Fundamental Shift:
A LOOK INSIDE THE RISING ROLE OF IT IN PHYSICAL ACCESS CONTROL

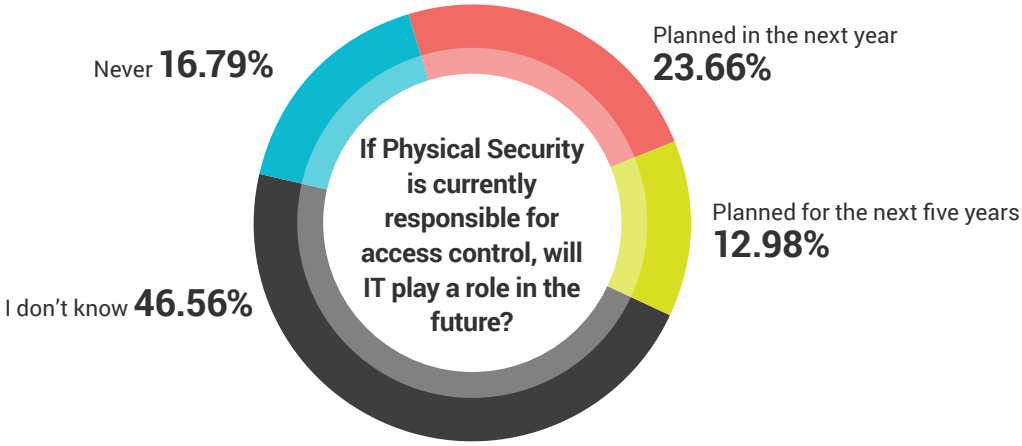
HID®

Shifting budgets and responsibilities require IT and physical security teams to consider fundamental change in day-to-day operations

While physical security professionals have suspected a shift toward increased involvement of the IT department in physical access control, recent research has shown this to be true. A survey conducted by The 05 Group of more than 1,500 IT Managers, Directors and staff, as well as Chief Information and Chief Technology Officers, found that IT departments are now more involved than ever in an organization's physical access control decisions and implementation.

IT departments are now more involved than ever in an organization's physical access control decisions and implementation.

According to the survey, more than half (55%) of respondents reported IT as primarily responsible or having shared responsibility for access control within their organization. As a result, IT leaders are tasked with spearheading not only the protection of their company's network- and cybersecurity-related initiatives – but also those set forth by the Physical Security department to protect employees, visitors and assets from internal and external threats. Similarly, the study showed that the IT department will increasingly play a role in physical security to influence technology decisions (76%) through the integration of access control within the ecosystem (72%), by implementing access control technology (59%), and through the management of access control systems (39%).

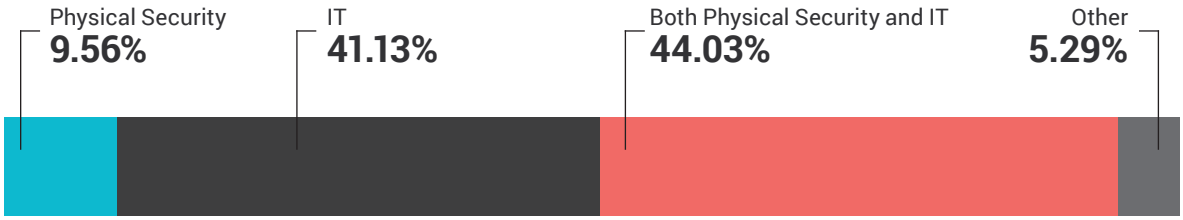


Along with the added responsibility to help implement security solutions alongside IT-related projects, IT leaders are also increasingly responsible for budgeting decisions within physical security. According to the survey, more than 85% of respondents reported that IT was involved in decisions regarding physical access control technology investments.

"The numbers speak to a trend we've seen over the last several years as access control solutions and physical security solutions move from a predominantly siloed approach to a more collaborative method of management," said Luc Merredew, Product Marketing Director, at HID Global. "Questions of connectivity, cloud-based vs. on-premise hosting, and capital investment vs. operating expense are common in this organizational environment."

The purpose of the survey was to gain insight into the relationship between an organization's Physical Security and IT departments, how the two work together and how investments in new technology are made. In this paper, we explore these results and how they can be applied in the increasingly collaborative world of today's organizations.

Which department primarily decides on investments in physical access control?



Physical Access Control Responsibility Rapidly Shifting to IT

While 67% of respondents reported having a dedicated physical security person, department or team in place, the majority of respondents (55%) reported that IT was at least partially responsible for physical access control within the organization. In fact, 26% reported that IT was primarily responsible, and 29% said that IT and the physical security departments shared responsibility. What this means is that since IT and physical security are starting to share responsibility, they also are beginning to share purchasing decisions and resources, including budgets.

Of the respondents who answered that IT is not yet involved in physical access control, 36% reported that IT will play a role within the next year to five years. This indicates a fundamental shift in how organizations manage physical security.

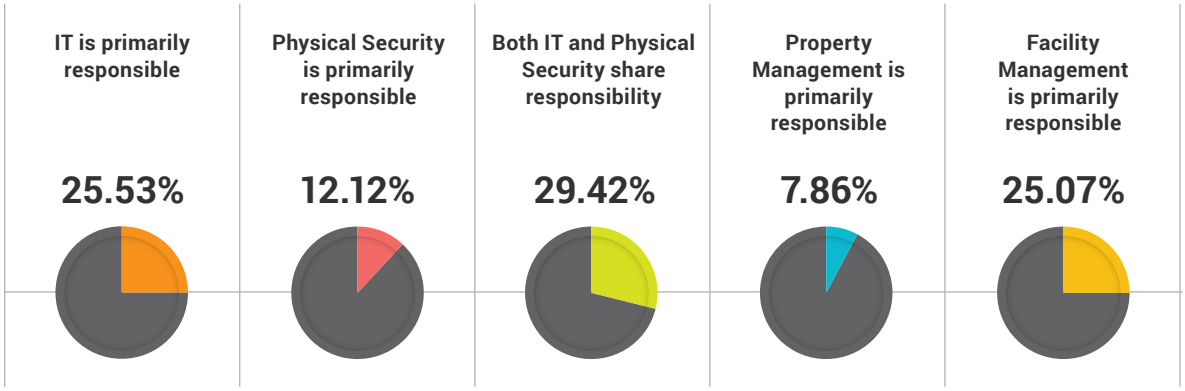
"This result shows the growth of collaboration between IT and physical security departments, necessitating improved relationships between the two entities," said Merredew. "This is a pretty significant change in the way physical security has operated historically – as a department that is able to make decisions unilaterally. Collaboration is no longer a recommendation; it is a requirement for organizational security."

Going further, when the results are broken down by company size, larger companies (more than 1,000 employees) are more likely to have both IT and Physical Security share the responsibility for physical access control (36%). Smaller companies report IT having an even greater role in physical access control, with 37% of respondents reporting that IT has sole responsibility versus 14% of companies with more than 1,000 employees.

As this fundamental shift takes place across organizations, many leaders are tasked with building or strengthening relationships between departments. This means incorporating best practices for communication, as well as establishing an emphasis on the influence of creating a holistic security approach with regard to decision-making. In this approach, the emphasis is on the entire breadth of a security solution, not just access control's potential to be the weakest link in an otherwise sophisticated network security strategy. According to the survey, 76% of respondents said that IT will influence technology decisions as a result of the collaboration between the two departments; while

72% said IT will play a role in integrating access control into the overall ecosystem of the organization. Close to 60% said IT will be responsible for the implementation of access control technology across the enterprise, while 39% said IT will need to manage the access control system put in place.

Who is primarily responsible for physical access control in your organization?



While this seems to be a relatively new phenomenon, of those who reported that IT and physical security shared responsibilities, 34% said that it has always been this way, while 39% said the change occurred within the last five years. For those who reported that IT owns this responsibility, 29% reported that this shift took place within the last five years. Many of these organizations have learned how to better understand the challenges each department faces with regard to security – whether it's protecting people and critical assets, or protecting the information being transmitted within an organization – both of which are important to the overall organization.

What role will IT play in physical security?
Select all that apply

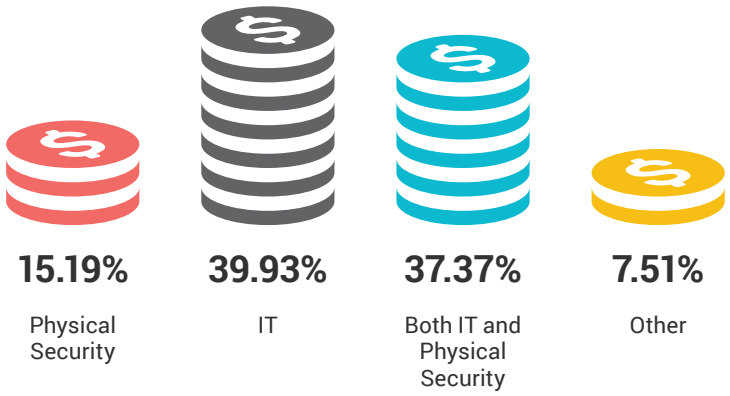
Influence technology decisions	76.60%
Integrate access control into ecosystem	72.34%
Implement access control technology	59.57%
Manage access control system	40.43%

Research Shows IT Absorbing Budgets for Physical Security

Nowhere is this shift as critical than in the process of setting budgets and allocating money for capital investments in IT and physical security infrastructure. As the role of IT expands, so too does the portion of the budget this department controls, making it imperative for open communication about an organization's security needs. Almost 44% of participants reported that both IT and physical security shared investment decisions related to physical access control, while 41% reported that IT is the primary decision-maker on these investments.

Where the money is coming from is also in line with this reasoning, with 40% reporting that physical access control investments come from the IT department's budget, while another 37% said that they come from both IT and physical security funds.

From which department's budget do investments in physical access control systems come from?



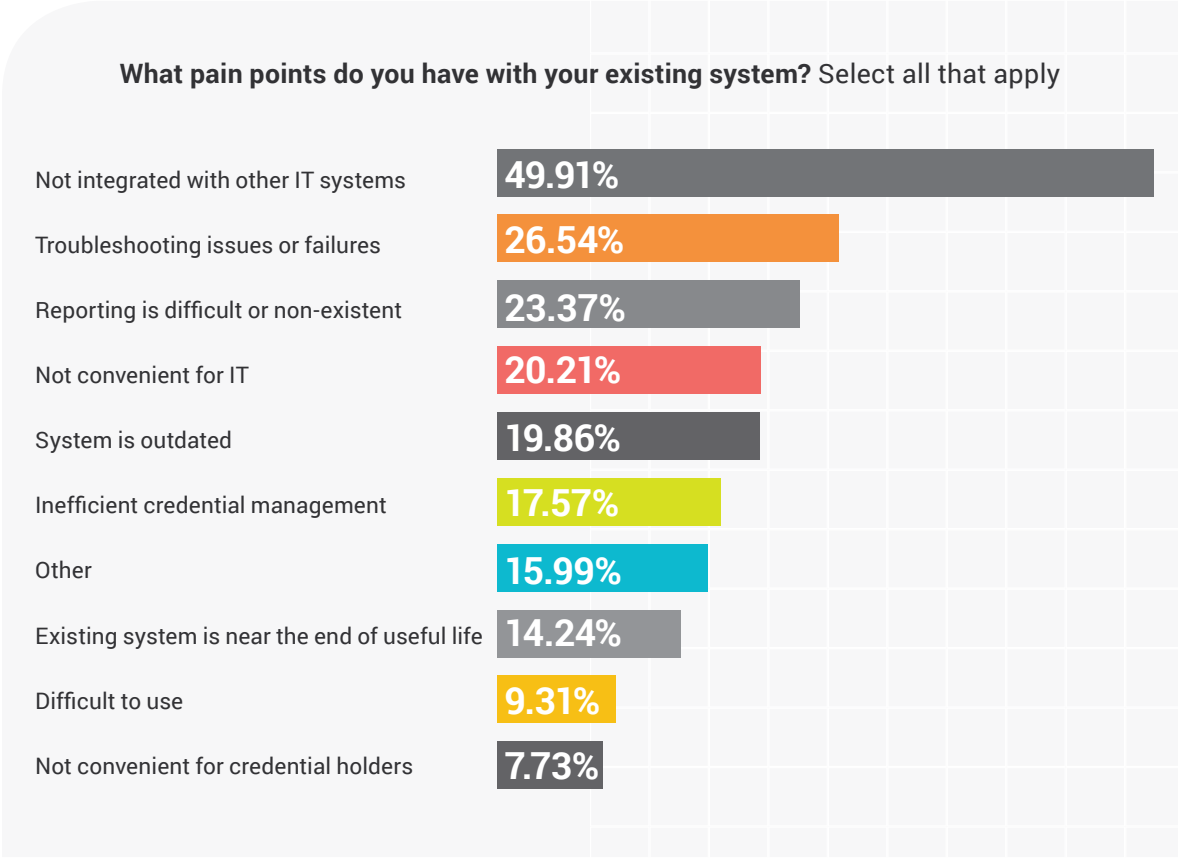
This shift is logical, as physical access control systems become more and more involved with larger network and cyber security strategies. With this increasing interdependence comes the framework for establishing physical access control devices on par with other connected hardware and software platforms. Legacy access control systems that do not place a premium on the latest security protocols should be replaced immediately in an effort to protect an organization's overall security posture. "Physical access control systems cannot be the weakest link in overall organizational security. Without proper IT-centric oversight, they risk being just that," said Merredew. "The results of this survey are clear that across the board, today's organizations must treat physical security with the same focus and diligence exercised on IT networks. The good news is that many organizations recognize this and are evolving to meet this need."

However, the comfort levels of the IT department can be problematic when tasked with making decisions. Only 27% of respondents claimed to be 'very comfortable' with making decisions regarding physical access control systems, while 38% reported feeling 'comfortable' with making these decisions. This seems to indicate that while the decisions are shifting, there is still work to do in educating these individuals on the merits of various systems and solutions on the market. This demonstrates an opportunity for physical security teams to collaborate and showcase their experience to IT leaders when purchasing decisions are made and solutions are implemented.

For many organizations, investments in cameras and card systems are looked at in the vein of longevity. However, as technology evolves and vulnerabilities are publicly revealed, it becomes imperative that physical security equipment be updated on a cycle equivalent to that IT. As such, physical access control systems should continually be updated as needs change and threats evolve.

Addressing the Pain Points of Today's Access Control Systems

Across the board, respondents in both large (>1,000) and smaller companies (<1,000 employees) reported similar pain points related to their current access control solutions, with 50% reporting that lack of integration with IT systems topped their list. Another 26% reported that their access control solutions are difficult to troubleshoot or are prone to failures; 23% said that reporting is difficult or non-existent; 20% reported that their system is outdated; and another 20% said the systems are not convenient for IT.



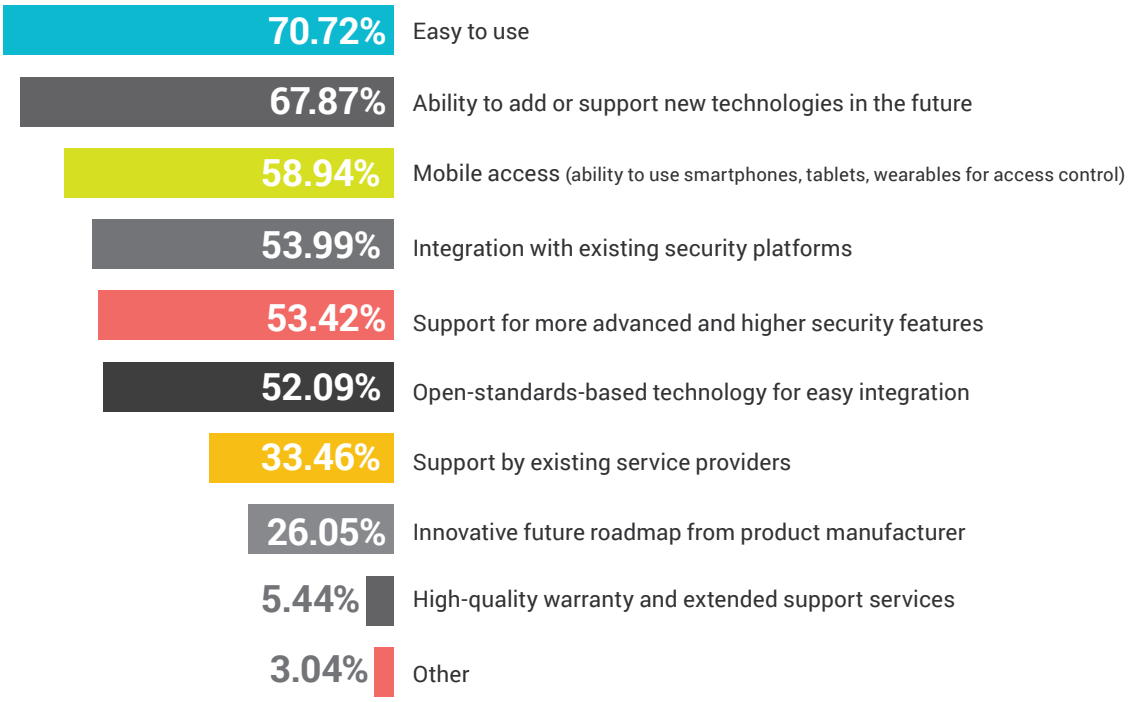
It's important to note that as this shift to IT takes place, the research shows there are still challenges that this department faces when managing physical access control systems. Almost 39% of respondents claim they are 'comfortable' with the individual features within their access control system, while only 16% are 'very comfortable.' Similarly, only 34% are 'comfortable' troubleshooting issues or failures, while only 17% are 'very comfortable' with the task. This leaves room for leaders within physical security, as well as vendors and integrators, to increase the level of training and education offered when a new access control solution is implemented within an organization.

Regardless of size, the results show the importance of developing a stronger relationship and shared training initiatives between the two departments to streamline and better understand the synergy between IT and physical access control. IT must also make the effort to become more familiar and comfortable with physical access control systems in order to better serve the goals of the organization.

Emerging Technology and the Features that Make Access Control Cohesive with IT

Critical to the success of a modern physical access control solution is the ability to prevent unauthorized individuals from accessing network-related hardware, while also presenting security directors with the ability to easily add options for emerging technology, such as mobile devices or biometrics. More than 68% of respondents agreed, saying one of the main feature requirements in a new solution is the ability to add or support new technologies in the future.

Which of the following features would you most require in a new physical access control system? Select all that apply



Ease of use is another critical component, with 71% of respondents naming this as a requirement of a new physical access control system. Ease of use saves time, effort and resources across departments, allowing for increased focus on higher-priority projects. Other requirements listed by respondents included: integration with existing security platforms (54%); support for more advanced and higher security features (53%); open standards-based technology for easy integration (52%); and high-quality warranty and extended support services (46%).

These answers support the argument that IT leaders want technology that is more easily integrated with existing and incoming solutions. This is also an indication of the need for organizations to be

able to scale accordingly; the older the technology, the less likely it is to be able to integrate with existing security solutions and align with networking needs. Today's organizations must invest in solutions that meet the requirements of IT and physical security leaders.

More than 58% of respondents named mobile access as one of the features they most require in a new physical access control system, indicating a shift toward mobility and flexibility for incoming solutions. 'Mobile access' includes the use of smartphones, tablets and/or wearables for access control. This also indicates an increasing acceptance of mobile credentials for access control, which allows organizations to have more flexibility in deciding which form factors are best for their unique access control needs.

Conclusion

Today's organizations must be more collaborative internally than ever, especially within the realm of security. Physical access control decisions and responsibilities are seeing a fundamental shift toward the IT department, requiring both departments to better work together to achieve true security across the enterprise. It is clear the shift toward the collaboration between IT and physical security departments are resulting in a more unified approach to security, which results in a more united front to combat incoming problems.

As a result, IT professionals need to rely on physical security teams for their expertise and support when implementing new technology, while physical security teams must do the same with regard to IT-centric decisions. Additionally, it is critical for physical security teams to demonstrate their value to the overall security posture of the organization. By focusing on the collaboration between the two departments, physical security teams can retain control over their budgets and investment decisions, as well as the ability to prioritize the safety and security of the organization.

Similar to the threats today's organizations face, the needs of these organizations are constantly changing, leading companies of all sizes to the realization that physical access control solutions must fall in line with the standards that the IT department has set forth to protect assets and people. As new technology is introduced into the ecosystem of an organization, it's imperative that close collaboration between physical security and IT departments continue to grow and thrive to meet and exceed the expectations of safety and security.

METHODOLOGY

The 05 Group surveyed 1,576 individuals, representing more than a dozen different industries, including Education (19%), Information (16%), Government (11%), Manufacturing (8%), Health Services (8%), and Security, Professional and Business Services (8%). Of the respondents, 35% were IT Managers, 26% were IT Directors, 13% were IT Staff, 8% were CIO/CTO, and 3% were VPs of Technology. Breakdown of business size is as follows: 24% have less than 100 employees, 22% have 101-500 employees, 11% have 501-1,000 employees, 17% have 1,001-5,000, 6% have 5,001-9,999, and 6% have 10,000-24,999 employees.