SPONSORED CONTENT | WHITE PAPER

Market Pulse

The Opportunity for Convergence:

Integrating and Improving Physical and Network Security

CIO

SPONSORED BY

cisco Meraki

Executive summary

Physical security is no longer analog. Surveillance cameras, locks, access devices—all these historically physical security measures are now connected to IP networks. Previously, network security and physical security teams had little reason to interact; their domains were separate. Today, they are inextricably intertwined.

For IT teams, these connected devices pose potential risks to network security. At the same time, physical security teams increasingly depend on the resiliency of the network to do their jobs. A recent survey from Cisco Meraki and Foundry highlights the opportunity to strengthen overall security by integrating these two teams.

According to most respondents (81%), it's critical or very important to create a more unified security environment. However, in just over half of surveyed organizations, physical security is still a standalone department.

The survey also reveals a significant gap between the perceptions of the C-suite and less senior titles regarding information sharing. More than three-quarters (77%) of C-suite respondents believe that all relevant information is shared between physical and digital security teams, while just 56% of those with less senior titles say the same. As a result, upper management may be too optimistic about how well their teams are working together and may underestimate the limitations their organizations are facing.

For businesses that have already integrated these two teams, the benefits are clear: better visibility into security threats, better control of physical security technology, improved cost control, and an improved user experience—all of which translates into a more efficient, secure organization thanks to a tightly knit network and physical security team.

In fact, 96% of respondents who reported at least partial integration experienced at least one of those benefits.

In the not-so-distant past, physical security was an analog world of coaxial cables, where video streams from hardwired cameras were recorded onto videotape—if at all. Network security, which dealt in digital bits transferred using IP protocols over Ethernet and other networking technologies, relied on a completely different infrastructure. In years past, it made sense to keep these two teams separate. But not anymore.

The situation is far different today. Video surveillance data is now completely digitalized, traveling over IP networks alongside all other network traffic, with video files often stored and managed in the cloud. Door locks are digitally controlled and rely on digital identity verification, and security guards communicate using digital channels.

The days of analog physical security are numbered. Today, physical and network security don't just overlap—they are completely entangled with one another. Nevertheless, the historical legacy of separate network and physical security teams persists in many organizations, leading to intradepartmental gaps and communications issues.

"Each group is used to doing things their own way, and now they're required to work with and consult with each other," said Saralyn Dasig, Marketing Leader at Meraki. "Physical security teams fear they will lose control over their systems. They can't do their jobs if IT is making decisions about physical security technology and choosing tools that won't equip them with what they require. The team responsible for

network security is concerned that if they're not involved, they're going to be open to attack. If not properly secured, IP cameras can be an attack vector. Someone could hack into the camera system to view video or access other parts of the network."

To better understand how organizations are aligning physical and network security, Meraki partnered with Foundry on a survey of 100 senior decision-makers—both in IT and executive management—at US enterprises. Most (90%) were involved in either physical or network purchasing decisions, if not both.

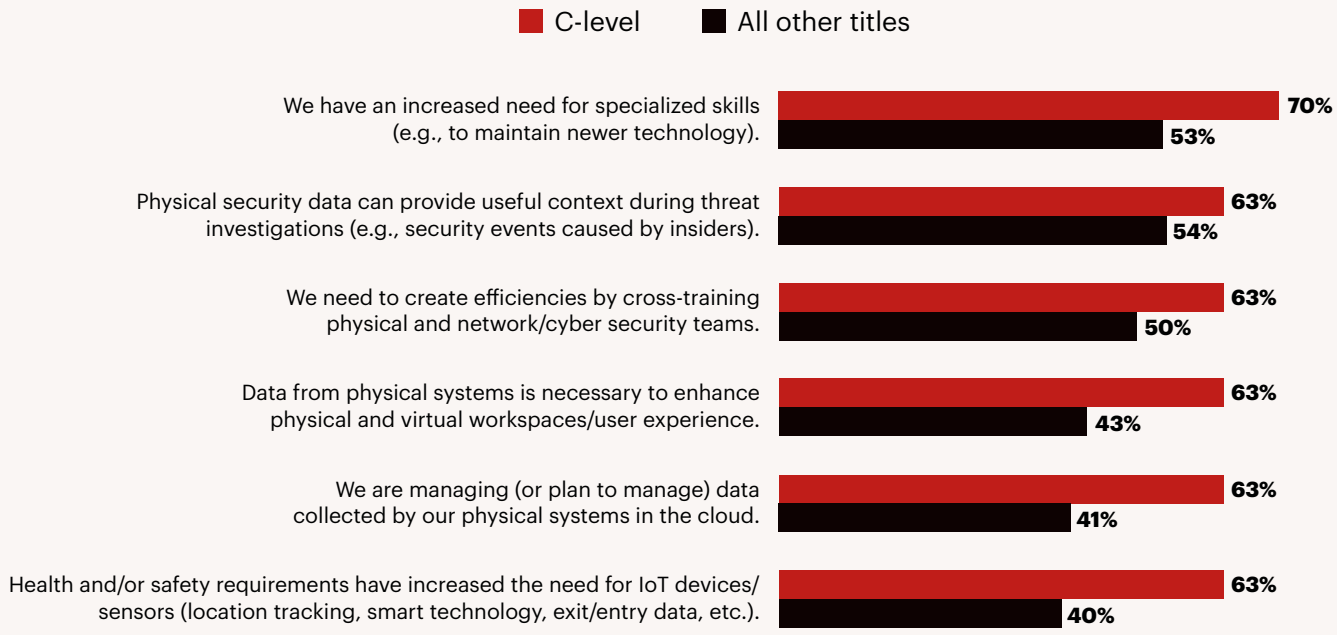
The current state of physical and digital security collaboration

The consensus is clear: nearly everyone (81%) wants a more unified security environment, and they have a clear idea of what they are looking for: greater control of physical security technology (60%), an improved ability to perform security analytics (47%), and better visibility into security threats (47%).

But this desire for unity between physical and network security isn't showing up in the organizational structure. There's no dominant practice for managing physical security. In 51% of organizations, physical security is a standalone department; 48% manage it together with network security. State and local governments (71%) are more likely to segregate physical and network security than financial services (51%) and manufacturing (34%).

Interestingly, the data show that the C-suite may have too rosy a picture of the actual situation when it comes to information sharing between physical and network security teams. Because while information is being shared between the two departments—six in ten (62%) of the total respondents say that all information is proactively shared between physical and network security teams—more than three-quarters (77%) of the C-suite say all information is shared, while just 56% of the other titles say the same. Senior management may miscalculate just how well network and physical security teams are working together, which could lead to bad decisions down the line.

Agreement statements regarding security environment (% strongly or somewhat agree)



Respondents fell at different stages of integration: just one-third (35%) have fully integrated network and physical security, while 43% have partially integrated these functions, and 12% plan to do so. Fewer than one in ten (7%) are considering integration, and only 2% have no plans at all to do so.

Once again, we see a significant gap between the C-suite and other titles, with 50% of the most senior titles saying they've already fully integrated physical and network security, versus 29% of all other titles.

That said, almost all (96%) of those surveyed report one or more benefits from the unification of security functions.

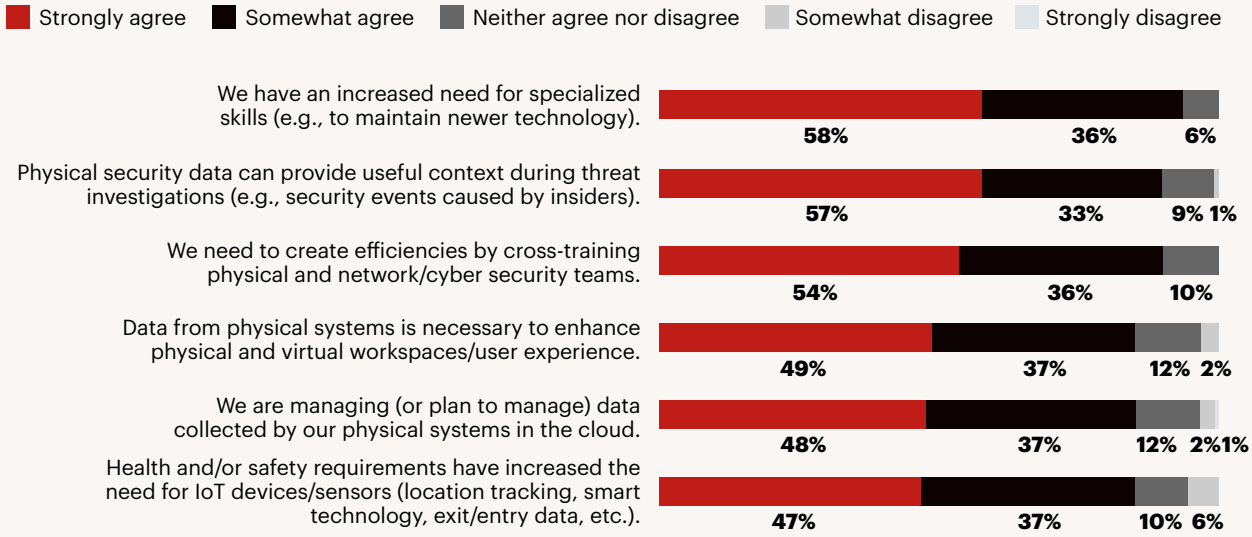
Benefits experienced from closer alignment between physical and network/cyber security (Select all that apply)

Integration challenges

Unsurprisingly, more than half of respondents (54%) say it's challenging for physical and network security teams to effectively collaborate. Organizations that have physical security as a separate team are even more likely to report communication challenges: one in five (20%) say it's "very challenging," compared to just 8% of those with integrated teams.

Technology integration represents the leading challenge to aligning physical and network security (55%), but it's not the only barrier. Respondents also cited cost and budget (43%) and skills gaps (42%) as significant roadblocks. In fact, nearly every respondent (94%) recognized a growing need for specialized skills. Just over nine in ten (91%) say there's an increased need for technology integration skills as they unify their security teams. At the same time, 90% say there's a need to create efficiencies by cross-training physical and network security teams.

Agreement statements regarding security environment



The concern over skills highlights the need for a unified platform that simplifies security.

"An intuitive role-based platform that unifies physical and network security by default reduces the need for highly specialized skills, which reduces the risk of human error and allows your internal teams to work more efficiently," Dasig said.

Real-life security integration success stories

The College of New Jersey is an institute of higher learning with 7,400 students and one of the highest four-year graduation rates in the US. When their current CIO arrived, the campus security architecture was monolithic and cumbersome. Cameras were very difficult to change and often went offline. What's more, the campus perimeter cameras weren't managed by campus police, but by construction and facilities, which complicated maintenance and the purchase of new cameras.

The CIO and campus police decided to replace their analog security camera infrastructure with cloud-based Meraki MV smart cameras. There were many benefits. First, the cameras could all be managed from a single platform. Video was easy to record and save from a single screen, and it could be securely sent to any relevant parties for viewing on a mobile device. Also, the Meraki solution made it easy both to update existing cameras and integrate innovations with a software-based environment. And, finally, because the system was so efficient to manage and deploy, the school was able to substantially reduce the total cost of ownership.

"The data show that the C-suite may have too rosy a picture of the actual situation when it comes to information sharing between physical and network security teams."

"Technology integration represents the leading challenge to aligning physical and network security."

This integration of physical security with the network was so successful that the college made plans to digitalize and integrate card swipe and network security systems and establish triggering events, such as a propped-open door alert, so police can check for unusual activity. All of it can be managed from the unified Meraki dashboard.

The College of New Jersey is far from the only organization that is integrating physical and network security. ESBO Logistics, a multi-client logistics operator in Spain with more than 65,000 square meters of storage facilities, recently overhauled its network. The company deployed secure SD-WAN and Wi-Fi 6 to provide a robust, reliable, agile network for a wide array of use cases, such as controlling and monitoring sensors for cold rooms, managing autonomous robots, and receiving data from scanning guns.

They also integrated Meraki MV smart cameras for physical security. Because they are managed from inside the Meraki platform, they benefit from unified management and secure access service edge capabilities, ensuring that these cameras enhance security without themselves becoming a security risk on the network.

A commissioned study conducted by Forrester Consulting on behalf of Meraki demonstrates the economic benefit of Meraki MV smart cameras, finding that a composite organization comprised of interviewees with experience useing Meraki MV smart cameras saw an ROI of 43% and $2.6 million in net benefits over three years. The solution also reduces the average time to access and share footage from two hours to 12 minutes.

"We bring physical and advanced network security together on a single platform to secure IoT, physical security, and user devices," Imran Idrees, WAN Product Marketing Manager at Cisco Meraki, said. "You give physical security and IoT a policy in the same way you'd do any other device. It's no different than anything else on the network. Regardless of which team you're on, you log in to the same platform. Role-based access is built in to provide different views of the platform depending on what you're responsible for."

Meraki provides a comprehensive cloud-based platform that natively consolidates physical and network security to ease management, enhance security, and facilitate information sharing.

For more information, visit meraki.cisco.com/products/platform.