

A Guide to Managed Video Services: Part I

How to increase security, enhance safety and improve operational efficiencies

The last several years have presented businesses, large and small, with growing security challenges from a multitude of directions. To help further reduce false alarms, many municipalities are passing stricter alarm ordinances, which require verification of actual security events before police officers are dispatched, and which often impose escalating fines and law enforcement nonresponse in the absence of verification.

In the U.S. the federal government has stepped up homeland security requirements, with the Department of Homeland Security enacting and enforcing regulations such as Chemical Facility Anti-Terrorism Standards (CFATS), while the Food and Drug Administration (FDA) and Customs-Trade Partnership Against Terrorism (C-TPAT) more aggressively enforce security regulations.

Executives routinely change jobs meaning that companies are being forced to more aggressively protect proprietary business information and intellectual property. Violence, harassment and other workplace threats are continuing to escalate, and companies are being compelled to add more policies, procedures and technologies that help enhance employee safety.

All this is happening in a business environment where companies are decreasing capital expenditures, downsizing workforces and cutting budgets. Management on every level is being forced to rethink processes that have been mainstays in security, operations and human resources.

Feeling the squeeze

More than ever, companies are looking for competitive advantages to differentiate themselves. Yet, managers throughout today's companies are feeling squeezed from all sides while being given fewer resources. Staying competitive and profitable means minimizing losses and maximizing resources wherever possible. Seeking ways to increase security protection, improve operational efficiencies and reduce costs can be a strategic formula for success. More and more companies are looking for new processes and technologies to help accomplish the following:

- // Improve customer service and satisfaction
- // Better protect employees and visitors
- // Reduce insurance liability
- // Support compliance with AHJ (Authority Having Jurisdiction) requirements and government security regulations (i.e., CFATS)

- // Control internal and external theft
- // Protect sensitive proprietary business information and intellectual property
- // Secure highly sensitive areas and data storage
- // Fulfil client contractual obligations for security
- // Comply with governmental regulations
- // Reduce noncompliance and develop employee best practices

While every company has its own unique set of issues and challenges, newer technologies are helping to bridge the gap between needs and resource allocation. Managed video services are one way to help your company better protect its people, property and profits.

Improving services and technologies

Many companies already have installed video security surveillance systems and are looking for ways of leveraging those investments. One cost-effective way may be to add managed video services which can help make legacy systems become even more productive. With managed video services, the end result can be a significantly upgraded video system, with an array of enhanced features, for little or no capital investment.

Market demand for remote viewing capabilities has pushed video technology to new levels and opened up new applications. Innovative software solutions, recording technologies, cameras and recording equipment and other new hardware and services have played a major role in video's advancement. The latest video solutions feature advanced technologies for capturing, transmitting, storing and analyzing video data.

Cameras are smaller, more reliable and offer higher picture resolution. There are new, more efficient, computer-based options for recording and storage. The most important of these technological breakthroughs is the digital revolution. Today, companies can also leverage existing investments by using digital encoders to convert analogue cameras to Internet Protocol-based (IP) cameras.

Video from legacy analogue cameras can be run through a converter to create a digital signal. IP-based cameras can be added or moved anywhere on a corporate network with about the same effort as hooking up a new printer. This can allow for greater ease of ownership and more flexibility. Recording on the "edge" of the system is now possible with microprocessors so small and powerful that they are installed directly in cameras. Recording and storing video at the camera can make the overall network more efficient by allowing transmission of video footage over a network at nonpeak times, which in turn can lessen the impact on corporate bandwidth.

Data transmission technologies are also evolving. Wireless mesh networks have eliminated the need for expensive trenching for cables to connect cameras. Wireless cameras can now be placed in locations that only a few years ago would have been impossible or too costly to consider. Video transmission has always required high bandwidth connections. Higher bandwidth networks are now readily available and are becoming much less expensive every year, opening up new applications for video surveillance.

These advancements make possible the surveillance of remote substations, treatment facilities, construction sites and many other locations.

Better security and cost savings with video services

Video services are defined as any service added onto an existing video surveillance system in order to use it for more than its original purposes. Managed video services use interactive video, and sometimes audio, to interact with a customer's facility, staff and customers. This can be done 24/7 and often in real time. Many of these services can be outsourced to a service provider that creates and then maintains the infrastructure – cameras, servers, software and other equipment – to supply a wide range of service options for a customer.

Video verification – This service provides a cost-effective alternative to on-site security guard services and allows service provider operators to remotely verify intrusion alarms. Specifically, the operators view video images from cameras installed at the customer's site to determine why an alarm was activated. The video feed provides visual evidence for the operators to determine whether the alarm is false or if there is a security event taking place. If the operators see anything suspicious, they then follow pre-determined protocols. For example, they might be directed to notify a customer contact and/or local law enforcement.

Holdup alarm systems can also be tied into the video alarm verification systems so that when a holdup alarm is activated, video images from the site can be viewed by remote operators and local law enforcement can be dispatched.

This service can be invaluable in helping to reduce false alarms and associated fines and in helping reduce police response time. Currently, a number of municipalities require, or will be requir-



ing, verification of alarm events before they dispatch police personnel. In the case of a true emergency, remote video verification can help assure valuable response in a timely manner. Where no emergency exists, remote video verification can reduce false alarms, the expense of fines and help relieve the burden on limited municipal resources.

Video verification has many applications, including petrochemical facilities that must comply with CFATS regulations, banks, retail stores, real estate management companies with numerous tenants, universities and K-12 schools, mass transit systems, warehousing and manufacturing facilities.

Video guard tour – Operating similarly to a physical security guard tour, remote video guard tours use video cameras and remote operators to "tour" the premises at pre-determined intervals. Specifically, operators use cameras installed at a customer's site to perform these security checks at set times. In contrast to video verification, video guard tours are performed proactively rather than as a response to an alarm event.

By way of example, an operator can be instructed to look for specific conditions in specific locations, such as an unlocked gate or open door. When an operator sees something suspicious, a notification is made. These notifications can be directed to a company's security staff or designated contacts, to a security guard service or directly to law enforcement, depending on the severity of the situation and/or pre-established protocols.

As with some other managed video services, customers have the option of adding audio to video guard tours. With the audio component, remote operators can help alert on-site employees, customers and visitors that the site is being remotely monitored and that their actions are being observed by a remote guard.

Remote video guard tours can offer many benefits, including enabling a company to potentially reduce security guard staffing; redeploy existing security resources more effectively; increase levels of security during off-business hours; monitor remote facilities more efficiently; increase compliance with governmental mandates, such as CFATS; comply with governmental contractor requirements, such as UL 2050; and secure highly sensitive areas within a facility.

A variety of commercial properties, such as retail locations, office buildings, real estate companies, banking and financial institutions, warehouses, mass transit systems, petrochemical facilities, utility properties, and K-12 and university campuses could add remote guard tours to enhance their current security solutions. This concept is sometimes referred to as security-in-depth and offers an additional layer of protection that can provide a more comprehensive approach to premises security.

Video assist – A service enhancement to traditional holdup systems, video assist helps provide employees with a distress alert system for use in emergency situations. Many times, an employee is working alone or may be concerned

about becoming involved in a suspicious or potentially dangerous situation. If an employee becomes concerned about a situation, he or she can press a hidden panic button which activates nearby video cameras to immediately begin recording the scene. The engagement of the button also triggers an alarm at the remote monitoring station where an operator begins viewing the situation via the video camera feed. The operator can then determine whether law enforcement should be notified. Some video assist systems also have an available audio component. This two-way audio connection can be helpful in specific situations where the protocol is to let a suspicious person know he or she is being monitored. In this case, a remote operator can speak to the on-site employee and also alert the suspicious person that the area is being monitored. Once given feedback from the employee, the remote operator can then take appropriate action.

Video assist can be particularly beneficial for convenience stores, gas stations and other retail facilities that are open overnight, have frequent loitering issues or are often staffed by one employee. It can help improve employee safety, reduce insurance liability premiums and reduce shoplifting. It could also be used as a recruitment tool for hiring employees to staff late-night and overnight shifts.

Video escort – This service allows an operator at a central monitoring centre to view video images of employees entering and exiting sensitive areas within a facility. When contacted from an employee's cell phone, the operator can view a location using a video camera feed to virtually "escort" the person between the parking lot and the facility.

Video escort service can help increase employee safety, reduce security guard staffing and increase employee peace of mind. The service is particularly well-suited for organisations such as jewellery stores, banks, check cashing facilities, corporate offices and high-risk business-

es that have a potential risk for employees being watched and forced into the facility. Video escort could also be used as an employee recruitment and retention tool.

Unattended delivery – Any company that receives deliveries during peak selling hours or wants to receive deliveries during off-business hours knows how challenging and time consuming it can be. The security risks of receiving deliveries during off-business hours can be more challenging. However, even receiving deliveries during peak times can significantly undercut revenue potential. During peak hours, sales personnel should be on the main floor, helping customers rather than having their attention diverted to receive deliveries. Unattended delivery is a smart operational choice that could directly impact a company's bottom line. Unattended delivery allows delivery truck drivers, vending company employees, even maintenance workers to enter a facility and deliver merchandise, supplies or perform their services without a facility employee or security guard being present.

Upon arrival, a driver disarms select portions of a special alarm panel outside the facility using a unique code that indicates the driver is ready to make the delivery. A remote service provider operator views live video images of the site, remotely unlocks the door and continues to observe the driver throughout the delivery process. If the operator observes suspicious activity, the operator can make an audio connection to the facility speaker system that informs the driver that he is being monitored.

A customer may also choose to have the operator view video only when a driver generates an alarm by moving outside of specifically designated delivery areas. This type of exception unattended delivery system means that during a normal delivery (when the driver remains within designated areas), no alarms would be generated.

The advantages of unattended delivery can include reducing overtime for security guards and/or store employees, allowing store managers to manage staff instead of supervising deliveries and lowering costs by optimising the efficiency of delivery routes. In addition, receiving new merchandise in an overnight delivery could help a company increase sales by having the new merchandise available for purchase at the start of the next business day.

Applications for unattended delivery include retail stores, wholesale facilities and businesses that operate around the clock.

Outsourcing: A cost-effective way to add managed video services

In tandem with physical security technological advancements, the capability of remotely managing video services has contributed to the overall success of these systems. In fact, a leading professional consulting group recently surveyed many of the nation's top chief executive officers – 70 per cent of whom said they had or were planning to outsource an important business function within the past or coming 12 months. It is clear that outsourcing is gaining momentum.

Within the security industry it makes economic and operational sense for companies to outsource managed video services.

Some benefits of outsourcing video services:

- // Preserve capital
- // Reduced impact on security budgets
- // Offload responsibility for maintenance, upgrades and operations for a managed video solution
- // Reduce false alarms and improve police response time

// Provide access to enterprise-grade security solutions for smaller organisations

// Allow better scalability for larger organisations

// Provide more comprehensive security system reporting

Outsourcing the video management portion of a video surveillance solution can help save considerable amounts of a security capital investment budget by helping to eliminate major capital investments for equipment and software. In addition, a managed video services



solution can help eliminate the need to increase the internal security staff. The service provider can install all necessary components, including additional cameras (if needed), switches, network connections and other devices. Many times, if contracted, recording servers can be stored, maintained and administered by the service provider off-site at its central monitoring centre. The solution provider's system should be fully reportable, as well as providing the ability for the customer to receive customised reports as events occur at pre-determined intervals – daily, weekly or monthly.

Managed video services can be a cost-effective option for small to mid-sized organisations that lack larger security budgets. These organisations can augment their in-house technical staff and extend their security coverage for a fraction of the cost to deploy their own security departments.

Larger organisations can also benefit from managed video services by using the scalability of a service provider and its ability to extend managed video to remote or geographically dispersed locations.

This can help provide a more consistent and comprehensive corporate security plan. Even those with legacy video surveillance systems can take advantage of managed video services.

Most importantly, managed video services can enhance the video security solutions companies have deployed already and increase the return on investment for the video system. A service provider can integrate the systems and provide all the add-on software needed to interconnect the systems. When necessary, a service provider can also install additional cameras and other hardware.

Managed video services and IT impact

When a reliable security service provider is used, managed video systems can be integrated smoothly with other security technologies.

Information Technology (IT) department personnel will often be involved in the selection and/or deployment processes. There are many questions and considerations IT might have, including requirements, infrastructure, connectivity and network design and security.

The first IT consideration will probably be how the video images will be transmitted to the service provider. In some cases, a stand-alone network is the better option and, in other situations, the transfer of video images might be accomplished through the overall corporate or security networks. Either solution is possible, depending on how many cameras are being added and whether a stand-alone network has scalability.

As a solution expands, it may become more difficult to integrate the two networks at a later date. Many organisations are finding that a shared infrastructure is the most cost-effective solution for the long term.

Next, the IT team are likely to have questions about connectivity – in other words, the equipment that will be used to connect the corporate facilities with the service provider's central monitoring station. For example, an IT department with a Cisco-based network will want to select a provider that understands Cisco configurations and can work with Cisco equipment. Also, the IT department may want to know if managed video services will require connectivity back to the provider for delivery of any services, updates and remote support.

If so, IT may want to be involved with exploring connectivity options and any potential security risks that could expose their entire enterprise network.

In addition, IT departments may have preferred computer vendors and may require a specific class of equipment be used. They may specify a network to be built with redundancy and high availability to ensure that their portion of the project will meet the service levels required of the project.

Security is often the most important consideration for the IT department, as a network security breach could take down the company's entire network. IT professionals have to ensure that nothing exposes the networks to these risks. This takes a methodical and proactive approach, and IT professionals are noted for testing and being careful before deployment. It will be extremely important that a service provider knows how to work with IT and is comfortable speaking its language and answering its needs.

Choosing a managed video services provider

When a company makes the decision to outsource one or more managed video services, a critical step is choosing the best service provider. With managed video services, the emphasis is on "service," and not all providers are created equal. Some might only have a few service options and limited scalability, which might be fine for a smaller organisation. However, a large organisation may require a multitude of services for its different locations, and may need to have the flexibility to scale a system as needed.

Let's take a closer look at some of the areas that should be addressed.

Monitoring centre – Some providers may lease or share a monitoring centre with other providers. These types of providers typically offer pre-packaged, off-the-shelf managed video services. This scenario can open up issues, such as quality control, lack of monitoring centre redundancy and priority hierarchies for emergency situations. That's why it's critically important to understand whether a potential service provider operates its own facilities.

Trained staff – Managed video services require highly trained operators to be effective. A service provider needs to offer documentation of the level of training it provides its operators and system designers. In highly specialised industries, a service provider should have the capability to offer a dedicated team able to provide the degree of services required for the vertical application.

IT speak – When it comes to hanging something new on the corporate network, nothing calms an IT member of staff more than dealing with profession-

als who can speak its language. Early in the relationship, service provider professionals need to establish immediate credibility with IT staff members. The provider should be able to supply documentation and examples of deployments they have completed as well as a solid understanding of IT concerns. A good service provider has a team that can anticipate potential questions IT will ask and then be prepared to answer any and all of those questions. Due to the highly technical nature of IT networks and infrastructures, it is also very important to ask whether a potential provider has network certification from industry vendors, such as Cisco and Microsoft.

Often the vendor can be the critical link between physical security and IT staff. In a large organisation, it is not unusual for these two groups to be isolated from one another and to not clearly understand each other's objectives, priorities and mandates. A good service provider has professionals trained in both areas and can work through issues for both sides.

A trusted security advisor

Tyco Integrated Fire & Security has an international footprint with offices in 12 countries in Continental Europe. With approximately 4,000 employees, 300,000 customers and five monitoring centres, we are proud to be recognised by our customers as the quality leader and preferred partner for integrated fire and security solutions. Our certified technicians develop and install managed video solutions that match your specific security requirements.

For further information please contact: ce.communications@tycoint.com or visit our website: www.tyco.eu