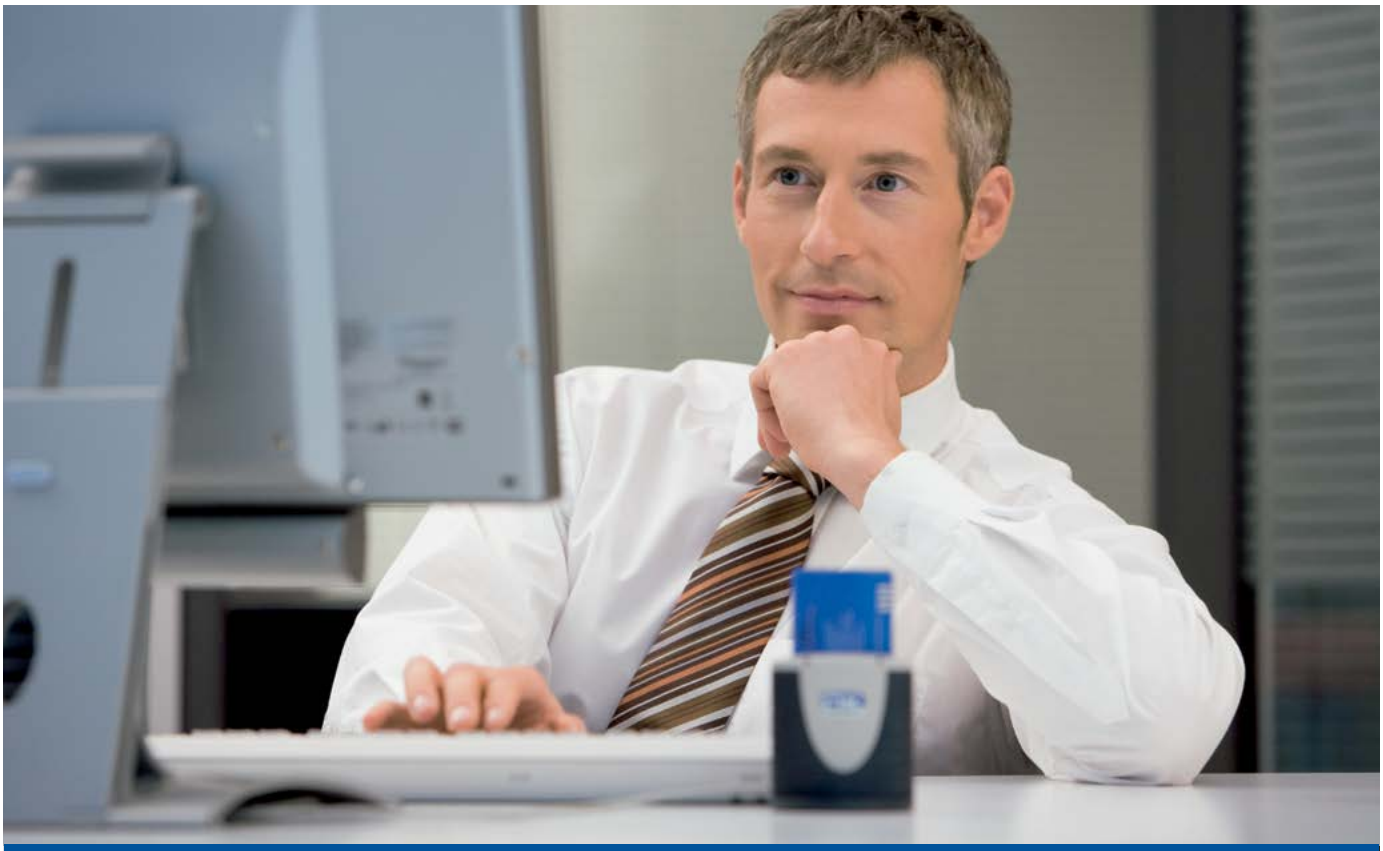


THE CONVERGENCE OF PHYSICAL AND LOGICAL ACCESS:

WHAT IT REALLY MEANS FOR AN ORGANIZATION'S SECURITY

FOR MANY SECURITY PROFESSIONALS, recent high-profile data breaches have shifted attention to external cyber threats. Despite this newfound focus, the Institute for Critical Infrastructure Technology reports that more than half of all cybersecurity incidents can be traced to insiders with legitimate access to corporate facilities and networks. Another survey from the Ponemon Institute reveals that the majority of respondents are more concerned by outside threats than those that originate internally.

Contents

HID

WHILE EXTERNAL THREATS ARE VERY REAL, working to confront internal vulnerabilities can prevent incidents from happening in the first place. By addressing both physical and logical access in a more unified approach, organizations can reduce their risk for a costly breach while also improving user experience and operational efficiency. This idea is frequently referred to by the industry buzzword of "convergence".

From a technical standpoint, convergence is defined as "the merging of distinct technologies, industries, or devices into a unified whole." In terms of access control, convergence can be viewed as "the merging of physical and logical access control technologies to provide a more unified and simplified approach to identity management."

"Convergence means a simplified approach," said Sheila Loy, Director of Healthcare Industry, Identity and Access Management at HID Global. "That can mean many different things, but it's essentially making it easier for the user to get both digital access and door access. That usually comes in the form of a card or a mobile device—something that can do both."

While the notion of convergence is nothing new, this approach to security is becoming an increasingly viable way to mitigate threats. To explore this further, ASIS International recently partnered with HID Global to survey security professionals regarding their experience and related plans on convergence projects. The data in this paper is based on the responses of 745 ASIS International members who have direct responsibilities in Physical and/or Information Security.

The Benefits of Convergence: Improved User Experience, Operational Efficiency, and Security

Security administrators are looking for solutions that are easy, convenient, and fast. By introducing solutions that better blend physical access control (PACS) with logical access control (LACS), organizations of all types will enjoy three key benefits, including: 1) positive user experience, 2) enhanced administrative experience, and 3) improved security.

Positive User Experience

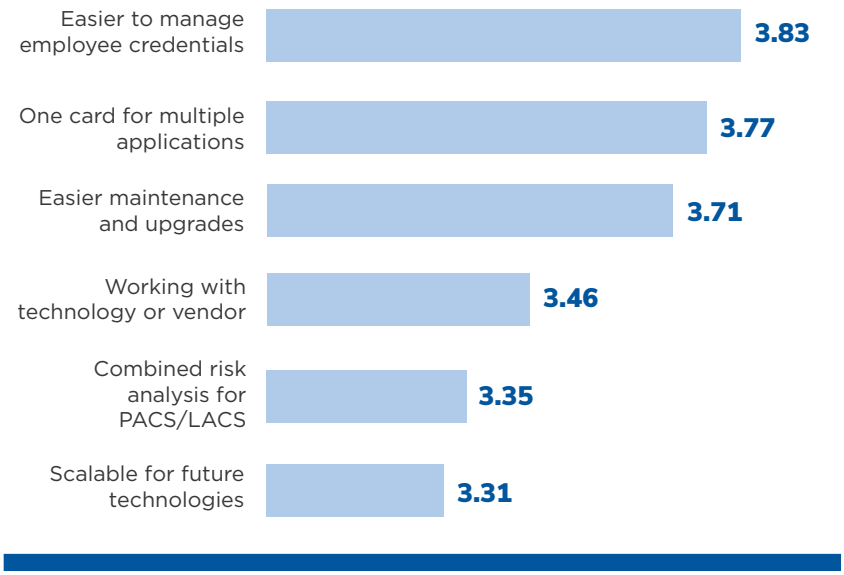
Oftentimes, the weakest link in even the strongest of security systems lies within the end user. If interactions with security technologies are confusing or cumbersome, employees will take shortcuts that introduce unnecessary vulnerabilities. Converged PACS and LACS solutions help reduce this risk by boosting convenience, particularly by requiring employees to only carry one card or mobile device. This type of solution also eliminates the need to constantly refresh passwords.

In today's world, most end-users wear an ID badge to access facilities, which is a form factor they are accustomed to using. Even more, many employees either use a username and password or a one-time password fob or token to access networks. While this approach may provide an additional layer of security, it is prohibitive in terms of convenience. Alternatively, providing a single form factor for both physical and logical access creates a more streamlined user experience, which ultimately increases user adoption to desired security policies.

"Building occupants who have entitlements to both physical areas and logical applications will see an en-

RANK THE FOLLOWING BENEFITS OF INCREASED PACS AND LACS CONVERGENCE

Average Rank on scale of 1-6



> ***Convergence results in greater employee efficiency and a more pleasant work environment for building occupants. It's easier for employees to carry one card or one mobile device to access both systems, rather than having to carry a card for the door as well as a fob for the computer or having to remember passwords."***

hancement in their experience," said Brandon Arcement, Director of Product Marketing at HID Global. "Convergence results in greater employee efficiency and a more pleasant work environment for building occupants. It's easier for employees to carry one card or one mobile device to access both systems, rather than having to carry a card for the door as well as a fob for the computer or having to remember passwords."

In terms of logical or network access, one major pain point for end users is the need to remember and frequently reset their passwords. When ASIS International members were asked, "How is access to network and logical applications done today?", a resounding 85% of respondents indicate that they use a username and password. 85% of respondents also indicate that they have an organizational policy regarding the creation of passwords, such as requiring numbers or special characters. Not only is this inconvenient for users and administrators, it presents another common security risk: employees writing their passwords on notes left visible on their desk.

Enhanced Administrative Experience

Converged access control solutions provide an improved administrative experience. When survey respondents were asked to rank a series of benefits of PACS and LACS convergence, the top response was "Easier to manage employee credentials", followed by "One card for multiple applications".

These top responses reflect two key angles within an improved administrative experience. First, many applications used to manage credentials are now web-based with secure, simple access for administrators. This allows security teams to issue, modify, or revoke credentials away from the office or during off-hours. The second angle is the ability to deploy a converged, "high value" form factor that allows for multiple applications. For example, using one card for multiple uses reduces costs for additional or replacement cards, as well as reduces the time required to produce multiple credentials for individual applications.

According to survey data, the value of leveraging smart cards for applications beyond physical access is more than theoretical – 73% of respondents agree that they have interest in using smart cards for applications beyond traditional physical access control.

Finally, more converged access control solutions provide security administrators with more visibility into audit data. This makes achieving compliance easier, thus reducing the potential for associated fines and damaged reputations.

Improved Security

The most important benefit of any technology is improved security. Innovative technologies for physical access include contact and contactless cards with encryption that adds additional layers of security upon entering doors, elevators, or parking garages. Meanwhile, digital certificates loaded onto that same smart card can ensure trusted login to networks and appli-

cations, as well as encrypt emails and digitally sign documents.

Converged solutions improve security in three key areas:

- **Increased Adoption Rate of Converged Credentials:** With a simplified experience, users are more likely to adopt desired security protocols. HID Global's Loy says, "Your employees may have had a badge to access doors for quite some time. But when they don't have to carry extra form factors like a fob or token, or they don't have to take extra steps by entering a username and password, it provides a streamlined end user experience that increases adoption rate."

- **Credential More Closely Guarded:** A converged credential is used more frequently and is relied on for more daily activities, thus is more quickly noticed when lost or missing. "Whenever someone uses a credential for applications beyond basic physical access control, it increases value to that card and adds more reason to keep it handy – now that card becomes more closely guarded," Arcement notes.

- **Reduced Need for Strong Passwords:** Security is also improved because cards can eliminate the need for passwords, which are often the weak link in logical access control. Beyond reducing this vulnerability, leveraging a converged card requires users to remove their card to move around in a secure facility, automatically locking a computer upon card removal.

From improving user and administrative experience to strengthening organizational security, upgrading access control to leverage a more converged credential seems like a valuable exercise. However when it comes to actually implementing convergence-based projects, multiple barriers can disrupt progress.

Challenges to Achieving PACS and LACS Convergence

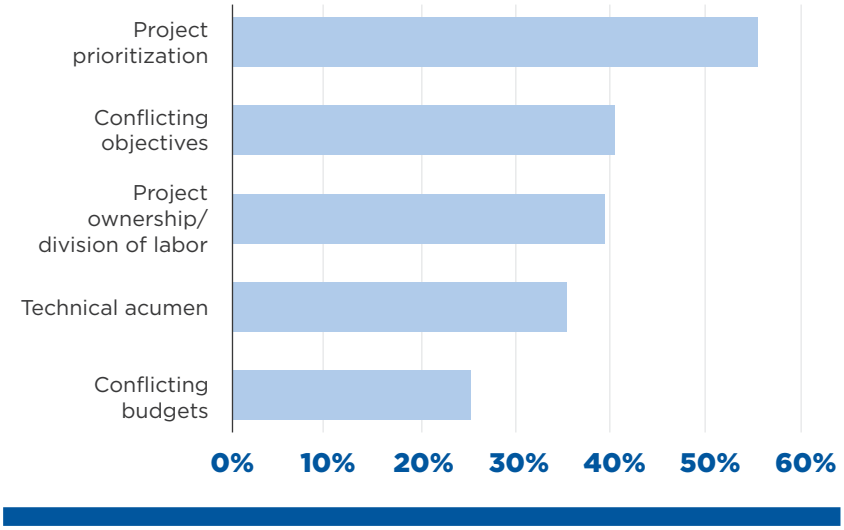
Despite an increasingly relevant business case and a growth in available technologies, the implementation of convergence projects can be described as surprisingly slow. This lack of adoption can be attributed to two primary obstacles: organizational and technical challenges. Organizational challenges include common conflicts between Physical Security and IT departments, like budgets and priorities, whereas technical challenges encompass the implementation itself, such as upgrade paths and compatibility.

Organizational Challenges

Organizational and internal communication challenges serve as a key barrier to implementing convergence projects, most often due to a lack of alignment between priorities and objectives. When asked what obstacles Physical Security professionals face when working with their organization's IT department, top answers included:

WHAT CHALLENGES DO YOU CURRENTLY HAVE WHEN WORKING WITH YOUR ORGANIZATION'S IT DEPARTMENT?

Select all that apply



> ***Executive leadership is willing to spend money to avoid similar outcomes for their organizations. There's no guaranteed assurance, but they want to ensure they're keeping up with risk mitigation best practices, which includes attention to both physical and cyber security.***

1) project prioritization and alignment, 2) conflicting objectives, and 3) project ownership/division of labor.

"Traditional Physical Security professionals often have a background in law enforcement or military. They're well-skilled in forensic investigations, executive protection, and physical security measures— guards, fences, and alarms," Arcement says. "On the other hand, the IT teams are traditionally more comfortable with data protection and cyber security measures—but, they are not as comfortable in the physical domain, even with something like cards." Because these departments have evolved separately, the two face challenges in collaboration and communication.

Fortunately, progress in building stronger relationships is growing. When Physical Security professionals were asked how they currently work with their IT departments, a resounding 60% said they collaborate to establish security best practices, with 55% indicating they look for new technologies together.

Budget is another common concern for convergence projects. IT departments typically enjoy much larger

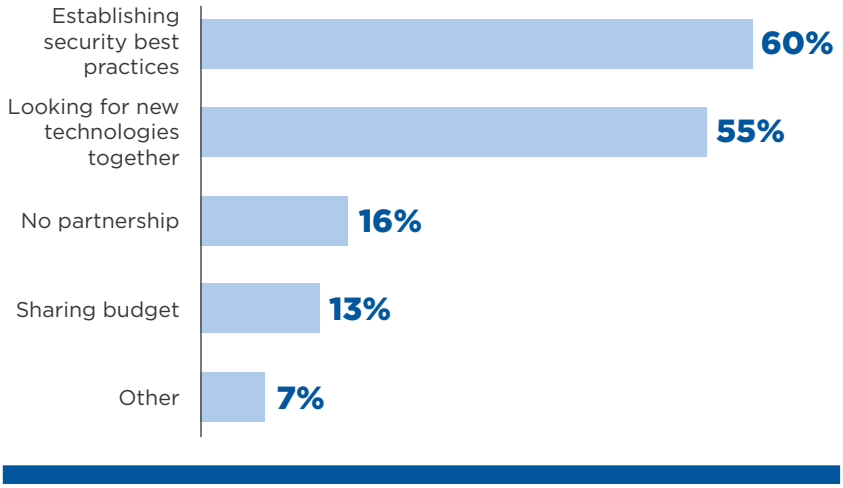
budgets than Physical Security departments, and they're used to receiving funds for constant updates to keep up with advances in technology. Physical Security departments, on the other hand, may invest in cameras and card systems that are expected to remain in place for decades. Such thinking is no longer practical as technology evolves and vulnerabilities are publicly revealed. Physical security equipment needs to be on a refresh rate closer to that in the IT industry.

Most convergence projects—54% according to the ASIS survey—are shared in both the Physical Security and IT budgets, with 24% percent coming exclusively from the Physical Security budget and 22% percent from the IT budget.

Physical Security departments should work to leverage IT budget and justify their investments by highlighting improved risk management and asset protection to the organization. They should stress to leadership that a budget that covers convergence would enhance user experience, which can attract better em-

IN WHAT WAYS DO YOU CURRENTLY WORK WITH YOUR ORGANIZATION'S IT DEPARTMENT?

Select all that apply



ployees and be used to differentiate the organization from its competitors.

Convergence can also help mitigate risk, which is especially necessary in light of the recent high-profile hacks of companies including Home Depot, Target, and Equifax. "Executive leadership is willing to spend money to avoid similar outcomes for their organizations," Arcement said. "There's no guaranteed assurance, but they want to ensure they're keeping up with risk mitigation best practices, which includes attention to both physical and cyber security."

Technical Challenges

Many organizations may be hesitant to adopt a more converged access control system due to implementation concerns, including establishing an upgrade path, compatibility with existing systems, and overall complexity of the upgraded solution. Furthermore, there is an understandable fear of needing to rip and replace existing systems to complete the upgrade.

To illustrate this point, survey respondents were asked to identify their concerns regarding more converged PACS and LACS solutions. The top answer involved managing multiple credentials in various systems, which speaks to operational efficiency, whereas other top concerns included difficulty of implementation/maintenance and increased technological complexity.

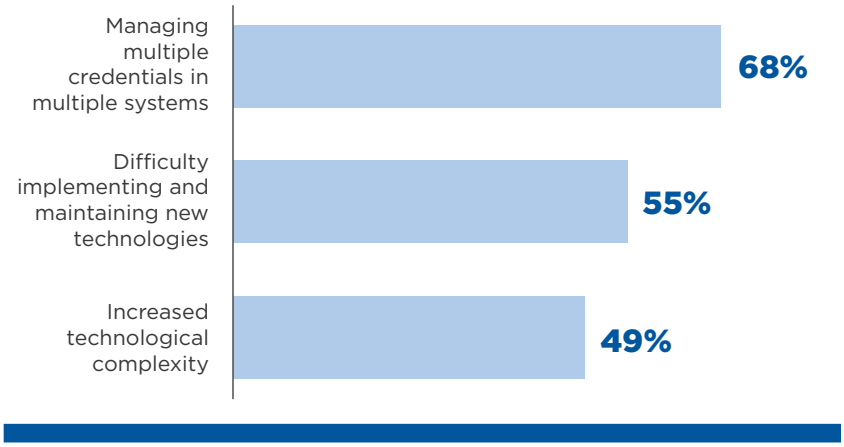
Despite these challenges, understanding implementation best practices, leveraging modern technologies, and collaborating with trusted partners can facilitate the introduction of converged access control solutions more easily than ever.

Best Practices to Successfully Launch Convergence Projects

The primary technical challenge for organizations is the notion that introducing converged access control requires an interruptive rip and replace of existing technology. The reality, however, is that the process can be more simple, such as by starting with converged cards.

WHAT CONCERNS DO YOU HAVE ABOUT MORE CONVERGED SOLUTIONS?

Select all that apply



"We're seeing a trend toward converged cards where it's no longer exclusively the physical access control credential. Organizations are looking to either extend the contactless technology on the card or to embed an additional contact chip on the card for strong authentication to logical access applications as well," Arcement said.

72% of survey respondents indicate that they would like to leverage smart cards for additional applications, with the most useful including network and computer login.

Beginning with a "converged card" approach essentially adds logical access to an existing physical access control system. By doing so, organizations can create a migration path that increases security and convenience but still utilizes existing infrastructure, access control systems, and panels. This allows more converged solutions to be implemented without needing to rip and replace, making upgrades to newer technology less disruptive.

"In terms of logical access, this process usually includes adding credential management software solutions to the IT side of the house to manage the lifecycle of digital certificates on a single ID badge," Loy said. "There can also be multiple integration points to help ease the workflow of getting those cards provisioned for desktop use, making it as streamlined as possible. Some providers also offer professional services to sup-

port whatever is needed to get the system running as quickly as possible."

Arcement also recommends that organizations first pilot the technology before deploying it company-wide. "A marathon starts with one step, and it can be overwhelming to think about all the things that need to be done during the transition of an entire organization," he said. "We have seen companies be most successful by structuring pilots and deployments in phases and by starting deployment in a single building, floor, or department. This enables the project team to clearly understand the opportunities they have with the new technology, the limitations that may exist, and the policy changes that might be necessary to consider before deployment throughout the entire organization."

To overcome organizational challenges, increased collaboration between Physical Security and IT is key, particularly when budget is involved. Loy notes that while budget is a concern, the two departments can share expertise and information to be more cost effective. "Sometimes to get greater security you have to spend more money," she said. "For example, companies typically spend under $10 on a card, but with a converged solution that card could cost $20. You must understand what you're getting and why it's more expensive, and you have to understand risks and associated risk tolerance. Think how expensive it will be if you become the next headline or ransomware attack versus making a change in your everyday security to shore up systems from a physical space and a digital space."

Bridging the communication gap between IT and Physical Security presents another opportunity for increased collaboration. To start, both sides should acknowledge their shared objective – the security of the organization – and recognize the expertise that each side has in the equation. Departmental leadership must understand that their security responsibilities are dependent on vulnerabilities on the other side of the house, because it can mean entry points that ultimately threaten the overall organization.

Facilitating a more collaborative environment can begin with physical proximity and project involvement. To start, IT and Physical Security can share a common workspace, such as an operations center or server room. These teams can also establish a recurring forum to provide updates, discuss vulnerabilities, and share audit data. Survey results shows that while 89% of respondents indicate they conduct a Physical Security risk analysis, only 2/3 of those respondents share the findings with their IT team.

This collaboration should be leveraged to create joint proposals to company executives that show mutual benefit - for example, with increased convergence, ticket volume to the IT help desk will decrease due to a reduced need to reset passwords.

Finally, once a convergence project begins, it is important to train users on the benefits of the new approach. Arcement offers, "Managing expectations is critical as organizations move to more secure technologies—there is a slight change to the user experience." He compares it to shoppers adjusting to using smart card chips on their credit cards instead of magnetic stripe, noting, "At first, the change presented an inconvenience to the user, but cardholders accepted the change because they recognized the added security it provides in this age of identity theft. This offers a good analogy to share with your user population—that this transition is first and foremost designed to elevate security for the organization and all who occupy its facilities."

Conclusion

Physical Security and IT departments are recognizing that now, more than ever, converged threats are real. Vulnerabilities that exist in both domains are fronts that have traditionally been handled separately. In isolation, they can be viewed as managed risks. But when malicious attacks or simple carelessness connect these vulnerabilities, the risks become more than the sum of their parts.

To meet the growing security needs of today's organization, Physical Security and IT must better align their budgets and objectives to reduce risks while ensuring convenience so end users abide to company policies. While more converged physical and logical access technologies can help show the way, the ultimate responsibility lies within security professionals to chart the right course for their organization.