

Getting a blended security culture right

Navigating what's at stake for physical security during an acquisition



When one company acquires another, their physical security programs get blended together. As part of this, two security cultures—the daily life of how users interact with the program they're previously accustomed to—that are often dissimilar must somehow get blended as well. Managing expectations throughout this time can be even trickier and more consequential than managing the logistics and systems reality of the acquisition.

In the course of overviewing physical security considerations during M&A activities and offering helpful examples, our recent white paper, [Aligning Roadmaps for Acquisitional Growth](#), touches on the topic of culture challenges. Here, let's look at it in more detail.

How culture can erode

Culture clash examples range from the sweeping to the mundane:

- + One company wears badges prominently and has a culture of challenging people when they're seen not displaying them, while the other company is more lax.
- + The marketing team at one company prefers using corporate branding on badges, while the other company considers that an undue risk when badges are misplaced.
- + Photos on badges are considered a security strength at one company, but a privacy vulnerability at the other.
- + The loading dock at one company likes the time savings of letting visitors in over a remote intercom, but the other company's intercom policy stipulates the access point being controlled must be within line of sight.
- + Certain employees at one company are accustomed to carrying physical keys and having the freedom to use them as an alternative to the stricter electronic access requirements of the other company.
- + Tailgating is a way of life at one company, and conforming to the other company's policy of enforcement is bound to be radically unpopular.
- + Cameras at one company are purely an investigative and monitoring tool for the security team, whereas the other company regularly grants camera placement and footage access to operations and retail managers to check on day-to-day activities.

This article covers the various dimensions of shift that occur when security cultures are brought together from two companies becoming one. Failing to plan, implement, and manage security policy changes



Solving for morale

Acquisitions are fraught with the potential for misunderstandings and hurt feelings. This impacts physical security because a buoyant morale is important for maintaining a user mindset that prioritizes the core tenets and policies of your security program.

The key to smooth sailing throughout an acquisition is to choose your policies and messages carefully as you implement the changes in your newly combined security culture. Keep in mind that emotions are running high already due to the many uncertainties users experience during an acquisition, such as how their jobs will change or whether they will even continue to be needed. This sensitive environment gives security leaders all the more reason to provide certainty, clarity, transparency, and a sense of empowerment when communicating and implementing new security policy.



What failure can look like

To paint the picture of a corporate acquisition where security cultures are poorly merged, consider the following scenarios:

- + **Violations.** Feeling inconvenienced, users create their own workaround to new security rules, not always aware of the harm it may cause. A classic example of this is the proverbial “coffee can” holding an external door open so workers can come and go for smoking breaks outside, violating protocol for the sake of user convenience.
- + **Operational disruptions.** Failed cultural unity yields every kind of obstacle in day-to-day security operations, ranging from the pesky to the severe. Users lose access to areas they expect to get to, theft occurs thanks to the confusion around gaps in oversight, incident reporting is ambiguous without proper training, and staffing shortages lead to missed expectations if you don’t account for them in advance.
- + **Sabotage.** Resentment boils up to the point where users willfully defy the rules and even break them to send a message or as an excuse to underperform at their jobs. This can take many forms of “malicious compliance” that undermine security and productivity for all by discrediting security policies and disrupting core business operations.
- + **Exodus.** Good people sometimes leave—and take their institutional knowledge with them—in part over a dislike or intolerance for poorly implemented security rules. This can occur for various reasons, including because they were never helped to understand the rules’ importance or because they felt disrespected and their voices weren’t being heard.

Focusing on failure isn’t always a happy tactic, but it’s often important for understanding what’s at stake. Always bear in mind the potential pitfalls of any journey. Knowing what to avoid helps you keep the true end goals in sight, and how you get there is going to make all the difference.

A few top-level guidelines

The rest of this article spells out tips and tactics for dealing with physical security culture clashes throughout an acquisition, but as a general rule physical security teams can do the following to help uplift user morale:

- + Practice **transparency and proactive communication** once you've chosen the message for your updated security approach.
- + Get out in front of **burnout** by advocating new security directives directly to all users and teams who will be affected.
- + Figure out **critical functions** within your team and how to be more efficient, so you can focus efforts on bringing users around to the new policies.
- + Be ready with **metrics** to describe the increased workflow for your team. This will help with securing budget and other resources for your compliance efforts.

As a rule, you'll succeed by making your message to users less about WHAT they must do and more about WHY their participation is important. Rather than scare them with any punishment they'll receive for not toeing the line on new policy, motivate them to understand the benefits of compliance. Appeal to their sense of intelligence and duty to the organization rather than making security a black box they're not allowed to see inside.



4 steps to success

1. Listen

Psychologists opine that roughly 90 percent of human anger is the result of not feeling heard by other people. Help your security culture succeed by taking the time to hear what users want, feel, and have to say.

- + Interview users to learn about their roles, their daily activities, and their thoughts and impressions around physical security.
- + Build a committee in advance of defining new rules, and populate the committee with users having different perspectives and opinions that you learned about during the interviews you conducted.
- + As you meet with users and learn about their concerns, look for ways you can give them some of what they want. If their cultural expectations are significantly at odds with new policy directives, try figuring out how to meet them half-way.

2. Strategize

Try out some thought exercises prior to carrying out a new policy campaign. You can afford to be scientific in your merged security culture approach if it means bringing more users along and warding off difficulties down the road.

- + Appoint one or more “culture champions” who have respect and visibility within the user environment, and work with them to model and demonstrate the new security culture.
- + Develop user personas that resemble and aggregate different needs, expectations, and job roles of the users they represent:
 - “Jose is an assistant controller in accounting. He’s an hourly employee, he parks on the west side of the building, and in a typical day he interacts with teams on the second and third floors of the headquarters building.”
 - “Jill is a sales manager. She’s a salaried employee, and her work schedule takes her to multiple facilities in the course of each month.”
 - “Tim is a temporary contractor. He has permission to be on site at our Detroit facility for two days to work on electrical changes. During that time, he’ll need access to three secure spaces and two full-time personnel.”
- + Then, walk through a day in the life of each of these fictional personas to see what areas of compliance with new policy might encounter friction. Try to anticipate the most likely pushback your security changes will encounter. Don’t plan for the best outcome; start by planning from the worst scenarios.

3. Sell!

In the business world, you ultimately sell a product or service by showing consideration for the people who will consume it. This means understanding your target audience and delivering a message to them in ways they can relate to about the value you seek to provide. How you message your user base for security changes can follow this model as well.

- + Approach physical security change management during acquisitions as a re-branding opportunity for your security organization. You want to achieve a fresh, new understanding by all users at both companies about what you do, how you do it, and why your policies are important for them to understand.
- + As you craft your message, go beyond the need for protocol and take extra care to appeal to users' intelligence. Once again, tell them the WHY of what you're requiring of them, not merely WHAT you expect them to do.
- + Choose the right tone for your message as well. Remain upbeat while showing how seriously they ought to take the physical security discipline you represent.

4. Implement

When your strategy and sales campaigns are ready, it's time to implement the changes. The same guidance from the earlier tasks applies here: Proceed thoughtfully, with diligence, proactive observation, and respect for users' intelligence, time, and state of mind.

- + Put the right people on your team in charge of deploying the new security culture. People don't like to be forced, so choose leaders on your team who will model policy alignment rather than dictate it to others.
- + Post the new rules where needed in a way that doesn't make them feel like Big Brother is watching.
- + Understand up front that there will invariably be some level of complaining and non-compliance. Be intentional and resilient with the rules you present, and have a thick skin for dealing with the naysayers.



Manage up for top-down support

The best-laid plans for managing changes in security culture won't work unless they're driven from the top down. Get executive-level support for your efforts, and as part of this, work hard early on in the acquisition cycle to make sure your executives understand what's at stake for achieving a unified user environment. And while you are pushing to retain top-down support, you're also pushing to remain clear and transparent with users about the changes you make.

All of this requires patience, planning, and careful orchestration of your security team's efforts, energies, and ideas. When it's all done correctly and the dust has settled on the overall acquisition event, you'll emerge with a stronger, more unified sense of purpose and solidarity that will keep your newly united user group safe and happy—and hopefully carrying a newfound understanding and respect for the work that you do.



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

