How technology integrators can successfully merge IT with physical security systems.

Author - Eric Bracket

Published on March 19th, 2020 - securityinfowatch.com

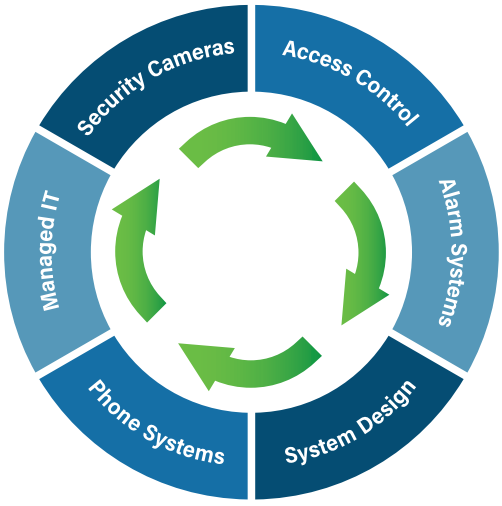
"When engaging with a technology provider, it is important that customers know what they are paying for"

Managed IT providers that can handle phone (VoIP), physical security and company networks can extract more value from a fully integrated implementation of all these aspects.

Traditionally, security cameras and access control systems were installed as independent systems by security integrators – even in the early days of IP-based devices. However, the continuing advancement of IP-based technology, as well as the inherent cybersecurity vulnerabilities of physical security systems, now place that task squarely at the feet of technology integrators with extensive knowledge and background in IT.

By entrusting this task to integrators with extensive knowledge of the available products and component parts of security systems and how they can be interconnected, there can be a tremendous added value at facilities such as hospitals, says Stanley Horn, Facilities Director at Olympia Medical Center, an Alecto Healthcare Hospital in Los Angeles, California.

"I've worked in other facilities where one vendor puts in the security cameras and another vendor puts in the card key access and the two are not integrated," explains Horn. In addition to some aspects of security, his responsibilities range from building engineering to housekeeping, bio-med and all construction projects.



Solid Integration Solutions Key for Healthcare Facilities

For today's healthcare facilities, this is unacceptable given the potential safety risk to patients and staff, the potential theft of medical equipment or medications and other security concerns.

"You can't have [unauthorized] people wandering through the facility, and if anyone can just walk in and out, there could be an issue," says Horn. "So, it's extremely important to have a comprehensive, integrated security system."

As part of his duties, Horn worked with other staff at the hospital to upgrade the existing security system, which included a card access system and some older analog security cameras.

"The key card access was installed by somebody that really was not familiar with what they were doing, and so all it did was open the door," explains Horn. "You can do the same thing with a key."

According to Horn, the security upgrade project was completed in two phases. The new digital cameras were installed first in critical areas, including the emergency room, while also integrating the existing analog cameras installed outdoors.

"We did not want to have to throw everything out that was already installed," says Horn.

In the second phase of the upgrade, a more advanced access system was installed. The system was integrated with the security cameras so that each time staff entered or left a secure area, the camera footage was bookmarked for easy reference.

"Now, from a security standpoint, if somebody comes into this hospital, we can see the time they entered and verify who they are," says Horn. "We can track them with the cameras and quickly bring up history. It is really great for security, and it really moved the hospital up a notch."

The benefits of an integrated access control system with the IT network, including the HR database, also has advantages when coordinating changes in employee status. If an employee is terminated, for example, the system automatically deactivates the employee's keycard. If that same employee has remote access to the security cameras, the network can disable the account immediately.

"...I am always in the know whether I am at work or remote, and I only have to deal with one vendor," - Charles Lomboy

For Los Angeles-based AltaMed, a 46-site health clinic network that serves nearly a million patient visits annually, managing the access control cards for employees required four full-time employees in 2016. With so many sites, there could be 100 new hires and 25 people leaving the company or being reassigned in a single week.

However, the existing system was not fully integrated, which soon drew the attention of the CIO, Facilities Manager, Safety Coordinator and VP of Administration. The CIO immediately had questions about why the system was not connected to their company-wide database, as well as why four people were needed to manage the access cards.

After submitting a proposal, BTI installed and now manages the CCTV, access control and burglar alarms for all 46 sites. Today, they are still growing rapidly, but they don't require any people in the organization to manage any of the physical security.

The role of the technology integrator does not end once the system is installed. Proactive monitoring should be employed so that the system actively oversees technology performance to identify anomalies even before a malfunction occurs. Problems are addressed efficiently, often without the customer even knowing about it. When site visits are required, the monitoring system dispatches an engineer without interrupting the customer.

"Our 24-hour monitoring system sends me alarms by email, text, and phone. I am always in the know whether I am at work or remote, and I only have to deal with one vendor," says Charles Lomboy, Director of Physical Plant Management at AltaMed.

"We trust them as subject matter experts on security," adds Lomboy. "They surveyed our offices and recommended the areas that needed improved security. They also listened and responded to our needs as they relate to patient rooms, medication cabinets, entrances and exits, etc.

Managing Costs

Although technology integrators sound like a high-end service with a commensurate price tag, that is not necessarily the case. An integrated approach with the best-of-breed solutions on the market delivers economies of efficiency and scale that are often passed on to the customer.

If you go to a vendor in commercial security that sells a specific brand, they may try to interest you in their products that are currently being promoted. It might not end up being a fully operational solution to the business problem they are attempting to solve.

Lower price solutions, including security cameras from overseas providers, can also often cost more if a hack or other breach occurs. Many customers are not aware of how products, especially those purchased based on price, can bring embedded vulnerabilities into a network. Some cameras manufactured in China, for example, have susceptibilities that are known to hackers. Major breaches have already occurred with what we call pre-hacked technology.

Even technologies that don't carry the risk of being pre-hacked can become vulnerable when users fail to fully implement the security features on the connected network. Fortunately, a technology integrator with a background in IT can implement advanced cybersecurity processes to block viruses and hackers from destructive solutions as well.

Finally, when engaging with a technology provider, it is also important that customers know what they are paying for with contracts that clearly spell out each installed product, feature, and support item or service they are purchasing.

Technology integrators should bear the cost of providing an initial assessment of their needs. The bid should itemize the costs for equipment and support. It should also anticipate future upgrade paths in order to provide transparency to future expenses. In this way, a customer knows their initial, ongoing and upgrade costs and can budget accordingly.

About the Author

Eric Brackett is President of BTI Communications Group, a technology convergence provider serving the healthcare, logistics and aerospace sector.

For more information on BTI Communications Group, please call 1-312-432-5300, or contact info@btigroup.com, or visit https://www.btigroup.com.