

Ready, set... acquire

Tips to expedite physical security planning as your company expands



For physical security leaders at midsize-to-enterprise organizations, the words “We’re acquiring another company” can spark both excitement and anxiety. Excitement, because growth means new opportunities for your program and your team. Anxiety, because you’re aware that the complexities of integrating two different organizations—systems, processes, cultures, and people—rarely receive the early attention they deserve in corporate deal-making.

In many companies, mergers and acquisitions (M&A) are orchestrated at the executive and board levels, with announcements delivered to operational teams as a fait accompli. By the time security leaders are informed, the deal may already be in motion, leaving little time to prepare. Yet those first hours and days after learning of an acquisition are crucial. The actions you take early will set the tone for how visible, credible, and effective your physical security program will be throughout the transition.

Our recent white paper, [Aligning Roadmaps for Acquisitional Growth](#), offers an overview and helpful scenarios for addressing physical security challenges during M&A activities. This article offers practical first steps and considerations to help you expedite planning and position security as an indispensable partner from day one.

Step 1: Get visibility into the acquisition process

The very first priority is ensuring you're not left on the sidelines. Acquisitions move quietly under the cover of an NDA, and decisions are made by a small group—the M&A committee (sometimes called the integration steering team, corporate development team, or similar). If physical security doesn't have a voice in that room, its needs and risks will be overlooked.

- + **Find out who's leading the process.** Identify the chair of the M&A committee and the executives involved.
- + **Make the case for inclusion.** Don't wait to be invited. Position security as a strategic function that reduces risks, prevents hidden costs, and smooths cultural integration.
- + **Offer quick value.** Come prepared with data points—your current security roadmap, cost models for typical integration activities, and examples of past cutovers or consolidations. The faster you show you can accelerate due diligence, the faster leadership will see your value.

Remember, visibility at this stage isn't just about defending your budget. It's about shaping the entire integration so that security strengthens, rather than slows down, the acquisition deal.





Step 2: Inspect your current environment

Before you can understand how the acquisition will impact your program, you need a clear picture of your own baseline. Many companies discover gaps only after trying to overlay their systems with the acquired company's, which creates chaos during integration.

Work with your security consultant to conduct a quick but thorough assessment of your current state that includes...

- + **Systems:** Catalog your access control, video, alarm, and other core technologies. Note models, versions, health, and end-of-life timelines.
- + **Locations:** Map the facilities, campuses, and remote offices currently under your security umbrella, so you can relate these details to the acquired company as soon in the process as you're allowed.
- + **People:** Document roles, responsibilities, and team structures. Highlight critical subject-matter experts (SMEs) who will need to be on call for high-impact due diligence and execution tasks.
- + **Costs:** Capture operating expenses, licensing fees, and maintenance contracts so you can provide an informed financial picture of the acquisition from a security perspective to your stakeholders and your team.
- + **Risks:** Assess and document known risks within your current physical security environment that could complicate or compound during acquisition integration. This includes outdated or unsupported systems, inconsistent policy enforcement, noncompliant sites, staffing shortages, or open audit findings.

By understanding these vulnerabilities upfront, you can set realistic integration expectations, avoid multiplying gaps when merging systems and teams, and strengthen your credibility during M&A planning discussions.

Having this baseline at your fingertips allows you to compare apples-to-apples when details of the acquired company's environment emerge.

Step 3: Begin scenario modeling

Even before you have full visibility into the target company, you can sketch likely and/or worst-case scenarios. Scenario modeling is especially important if your company is considering multiple acquisition targets, or if rumors have been circulating.

Ask yourself:

- + What would integration look like if we acquire a small regional firm? A large national player?
- + What costs will recur across any scenario—credential reissuance, retraining, travel, system cutovers?
- + How long would each scenario take, given your team's capacity and available resources?

By giving leadership options to consider rather than problems to solve, you demonstrate foresight and build credibility in high-stakes conversations.



Step 4: Prepare for budget conversations

Budgets are often where strategy meets reality. Acquisitions introduce dozens of hidden costs—system migrations, policy harmonization, cultural onboarding, travel for SMEs—that are easy to underestimate if security isn't consulted.

Get ready to:

- + **Defend must-have expenses.** Know which assessments and integration activities are non-negotiable for safety and compliance.
- + **Highlight opportunities for savings.** Show where redundancies can be eliminated like duplicate servers, licenses, or monitoring contracts, including contracts for guarding and break/fix services.
- + **Position budget as risk management.** Make it clear that underfunding security integration doesn't just affect your team; it exposes the entire organization to safety, compliance, and reputational risks.
- + **Have an alternative ready to present for contrast.** In the event you get pushback on your budget, be prepared with numbers to show what an alternative solution might cost, both in terms of capital outlay and risk of vulnerabilities.

In budget conversations, speak the language of executives: risk mitigation, cost avoidance, and business continuity. Doing so will help break down potential barriers and solidify your physical security brand within the newly combined organization.



Step 5: Identify and engage people early

Integrating two security teams is as much about people as it is about systems. Redundancies may be inevitable, but they don't have to translate into lost talent or morale.

- + **Map roles at both companies.** Understand responsibilities, overlaps, and gaps.
- + **Engage SMEs quickly.** Identify specialists, investigators, and technicians who will be vital to the transition.
- + **Advocate for fairness.** Ensure acquired staff are given the chance to retrain, reassign, or even advance within the new structure.

How you communicate during these activities matters greatly. Develop a thoughtful, purposeful, and upbeat message about security priorities during the acquisition and deliver it consistently to all involved. Your leadership during this phase can help smooth anxieties, retain institutional knowledge, and strengthen culture across the merged organization.



Step 6: Plan for cultural integration

Technology and budgets may dominate early conversations, but culture will determine long-term success. For the sake of near- and long-term unit cohesion, it's never too soon to get started. Employees at acquired companies often experience new security measures as intrusive, especially if they're moving from a more casual environment into one that's more highly structured or regulated.

- + **Anticipate perceptions.** Be ready to explain why changes are being made, and how the changes will benefit employees as well as the company.
- + **Promote transparency.** Communicate openly about timelines, policies, and what users can expect during the transition.
- + **Frame security as empowerment.** Position the newly integrated, post-acquisition security program not as "Big Brother," but as a safeguard for people, assets, and continuity.

By championing change management from the outset, you strengthen adoption and reduce friction across the new organization.



Make the first days count

The days and weeks following an acquisition announcement are a test of your readiness as a physical security leader. Even if acquisition approval is months away, use the time to plan and make strategic decisions about your existing program. Your ability to secure visibility, establish baselines, model scenarios, shape budgets, advocate for people, and anticipate cultural challenges will determine whether your program is seen as a value-adding partner or a reactive cost center.

Growth through acquisition will always be complex. But by taking deliberate first steps—by being ready, not just reactive—you can expedite planning, minimize disruption, and elevate the role of physical security in your company's expansion strategy.



When a company evolves through acquisitional growth, its physical security team needs a thoughtful approach to managing the changes. Read our white paper, [Aligning Roadmaps for Acquisitional Growth](#), to find insights and guidance to help your team when growth happens.



Our office:

700 Larkspur Landing Circle, Suite 150
Larkspur, CA 94939

Email and web:

info@zbeta.com
www.zbeta.com

Phone:

(855) 559 2382

