VIDEO SURVEILLANCE: THE FIRST STEP TO PHYSICAL SECURITY

Red River
There has been a great deal of recent focus on hardening IT infrastructure against digital threats, but fortifying physical plant and facility security is equally important. In fact, you can’t have one without the other. To get a sense of the wide ranging solutions that are increasingly put in place, look at the various classes of physical security, which include:

- **Intrusion Detection:** These systems detect and protect perimeters and buildings from unwanted intrusions, often relying on integrated IP-network-based facility-protection solutions, such as auto-lockdown and the arming of advanced protection systems and automated alerting of personnel response.

- **Physical Access Control:** This approach enables IP-based access control and remote lock-down to meet and exceed HSPD-12 and other regulatory compliance mandates.

- **Physical Security Information Management:** This approach integrates and analyzes data from disparate physical security devices and systems, while automating operations center management.

- **Environmental Controls:** These controls protect systems, buildings and support infrastructure from external and environmental threats.
• **Video Surveillance:** Video data, which can be subjected to sophisticated analytics, can improve security very economically. Because video surveillance is often an obvious and first step to take when tightening physical security, it is the focus of this eBook. We will examine the phases of implementing a video surveillance system, the infrastructure for which can readily enable other forms of security, to say nothing about how it can bring a security focus to your entire organization.

Why start with video? As threats have increased, and criminals have become more sophisticated, the ability to counter them using video surveillance has also grown in sophistication. Today, dramatic leaps in video surveillance capabilities have been driven by advanced HD cameras, facial and voice recognition software, advanced analytics and anomaly detection, and even the ability to link the physical structure through an internet of things network, so that first responders can be messaged and the building itself can automatically respond to threats detected by even low-cost video cameras. For those looking to fortify physical plants and facilities, video is clearly the place to start.
The first step to a video surveillance upgrade starts with the cameras.

The most advanced cameras available today, which can enable facial recognition and license-plate capture, offer crisp images, even in close zoom. The bottom tier high-definition camera is a 1-megapixel camera, but 3-megapixel cameras are required for the more sophisticated analytics. (As we later examine storage requirements, note that a single 3-megapixel camera will generate 31 gigabytes of data every 24 hours.)

Beyond upgrading to a 3-megapixel camera, there are less ambitious, less costly steps to take that can lead to equally secure facilities. One approach is to use lower-cost analog video cameras coupled with an IT encoder. An IT encoder will make the analog cameras “available” to a IT network, and the data from the cameras can be subjected to analytics, even with relatively low resolution.

What’s the cost of cameras and the cables to connect them? Here’s an index figure for “back of the envelope” calculations: Budget $1,500/camera and the cables to connect it to a network.
Chapter 2: Network Infrastructure and Expanded Bandwidth.

When a video camera captures image data from a location, the data must be stored, and there are two ways to do it.

Either approach – on-premises storage or off-premises storage – will affect the network that will be required to support use of video surveillance data. Key factors in the “decision tree” used to specify a video surveillance network are:

A) Whether the video data will be stored on-premises storage or off-premises;
B) Whether the video will be watched in real time, or stored and examined only when there is a security issue;
C) Whether the video data will be watched on-premises or off-premises.

So, let’s look at the network requirements. To stream high definition video for real-time off-premises viewing, a sophisticated, high-speed fiber network is required. Off-premises use of the video data – even data generated by the lowest level of image definition video – can require a fiber network capable of managing tens of gigabytes of data per camera for every 24 hours. If that much video data is to be moved over existing networks, and those networks are supporting other devices and business functions,
be mindful that up to 90% or more of the network’s capacity can easily be consumed by video data, grabbing the network bandwidth that is otherwise required for other business operations. Indeed, an independent network just for the video data may be called for. On-premises storage of video data can negate the need for a high-bandwidth network, since the data is simply stored at or near the point of capture. For the most economical approach, on-premises storage of video data is the path to take.
A security system that used six 2-megapixel cameras, capturing 30 frames per second, 24 hours a day, would generate 11 terabytes of data. How long the data is kept will dictate the number of terabytes required for storage, either on-premises storage or off-premises. How long do agencies and companies keep their video data before overwriting it? Data storage varies widely from 7 days to forever, depending on the security level of the site. No matter how long it is kept, even the typical minimum of 7 days, a week’s worth of data would require a storage allotment of 77 terabytes, and a month’s worth of data would require over 340 terabytes of storage. This is equally true for on-premises or off-premises storage. Clearly the one advantage of on-premises storage is that there is no need for a network to move 340 terabytes of data every 30 days. For on-premises storage or off-premises, analytics can be brought to bear with equal ease.
The near-term future of video analytics is right out of science fiction.

Facial recognition is right around the corner (it will require a minimum 3-megapixel camera), but practically speaking, for most agencies and companies, the application of facial recognition will be applications that match faces of people coming through an entryway with an existing database of faces, to detect the unauthorized intrusion of a stranger. Broader facial recognition of criminal faces in a crowd is still very much the work of national security agencies and Hollywood movie directors.

Whether video data is analyzed in real time within the camera’s software (which can have built-in analytics) or from streaming video, or through the examination of video shot retrieved for analysis, the practical application of analytics focuses on pattern disruption, image anomalies, and unauthorized movement. For instance, a common analysis detects movement from left to right, right left, down to up, and up to down, as when a person walks from the right side to the left side of the camera’s view, when motion is only authorized from left to right…perhaps indicating that someone has entered in an exit door,
or a patient has departed a hospital room. Also, image anomalies can detect when a bag has been left unattended. Pattern disruption can indicate when, perhaps, a trash bin has been tampered with and put back slightly in the wrong place or at the wrong angle. In addition to detecting camera sabotage, analytic software can also digitally “snap” a perimeter line on a screen and detect when it has been breached.

The analytic software can then trigger automated responses, like texts or phone calls to responders, or the camera can even trigger automatic building lockdowns through locks that have IP addresses.
Benefits

Are the costs worth the benefits for video surveillance? Consider that value of the property at risk. Consider the cost of disaster recovery of a security breach. Consider the liability of your enterprise for a space that is unprotected. A one-time $10,000 investment in the cameras, network upgrades and storage to protect a $10 million server farm is a small price to pay, to say nothing of the security offered to employees, which is by any estimation, priceless.

About Red River

Red River is an IT hardware integrator committed to helping customers optimize business processes and maximize the value of IT investments. Widely regarded for our special focus on the U.S. government, Red River has developed a remarkable reputation for delivering IT products and hardware-related services to military and civilian agencies and the companies that serve them. Our core values of hard work and honesty fuel our central mission to make IT personal.

Learn more at www.redriver.com.