The Convergence of Physical Security and Cybersecurity in Business
How the topic of physical and cyber security convergence began.

In 2011, John Carney, Senior Technical Manager of Cisco Government and Security Solutions wrote a white paper on the integration of physical and logical security (otherwise known as cyber-security) to address the concerns of government entities. He stated that when physical and logical security teams are disjointed, systems within the company, such as access control and video, become disjointed and less effective.

In most organizations today, physical security teams and the logical security teams track users separately. He used employee termination as an example. “In disparate systems,” Carney says, “there is time lag across all systems in terminating the employee, and in some cases can be missed altogether in one system, which imposes serious threats to a company.” When convergence of the departments occurs, there is a more consistent flow of information and processes that work to protect the company from all sides.

Advancements in physical security technology, now include new cloud-based systems, wireless cameras and alarms, and remote view for mobile devices over Wi-Fi. Businesses need to be concerned about how these systems affect their internal IT systems, and begin to think about how both types of systems can merge to benefit and streamline the process of managing both people and security.

Here at Allied, we have faced situations where businesses with federally protected or internally protected information have caused a roadblock in the physical security project as soon as IT leaders discover there are 3rd-party networks at play. This issue goes beyond government entities now, as more and more businesses rely on IT infrastructure to manage security.

What are some of the issues involved in integrating cyber and physical security?

Today, local and national security companies are finding that all businesses need to be aware of the two departments, and the departments need to be aligned or combined so they can work together. They need to have a common strategy. Policies need to be combined to cover standardization of both physical and logical security.

Physical security systems for businesses are now more technical than ever. They require network access and must include mobile. All of these features require integration into internal systems and networks. In addition, banking, healthcare, and government verticals are being forced to comply with federal regulations regarding Personally Identifiable Information (PII).
With new integrations between cyber and physical security, physical security vendors are being held to the same standards as traditional IT vendors. This change is causing integrators to struggle to adapt to a space they are not as experienced in. Any breach or system failure caused by a 3rd party integration could be catastrophic to the organization.

One successful approach is to start with the existing ‘on-premise’ and cloud-based services. Security integrators can then help IT Departments find a physical security vendor that will integrate with their current systems and make physical security an extension of current identity management systems. Utilizing the right service and integrating it with Active Directory, or cloud-based identity management systems, can give administrators a single pane of glass to manage both physical and logical access.

Companies can often use their current mobile administration tools to manage users, or may be given new mobile administration tools to suit the growing need for mobile management. If communication and processes are not functioning perfectly between managers of each system, something will be missed. By setting up integration between physical and logical systems, the chance for errors is greatly decreased.

**How can you align physical and logical (cyber) security?**

If your organization already has the physical security systems in place and they are capable of integrating with networks, it is recommended to begin a change management plan to integrate the departments. This will require information from the physical security provider and the IT department in defining the strategy and the plan to build out a successful integration.

Some of the more important items to consider in this project would be defining user access privileges, roles of individuals who have access to what modules or components and their controls within each system, and systems that will be in place to protect one system from another in case of, say, a breach of a firewall.

One solution often utilized here at Allied Fire & Security is running a parallel network so that the physical security system does not interfere with the logical security system within the company. This is done because most businesses don’t want a 3rd party integrated with their logical systems. When set up this way, no additional network nodes are required to be secured, and any breech in security vendor software would not cause a loss of PII.

Allied has also taken advantage of changes and advances in access control and video surveillance systems to utilize new solutions that are client-initiated, with no setup required and no infrastructure that could be compromised on-site.

With this new generation of security systems, Allied is able to provide the customer with best-in-class services, while ensuring an easy path to a successful audit. These systems no longer need to have the
additional cost and maintenance of a physical service. They provide the same level of service as integrations into identity management services that tie physical and logical security together.

Decision-makers will need to start thinking about how to merge the physical and logical security processes in their businesses, and develop a strategy that utilizes the varying use cases that security integrators have experienced, as well as the experiences of the IT people.