

# The human factor of physical security planning

Basing your systems migration roadmap on people, not just tools



## People run your business

Any plan to migrate your physical security systems ultimately comes down to technology selection and implementation. Why? Usually because specific pain points have flared up with how you leverage your security technology (or don't). But the process of roadmapping a systems migration also includes looking closely at the teams of people involved. As you develop a migration roadmap for your physical security systems, as covered in our [recent white paper](#), the human factor and tech factor are both critical.

Solid, future-ready solutions comprise people, processes, and technology—in parallel lanes of consideration. If you don't slow down to think about who will contribute to your planning and who will operate and rely on your new technologies, you risk eroding the return on your security investments, through both lost sponsorship/buy-in on the executive level and lack of adoption by users. Do your best to understand and predict all the ways users will interact with the technology you choose and what their needs are, not only during incident monitoring and response scenarios but also simply in their day-to-day activities within the facility.

As a general rule, process efficiency and system efficiency are a matter of reducing randomness and producing predictable outcomes. In reality, though, people can be hard to predict, and businesses often operate and evolve in random ways, so this objective can be a tricky challenge to meet. Because your roadmap success depends in part on this success, let's take a look at a few important areas of focus.

## Who uses your technology?

Use cases and functional requirements are key to planning a security migration with people in mind. At any business, technology is a tool for making processes more consistent, efficient, and effective. For your roadmap to be effective, your choice of systems must be based on clearly defined use cases and functional requirements. These in turn are based on the roles each user performs, including the ways non-security personnel at your company go about their jobs.

Roadmapping, then, is your chance to look at how people will use the new tools you specify. When advising our clients on their roadmaps, we at ZBeta consider everyone who works at the company to be stakeholders in the solution. This means that as we help security teams tackle their immediate challenges, we partner with them to reimagine how their people will deploy and utilize the new security technology.

To put it succinctly, ask: How can we, as a business, get BETTER at physical security—and who's involved with making that happen? It's about knowing your organization and its people before you start counting out card readers and cameras. Form follows function—not the other way around. So reserve some of your roadmapping focus for getting the right people following the appropriate processes and operating the right technology—not the so-called “best tech” but the tech that's best for you.



## Getting granular on operational requirements—as needed

How your new system will operate is the central human concern guiding requirements gathering for a roadmap. The more detail and rigor you can apply during this process, the lower your risk will be in selecting new technologies. Still, not every client has the time, resources, or inclination to go down ten levels of analysis trying to achieve risk-free results, and some are just not ready to do so anyway—in many of these cases, their security program is nascent, so idealizing the effort isn't yet worth the time.

Some of our clients at ZBeta have a clear understanding of their use cases, while others need help defining and developing them. In either case, their goal is to synthesize tools and the people who use them, while accounting for each use case actor's role in the organization. We meet each client where they are at and help them right-size their approach. Sometimes we all roll up our sleeves to get a comprehensive, detailed analysis; other times the goals are higher level and more strategic, so we help by showing them ways their migration can be accomplished in broader strokes.

In this spirit, organizations confront the need for roadmapping at differing levels of maturity and scale. Their migration approach varies in the number of use cases they consider and the detail at which those use cases are defined. Well-established security teams often have robust standard operating procedures (SOPs) and a time-tested operational philosophy. In these cases, while it's critical to make sure future-state solutions capture and support these procedures and ideas in future state solutions, there isn't always value in asking deep and detailed questions about specific functional requirements for a new security program, when a focus on higher-level capabilities might be a better use of funds and time.

For example, some organizations may start their roadmapping process knowing they simply need a path to having a centralized alarm monitoring capability in the future, as their enterprise and its programs grow. Others may know they need to retain the graphical maps that their operational center staff rely on while managing alarm events currently. Still others may identify the need for more advanced mapping capabilities that integrate geographic data or dynamic depiction of camera and sensor coverage areas.

Take time to know where you're going, and then start where you are. It's never one-size-fits-all.

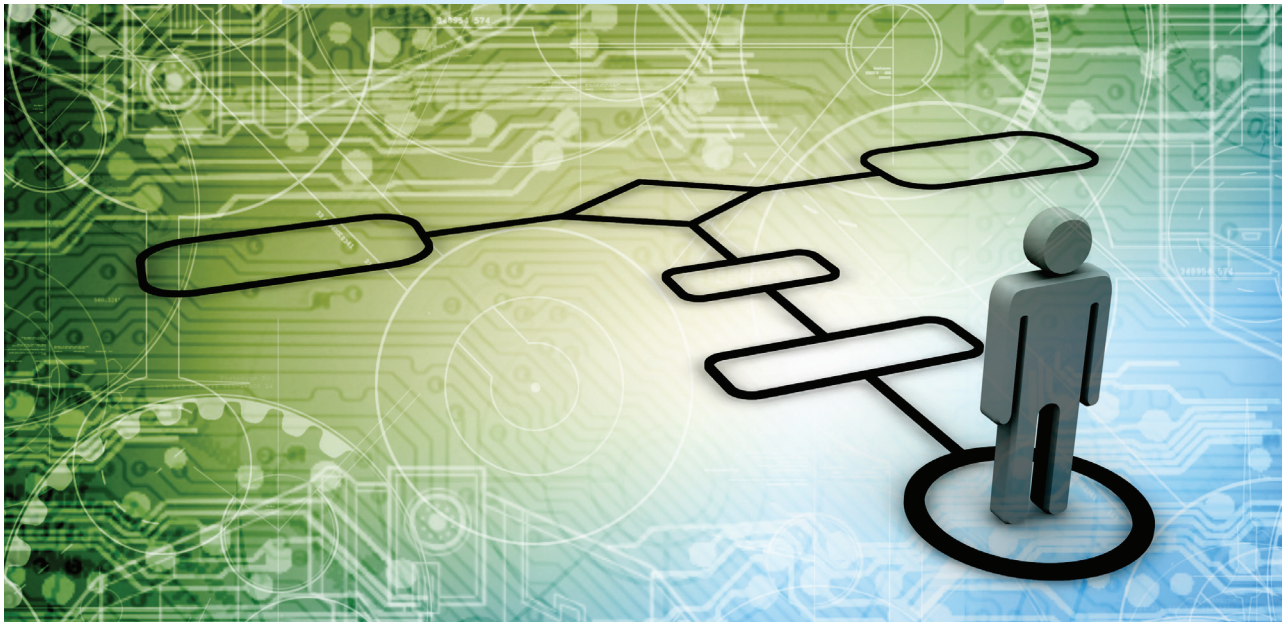


## Securing the right sponsorship

It's a proven principle that the best company-wide projects never get off the ground unless there's one person—usually someone with direct budget influence or control—who's bought into the effort and advocating for it on your behalf. With the right person providing this endorsement, they'll understand your needs and help amplify them across the organization. But more importantly, they'll run interference during periods of conflict by emphasizing the importance of your work to the business at large.

Early on in your roadmap journey, identify an advocate for your project who has:

- + **Buy-in** on understanding your physical security strategies and mission.
- + **Visibility** within the company to advocate for your roadmap.
- + **Credibility** for providing “air cover” when your plans encounter resistance or change.



Carefully choose the sponsor (or sponsors) who will champion your physical security initiative by speaking to the meaningful and thoughtful value statements you've included in it. With the sponsor's help, you can elevate the role of physical security in your business by educating other teams about the value you deliver. Coordinating and communicating with the business groups in this way not only helps justify the budget you'll need to deploy the roadmap—it also clears the way for future project support.

## Building your roadmap team

Next up, think creatively about who will be on your task force for launching the roadmap and providing ongoing input all along the way. First of all, of course, the team will include empowered and knowledgeable people from your security team itself. The security partner you engage to help advise and facilitate should also have a seat at the table from day one.

Elsewhere, however, bring in team members with competencies and interests in other parts of your business. Depending on your business type, these might be developers, production workers, data scientists, facilities managers, HR personnel, accounting professionals, or even sales and marketing people—or any other representative users who will regularly interact with or even depend on the new system, perhaps in unique or critical ways. Again, it all comes down to who has a vested interest in the positive outcome of your solution design. Your security partner will help you identify these roles.

Lastly, the executive sponsor you've chosen should be present throughout the project to lend force and credibility to the actions that result from your roadmap decisions. Sponsors can come from many areas of the business, but they're typically at an elevated level of executive leadership. The reason for this isn't just that they have the power to move obstacles in your path—it's also because they "get it" and can help spread a message about the importance of what you do.



## Achieving organizational alignment

When you're planning a roadmap that impacts every area of your business, stakeholder will come from various teams and workstreams across your organization, and it's important to know what they expect. Keeping everyone and everything secure entails accounting for their interests and needs in ways that produce a mutually positive outcome. This means getting to organizational alignment by coordinating efforts, resources, and procedures towards a common goal. With various teams working together collaboratively to achieve key business objectives, you can meet the goals and objectives in your roadmap on strategic and tactical levels.

Collaboration drives broad internal support and contributes to organizational alignment. Kick off your roadmap efforts by bringing stakeholders together to talk about security basics: What's working well currently, and what isn't working? What are our pain points, and where are our opportunities? In what creative ways can security will help foster new synergies and contribute to the company's bottom line? Discussing security improvements often yields new insights into business processes, because stakeholders have a forum for brainstorming ways of supporting each other in doing their work.

The outcome can be extremely positive. In a ZBeta engagement with a global finance company, the roadmap initiative we facilitated was the first time all stakeholders on the project team had ever come together to work collectively, and certainly the first time they had all applied a common focus on issues of physical security. Tensions arose between team priorities as the needs of different programs often conflicted. There was some circling of wagons, defensive posturing, and territory defending. But ultimately the conflicts were productive, not destructive, because we had effective collaboration.

The key ingredient in this example was the shared focus on security and business results. By keeping a positive focus on where the client wanted to go, rather than how they got to where they were, we were able to eventually overcome old habits of disagreement and entrenchment. The result was a long-term roadmap that the company is now executing with the influence and certainty they gained from resolving these early misunderstandings.

As with requirements gathering and use case development, alignment will vary according to the particulars of your organization. To see the forest for the trees, the best help often comes from the outside. Build your roadmap with a partner whose experience and perspective will help size up your needs and facilitate productive collaboration. The end result may well be arriving at a place you never quite pictured—but it's where your security program needs to go.



[Plotting a sustainable technology roadmap: Picturing and achieving the future state of your physical security solution](#) to learn about our methodology and best practices at ZBeta for developing your company's physical security technology roadmap from strategy to solution.

### Our Office:

700 Larkspur Landing Circle, Suite 150  
Larkspur, CA 94939

### E-mail and Web:

info@zbeta.com  
www.zbeta.com

### Phone:

(855) 559 2382

