CHAPTER 4

Building resilience and operational efficiency

After a merger or acquisition, organizations face a larger, more complex physical security landscape. Success requires a complete recalibration of existing strategies to protect assets across this expanded territory.

As your operations stabilize, three key areas become crucial for managing this new security reality: Incident Response, Project & Service Management, and Budgeting & Planning.

4.1 Incident response challenges & why it matters

M&As often mean merging different incident response protocols, communication systems, and reporting chains. This creates confusion, slower reaction times, and can make documenting and learning from incidents much harder.

A slow or ineffective incident response can increase damages, disrupt operations, and harm reputation. After a merger, the potential for incidents might even be higher due to temporary security gaps and employee confusion about the new procedures.

Action steps to consider:

- Unify and simplify incident response plans across ALL locations and assets.
- Conduct thorough training and drills for staff with a focus on the merged company's response procedures.
- Establish a clear chain of command for incident reporting and escalation.

4.2 Project & service management

Integrating security systems, updating access controls, or deploying new technologies are major projects post-merger. Inefficient management can lead to delays, cost overruns, and lapses in security during this vulnerable time.

Successfully executing these projects is what builds the robust security the new entity needs. Delays leave assets at risk and drain resources.

Action steps to consider:

- Prioritize projects based on risk and business need
- Assign clear project ownership and utilize effective project management tools.
- Coordinate closely with vendors and track progress rigorously, especially if outsourcing is involved.

INSIGHT # 5

SiteOwl's platform provides a centralized workspace for all security integration efforts. Task tracking, vendor communication, and real-time progress updates minimize delays and keep all stakeholders informed.

4.3 Budgeting & Planning

Mergers introduce new security costs: upgrades, expanded protection for new locations, and potentially ongoing management of older systems during a transition period. Hidden costs can derail the M&A's financial targets.

Why it Matters:

Underfunding security opens the door to incidents, liability, and long-term loss. Overfunding it cuts into profitability at a sensitive time for the new company.

SiteOwl's comprehensive asset management and budgeting tools give you unparalleled visibility into your security infrastructure. You can accurately assess upgrade costs, plan for phased system consolidation, and monitor the ongoing ROI of your security investments.

Successfully navigating the post-merger security landscape requires a proactive mindset and careful planning. Incident response readiness, streamlined project execution, and strategic budgeting are essential pillars for protecting the newly formed entity.

By addressing these areas head-on, organizations can avoid costly surprises and ensure a smooth transition to a robust, unified security posture. SiteOwl provides the tools and insights to facilitate this process, enabling security teams to adapt quickly, optimize resource allocation, and make data-driven decisions that protect both the bottom line and the overall security of the organization.

CONCLUSION

Mergers and acquisitions bring big changes, and physical security is no exception. As a security leader, you're suddenly responsible for more locations, assets, people, and potentially dealing with outdated tech and inconsistent procedures left over from the merger.

This guide has focused on strategies to manage this change, including:

Unified response
Develop a single security plan for all locations to minimize risk during the transition.

Streamlined integration
Plan carefully to merge systems smoothly and maintain protection throughout the process.

Strategic budgeting
Make informed decisions about security spending to protect assets and your bottom line as the company changes.

The Future: Challenges and opportunities

Your merged company has a greater physical footprint, potentially attracting new security risks. This means proactively re-evaluating your threat landscape and ensuring your security systems are ready to adapt.

A new era for your security team

This guide marks the start of a new chapter. Now's your chance to lead the development of a stronger, more unified security strategy for the merged organization. With SiteOwl, you can:

- **Build a unified vision**
  SiteOwl's centralized view of all systems breaks down silos. This facilitates collaboration with new colleagues to develop a single, effective security plan

- **Manage expansion with confidence**

  SiteOwl's scalable platform easily integrates new locations, devices, and personnel. Track progress, identify vulnerabilities, and proactively expand protection to cover the whole enterprise.

- **Demonstrate ROI**

  SiteOwl's budgeting and analytics tools help you link your security spending to real-world risk reduction. This strengthens your case for investment and builds support for your initiatives across the organization.

About SiteOwl

SiteOwl is the only physical security system lifecycle management platform that brings enterprise security teams, their integrator partners, and assets together on one unified platform.

The solution's suite of applications connect real-time data and workflows, specific to the physical security industry, to drive collaboration, visibility and efficiency.

To learn more, please visit getsiteowl.com.