arcules

The State of Physical Security and IT Convergence

Examining the challenges, benefits and quest for cohesion between the two departments

White paper

WHAT'S INSIDE

arcules

60%+

of security cameras shipped in 2017 were network cameras*

16%

compound annual growth rate for Access Control as a Service between 2017 and 2022**

***According to market research firm IHS Markit**, more than 60% of security cameras shipped in 2017 were network cameras.

Access control has been increasingly making its way to IP and the cloud, in particular, as **IHS projects that the market for Access Control-as-a-Service (ACaaS) will see a compound annual growth rate (CAGR) of 16% between 2017 and 2022, compared to just a CAGR of 6.2% for the traditional equipment market.

Examining the challenges, benefits and quest for the cohesion between the two departments

The concept of convergence, which is the intersection of physical security devices and systems with Information Technology (IT) within organizations, has been discussed among industry professionals ad nauseam for more than a decade. However, the slow migration from analog to IP within security, which has been notoriously slow to adopt new technology historically, meant that many of the promises of convergence – simplified management and streamlined maintenance of systems just to name a couple – were not available to the vast majority of end users.

But the proliferation of Internet of Things (IoT) devices and an ever-increasing number of video surveillance, access control and other security systems making their way onto the network has resulted in internet-enabled solutions becoming the norm in the market rather than the exception.

Despite the march towards IP and cloud technology, the goal of convergence remains elusive for many businesses today. Clearly the technological capabilities for convergence are readily available but there are myriad reasons why bringing these two traditionally separate departments together under one roof is still a major challenge in organizations, not the least of which involves corporate politics.

The days of operating in silos, however, is coming to an end and physical security and IT professionals must learn sooner, rather than later, how to work together to deliver value to the organizations they serve. Security has become the backbone of our connected world, but it cannot live up to its maximum potential without a strong IT infrastructure backing it up. It no longer matters who "owns" these systems but rather how they're providing return-on-investment (ROI) for the organization, which now expands well beyond the traditional purview of security.

arcules

A Shift in traditional roles and responsibilities

Before we delve into where overlap exists between physical security and IT today and where greater efficiencies could be achieved via convergence, we must first review how these functional areas have evolved within organizations.

Historically, physical security in corporations has been viewed through the lens of what many in the industry refer to as "guns, guards and gates," which really marginalizes the valuable contributions that security personnel make to improve the bottom line of businesses. This mischaracterization of security still permeates many organizations; however, the fact is that security leaders today come from a wide range of backgrounds and business experiences and they are helping to change these outdated stereotypes.

IT professionals have typically been those responsible for implementing and maintaining all the various technology systems, such as computer networks and applications, that a business depends on to properly operate. Of course, the number of systems that IT is responsible for today has expanded well beyond desktop PCs, email services and Microsoft Office programs to include a wide range of solutions, including many security technologies that reside on the corporate network.

As their role in implementing and maintaining security systems has grown through the years, IT professionals have also been given a seat at the table when it comes to the procurement of these solutions. A **study conducted by Enterprise Strategy Group on behalf of Axis Communications** several years back found that more than 90% of surveillance deployments involve IT departments. Additionally, 47% of IT professionals surveyed for the study indicated that their group was the most responsible for setting the organization's surveillance strategy and making final infrastructure purchasing decisions.

IT is also being leaned on more heavily when it comes to making decisions related to buying and deploying access control technologies. **A survey recently conducted by HID Global** of more than 1,500 IT managers and staff as well as CIOs and CTOs found that IT is primarily responsible or has shared responsibility for access control within 55% of organizations. In addition, 76% of respondents said that IT would continue to influence technology decisions related to physical security. Systems integrators also say that the shift of buying power to IT has had a profound impact on their businesses. According to the **2019 State of the Industry report published by *Security Business*** magazine, 32% of integrators surveyed identified this shift as one of the biggest threats to the commercial integration market

90%

of surveillance deployments involve IT departments

32%

of integrators surveyed identified this shift as one of the biggest threats to the commercial integration department

arcules

The combination of technology innovation and the changing roles of physical security and IT within organizations has thus created an overlap in the responsibilities of professionals on both sides which is why convergence has become paramount for companies that want to realize greater efficiencies moving forward. However, old habits die hard as they say, and true convergence remains lacking in most organizations today as IT and security personnel cling to their silos.

It's not just physical security and IT departments that have undergone a significant transformation in their roles and responsibilities within organizations, but also C-level executives charged with leading them, which include:

CSOs

The role of the Chief Security Officer (CSO) in organizations was borne out of a need for businesses to consolidate the job of security, which had typically fallen to facilities managers and/or guards, under the leadership of single person responsible for protecting the company's people and assets across their entire geographic footprint. In addition to overseeing physical security measures at an organization's facilities and developing executive protection programs, these individuals have been tasked more recently with ensuring that sensitive company data doesn't fall into the wrong hands.

CIOs

A Chief Information Officer (CIO) has typically been the person in charge of overseeing the implementation of various technology systems throughout an organization. However, in more recent years, the job has undergone a shift from being technically focused on the nuts and bolts of various systems to one that places a heavy emphasis on overall business strategy given the digital transformation that is currently taking place in many organizations. Many CIOs have also been saddled with security responsibilities — both cyber and physical – adding yet another of complexity to the role.

CISOs

A relative newcomer to the C-suite, the position of Chief Information Security Officer (CISO) was created to manage the herculean task of protecting the treasure trove of data that organizations are collecting today. Given the number of high-profile data breaches that have taken place at businesses both large and small over the past several years and the bevy of regulations being passed to hold organizations accountable for their data protection practices, CISOs are under immense pressure to implement technologies and practices that can keep pace with modern cyber threats. With more physical security devices making their way onto the network, CISOs must also ensure the cybersecurity of these solutions to prevent them from becoming a backdoor for hackers.

Overcoming internal obstacles to convergence

Considering the obvious advantages of convergence, which includes significant cost savings by reducing the number of disparate systems and the personnel needed to monitor them as well as improved situational response via the implementation of a holistic security management solution, the concept still hasn't taken hold in many companies due to the political challenges involved. Having operated independent of one another for so long, both physical security and IT leaders are afraid of relinquishing control of any aspect of their responsibility to their counterparts on the other side for fearing that once the horse is out of the barn there will be no turning back and that things that used to be their purview – and thus their way of delivering value to organization – will be no more.

A perfect example of this is the classic struggle that sometimes takes place between these two entities in determining who oversees various security technologies and deciding where the role of physical security and IT begins and ends in that. Physical access control for things like building doors and lobby turnstiles has typically fallen to corporate security departments and/or facilities teams to control, while cybersecurity and logical access – determining who can access computers and other technology systems – has been overseen by IT. As more physical access systems have made their way onto the network, however, IT has found itself increasingly being turned to issue and/or revoke credentials. Likewise, cybersecurity threats can sometimes manifest themselves in the form of a physical intrusion, making the physical risk mitigation expertise of security practitioners a key cog in an organization's overall cybersecurity posture.

arcules

24%

of organizations have converged their physical and cybersecurity functions*

52%

of senior professionals have converged 2 or 3 functions from physical security, cybersecurity and business continuity*

*See right for full data details

The Cybersecurity Component

Addressing threats related to cybersecurity are another reason why many industry pundits anticipated that convergence would have become more widespread now than it has. Data breaches and malware attacks have become almost a daily occurrence in the corporate world. Add to that the threat posed by unsecured IoT devices like surveillance cameras and video recorders that are proliferating business networks, there are more potential entry points into businesses now than at any other time in history. Despite these challenges, actual convergence numbers remain low.

The **results of a survey published in early 2019 by the ASIS Foundation**, found that just 24% of organizations have converged their physical and cybersecurity functions. When business continuity was factored in, the survey, which polled more than 1,000 professionals with senior roles in physical security, cybersecurity, disaster management, business continuity, and related fields found that 52% have converged two or all three of the functions together. In addition, of the 48% who had not converged any of the functions, 70% said they had no current plans to do so.

And while many in physical security and IT remain fearful about the potential outcome of combining their efforts, organizations that have undergone such convergence overwhelming say it was a good thing. In fact, the ASIS Foundation survey found that 96% of businesses that had converged two or more of these functions experienced positive results and 72% felt that convergence strengthens overall security. Also, when it comes to combining physical and cybersecurity, money isn't the primary driving factor as only 7% of converged respondents reported "reduction in security costs" as a primary benefit. The number one reason cited by survey respondents (38%) when asked what might convince them to converge was "better alignment of security/risk management strategy with corporate goals."

arcules

Cloud to the rescue

So where can organizations looking to begin the process of convergence turn to for help in kickstarting such an initiative in their business?

Beyond mapping out what goals you want to accomplish with your security and IT leaders, one of the best places to start a conversation about converging these departments, at least from a technology perspective, is by taking a look at how the organization could benefit from deploying systems in the cloud.

The benefits of cloud video surveillance and access control services are similar in that they allow businesses to shift what has traditionally been a capital expenditure into an operational expense spread out over a monthly, quarterly or yearly basis. Cloud platforms also reduce the onerous maintenance burden placed on IT and security teams as common technical issues, such as camera failures, can be quickly diagnosed and fixed by the vendor. Additionally, these solutions can help organizations stay ahead of potential cybersecurity threats to their physical security systems as device software and firmware updates can be pushed out automatically by the cloud provider, eliminating yet another common maintenance headache.

With one of the main goals of convergence being to streamline the management of systems residing on the network, cloud solutions provide everyone – whether they work in IT, security, HR or elsewhere – with universal access to a common operating picture regardless of their physical location. The ability to work in a singular platform for video and access control also means that personnel doesn't have to be trained on how to use multiple systems, breaking down another barrier between that has previously existed between security and IT.

Chances are you're already using the cloud for a variety of business applications, be it with something like Office 365 for email or Salesforce for customer relationship management (CRM).

About arcules

Arcules is aiming to set the standard for agility, security, and analytics for video surveillance in the cloud. Whether you resell, offer consulting and integration services, you will have access to a collection of resources to ensure your status as a trusted advisor to your customers and prospects.

Learn more at **arcules.com.**

The fact is that both physical security and IT are needed to address the broad range of threats facing organizations today and fortunately, data shows that the relationship between the two sides is improving. **According to the results of a study published last year by ASIS International and HID**, 60% of physical security professionals indicated that they work with their IT departments to establish security best practices, while 66% said they look for new technologies together.

Working together also means that costs can be shared evenly between departments. The aforementioned study also found that most convergence projects, 54%, are shared in both the physical security and IT budgets, with 24% coming exclusively from the physical security and 22% from IT.

Aside from cutting costs by eliminating duplicated efforts in an organization, convergence, if realized, will enable companies to strategically align their goals and Subsequently establish a common mission for security within the organization. At the end of the day, the board and the majority of the C-suite view things like data protection as enterprise risks that require a comprehensive mitigation strategy regardless of who "leads" it.

Arcules

info@arcules.com
arcules.com