At large hospitals, security directors find themselves facing a number of complex challenges. Not only do they have an overwhelming number of systems to integrate, monitor, and control, but they also need to manage, train, and coordinate manpower. And, while they are expanding their use of traditional systems like close circuit TVs (CCTV) and access control, they’re also deploying new and emerging technologies such as video analytics, biometrics, and radio frequency identification (RFID). In addition, powerful integration tools and capabilities are now available to “link” these various technologies together.

As a result, security departments are gathering data and analyzing information from an increasing number of sources, and they’re encountering a large stumbling block in trying to accomplish this task. Often, the information in the various systems cannot be easily shared, which delays the ability of the security department to investigate and resolve incidents quickly.

In addition, cost pressures have led many security directors who oversee multiple command centers to review and evaluate the opportunity to consolidate centers. Systems integration technology has advanced to the point where the cost/benefit analysis of operations center consolidation can provide significant cost savings as well as operational efficiencies vs. managing multiple command centers and their various, often disparate, systems.

To meet this challenge, one strategy is to consolidate disparate monitoring and operations centers into Security Operations Centers (SOCs)—centralized units that deal with security issues. By consolidating, large hospitals can get a handle on security system “sprawl,” create one central place to monitor and control multiple security systems, better manage and coordinate officers in the field, and implement new technology measures in a more efficient manner. This paper will examine some of the pros and cons of consolidating SOCs.

HIGHLY INTEGRATED SYSTEMS

The move to a consolidated SOC dovetails with the trend of hospitals to integrate physical and logical security systems. “As a part of this new economy, the software providers enable integration services, which bind together many different systems, including surveillance, networking, servers, storage, access control, and other building systems,” wrote security consultant Kevin Marier in Security Magazine. “This ultimately results in a highly integrated and more advanced physical security solution.”

Under a traditional system, a large health system might need one or more workstation to monitor each video or access control system. Security teams could be required to learn how to operate each system, then manage and
respond to each alarm coming from these systems. In turn, this will result in a larger workforce to manage as well as extensive training.

A consolidated SOC could solve many of these issues — while it requires a greater upfront investment, that is usually offset by a lower total cost of ownership.

One solution is the installation of a physical security information management system ("PSIM"), which synthesizes data from video, access control systems, and other physical sensors. The Proximex Surveillint™ PSIM solution leverages existing cameras and other security systems and technologies into one, fully integrated command and control center. As a result, this provides a centralized view of an organization's security environment in order to monitor events for response and resolution, thereby reducing costs associated with monitoring. For example, a hospital could track suspects across multiple camera views easily, without memorizing camera IDs and locations or manually searching recorded video clips.

At the same time, a PSIM can monitor system health and identify facilities incidents such as a water main break or a power outage, to trigger operational alerts through the same user interface so they can be addressed faster.

“One calling card of the consolidated SOC is they are less complex to maintain and expand. They are designed to be scalable and support thousands of sensors and virtually any type of security system, including video, intrusion, access control as well as advanced technologies, such as video analytics, biometrics, fire and life safety and RFID.”

When physical security systems are integrated with IT security, facilities management, and business operations, the data amassed from this complete solution needs to be managed and shared with outside stakeholders and agencies,” says Larry Lien, vice president of product management for Proximex.

The Southern Arizona VA Health Care Systems facility located in Tucson, AZ, which serves more than 170,000 veterans in southern Arizona and western New Mexico, is now bringing its existing security systems into a single environment. The project will integrate several legacy security systems, including hundreds of cameras and thousands of alarm points and card readers, into one command and control system.

This will provide a straightforward way to ensure policies and government regulations are met during an incident response. In addition, the consolidation allows the healthcare system to meet new compliance regulations by improving situational awareness and reducing reporting procedures from days to minutes.

In the past, SOCs were typically redesigned every five to 10 years, but this approach is being replaced by ongoing SOC technology lifecycle planning. In an interview on Microsoft’s TechNet Radio, Johnny Walker, a senior program manager for Microsoft Global Security, says that the nature of SOC upgrades has changed from complete “forklift” redesigns to designs that can evolve as both technology and security applications needs evolve.

Consider Hillcrest Medical Center, which recently implemented a new SOC that includes a sleek new custom security desk console, track lighting, and the addition of a thick sliding glass door that acts as a sound barrier between the SOC and the rest of the security office. On its web site, the medical center noted that after its physical improvements were done, it was also vetting new video analytics software solutions that...
would expedite searching for specific images and to replace existing software.

That new software would allow for a live search of a lost child by T-shirt color, alert when someone enters an exit-only door, determine when an unidentified object has been left behind, or use facial recognition. "This type of software gives staff the ability to scan and glean information from multiple security cameras, which can help save precious time during an emergency," the medical center stated.

Multiply this over many hospitals in a large system and it’s easy to see the challenges that are involved in keeping numerous SOCs up-to-date and coordinated. One calling card of the consolidated SOC approach is that it’s less complex to maintain and easier to expand and/or update than multiple, “disconnected” centers.

A consolidated SOC can be scaled to support thousands of sensors and virtually any type of security system including video, intrusion and access control, as well as advanced technologies, such as video analytics, biometrics, fire and life safety, and RFID. This provides a high degree of “future proofing” during a time when rapid technology advances make it difficult to foresee what security measures a hospital might need in just a short while.

For all of the advantages of a consolidated SOC, merging systems is not necessarily a simple task, especially when those systems were developed at different times by different people. James Woodbery, director of security for MedWest Health System in Waynesville SC, faced this task when the system added two hospitals in 2010.

He found that the merger brought challenges of integrating people, knowledge, and systems. “The camera system they had in place...was a mix and match and they really didn’t have a standard they were using,” he told Security Directors News. One of the campuses had a history of using different manufacturers for its equipment. “When something happened and a camera went down, we had all these companies who said, ‘Oh, it’s them or it’s them,’” he said. “We wanted to get one provider we could call for everything.”

Following the acquisition of a new hospital, one of the first hurdles was to simply become familiar with the physical design of each campus as well as the IT staff at those facilities. “We had to learn the building and try to work with the IT department because they do things differently than we do,” Woodbery said.

Also, with a consolidated SOC, a higher degree of collaboration is needed to bring all impacted departments together. For example, Chuck Klawans, the information security officer at Children’s Hospital and Health System, notes that there are pros and cons between having two security colleagues as part of the IT group at the 240-bed pediatric center in Milwaukee, Wisconsin.

“It’s the role of IT to get things done on schedule, and if security has concerns, there’s the potential for conflict when the IT director or CIO hurries the application or device in, and security may get bumped,” he told Security Directors News.
Security systems, especially at large medical centers, are becoming more complex, and they will become even more so as hospitals continue to add new security mechanisms. Consolidating Security Operations Centers (SOCs) should be considered as a way to help safeguard the future, improve processes and responsiveness, and enable the quick addition of new technology. This approach provides healthcare facilities with improved technology and a better command and control methodology, while allowing for consistent policy enforcement and compliance.

Consolidating SOCs does come with a higher upfront cost, which must be balanced against the lower, long-term costs of ownership. Hospitals must also weigh the challenges of technology upgrades, as well as the collaboration issues of bringing more people together during the consolidation of multiple systems and functions. However, for many healthcare organizations, consolidating SOCs can be an effective way to meet the security and compliance demands that are likely to grow even more stringent in the future.

ADT® Healthcare provides business solutions that help impact strategic goals within patient care facilities. Through integrated security solutions, ADT helps you improve processes and maintain compliance, while maximizing your return on investment. Our mission is simple: To help you provide a safe and secure environment in which to deliver patient care. To learn more, call 877-330-7404 or visit www.adtbusiness.com/healthcare and discover the ADT approach to healthcare security.