

## **Emerging Video Surveillance Guide 2010**

*What to Look for and what to Look Out for*

This report examines the benefits and risks of emerging video surveillance technologies for security managers and integrators. Special emphasis is placed on identifying the risks. They are regularly ignored yet critical to success of deploying emerging technologies.

### **Manufacturers Generally Assume Maturity**

Manufacturer marketing generally assumes the emerging technology is already mature - thus focusing on all the potential benefits and little of the technological and operational risk involved. Whether this is driven by hope, ignore or malice is debatable. What is clear is that this assumption is dangerous for security managers and integrators.

### **Risks are Rarely Disclosed**

The burden is regularly placed on end users and integrators to determine risks, which is inefficient and of questionable ethics.

Such risks generally falls in 3 types:

- Technological risk: that is, the product simply does not work at a basic level. For instance, video analytics faces far higher technology risk than IP cameras.
- Usability/Integration risk: that is, the product has issues working with existing

---

systems or processes of an organization. For example, many end users have video recorders that do not support IP cameras.

- Cost: Generally the most obvious of the risks, manufacturers often downplay the costs involved and use best case scenarios in their cost comparisons.

## **Emerging Technologies**

This directory examines ten emerging technologies. We define emerging technologies as those that are deployed by less than 20% of security users. The risks involved vary significantly amongst these technologies.

- IP Cameras
- Megapixel Cameras
- IP Based Storage (NAS/SAN)
- Storage On-Board IP Cameras
- Mesh Wireless Networks
- Panoramic Cameras
- Video Analytics
- Business Intelligence
- Remote Video Monitoring
- Managed Video / Hosted Video Surveillance
- Physical Security Information Management

This directory is meant as a survey of key risks for the non-expert. Inside the directory, 19 other IP Video Market reports are referenced for further information and analysis on these technologies.

## **IP Cameras (Standard Definition)**

Potential Benefits: The most important advantage of using IP cameras is the ability to directly connect these cameras to an IP or computer network. By contrast, analog cameras require the use of an additional computer (usually either an encoder or DVR). In certain

---

scenarios, using IP networks can significantly reduce the cost of installation. In general, the greater the distance that video needs to be transmitted, the more likely IP cameras will be beneficial.

Remote viewing of video, though generally marketed as a benefit of IP cameras, is really not an advantage compared to today's DVRs. Whether one uses analog cameras and DVRs or IP cameras, video can still be viewed remotely with only minor technical differences.

Cost: IP cameras usually cost 30%-70% more than equivalent analog cameras. These costs are often more than off-set in larger scale systems or when cameras must stream video over great distances.

- End-User Risks: While the technology is fairly mature, the main risk lies in operational/integration issues. Risk #1 is that existing recorders do not support IP cameras or only supports a very limited number of IP cameras. Risk #2 is that the existing IP network in one's facility is insufficient to handle the IP cameras (though this risk is rather easy to overcome in most situations). For details on addressing these risks, read our guide in [migrating from analog to IP](#).
- Integrator Risks: Lack of technical skills on an integrator's existing staff is the strongest risk to deploying IP cameras. With traditional electronic security systems, an integrator may find it sufficient to have only 1 or 2 highly trained IT technicians (out of a group of 10 - 30). However, with IP cameras, a far greater percentage will require IT skills to conduct basic installation/service activities.

Learn more: [IP Camera Advantages and Disadvantages](#), [Top 5 IP Camera Problems](#) and [How to Migrate from Analog to IP Cameras](#)

## **Megapixel Cameras**

Potential Benefits: The two most fundamental benefits are (1) reducing the number of cameras deployed and (2) increasing the quality of the video, leading to greater

---

identifications of suspects/incidents. Both benefits derive from the significantly higher resolution of megapixel cameras (compared to all analog cameras and standard definition IP cameras.)

Beyond the increased resolution, as megapixel is a subset of IP cameras, the benefits and risks of megapixel cameras inherits those from IP cameras.

- **End-User Risks:** The two biggest risks are (1) overhyped claims to increased video quality and (2) storage utilization. Often vendors will claim that megapixel cameras provide 4, 16 or even 81 times greater resolution. While this is 'technically' correct when comparing specified pixel count, this is generally not achievable because of 3 practical factors. (1) Multiple cameras can be placed in different locations while the megapixel camera's greater resolution only covers a single area (since it's a single physical camera). Often, this is 'overkill' for a given area. (2) Looking at pixel counts (e.g., 0.3MP for standard definition vs. 5MP) is fundamentally misleading. Most megapixel cameras provide only modest increases in visible quality - especially over 1MP. (3) In low light conditions, the effective visible resolution drops dramatically - to the point where a megapixel image usually provides no greater visible details than a standard definition camera. Additionally, megapixel cameras generally require significantly more storage. At some level, this is simply a matter of paying the additional cost of storage. However, the additional storage needed may be so great that a dedicated storage cluster may need to be used (see IP Based Storage below).
- **Integrator Risks:** Over-selling the quality of megapixel cameras is the most significant risk. It is likely that the sale of megapixel cameras will be based on either reducing the total number of cameras or one capturing specific details (e.g., people's face or car's license plates). Integrators should be careful about testing actual camera performance including low light abilities, as applicable.

Learn more: [Do Megapixel Cameras Provide Better Image Quality, How Well do IP Cameras Work in Low Light?](#) and [How to Win Deals with Megapixel Cameras?](#)

---

## **IP Based Storage (SAN)**

Potential Benefits: Traditional video surveillance deployments combine video management software and hard drives inside a single appliance (usually a DVR). In larger systems, this can result in hundreds of hard drives inside of dozens of DVRs. This can be difficult to manage, inefficient and difficult to upgrade. Also, DVRs often do not provide redundancy for storage.

IP Based Storage provides centralized storage clusters that offer built-in redundancy and simple expansion. Each video recorder transmits surveillance video from the recorder to the storage cluster. This also reduces wasted storage as all video is 'pooled' in a central repository.

Cost: For larger systems (20 TBs or more), IP Based storage is often cheaper than storage inside of DVRs. However, the startup costs for purchasing a SAN often make it significantly more expensive simply adding an extra hard drive inside a DVR. For instance, SANs usually start at \$5,000 USD, far more than the incremental cost of adding a few hard drives inside DVRs or NVRs.

- End-User Risks: Overall risk is quite low. Some DVRs do not support external storage (usually as a business policy rather than a technical restriction) so that should be checked. Using a SAN that is remote from IP cameras or existing DVRs (essentially the source of the video streams) can be a problem. Specifically, it is generally not feasible to use a SAN to store video from remote offices/branches. This is due to limited and costly bandwidth connecting facilities (WAN bandwidth).
- Integrator Risks: Setting up a SAN (depending on the vendor) can be significantly more complicated than storage on-board DVRs. At least 1 person on staff should be trained in installing and maintaining the SAN.

Learn more: [Examining Video Surveillance Storage Clusters](#) (IP SANs) and [How Much Storage is Needed for Video Surveillance](#)

---

## **Storage On-Board IP Cameras**

Potential Benefits: Some camera locations have limited or unreliable bandwidth. In those locations, ensuring that video can be streamed and recorded remotely can be expensive (or simply not possible). Putting storage inside of an IP camera can eliminate this problem. Of course, some network connection will be needed to remotely view/download record video. However, this will only need to be done periodically.

Cost: While storage costs drops continuously, today the cost of on-board storage is far higher than centrally storing video in hard drives. Moreover, for most video surveillance applications, it is simply not possible to solely store video on-board IP cameras as it is not technically possible (with the exception of 2 vendors supporting hard drives inside or attached to their cameras).

- End-User Risks: Using on-board storage may force compromises in the length of storage or the quality of storage (because of limitations on how much video can be stored inside the camera). Additionally, most VMS systems do not support remote playback of video recorded on an IP camera. This could make it difficult to access and use this video.
- Integrator Risks: If the on-board storage cannot be remotely accessed using the existing VMS playback, the integrator may be called for additional service calls. Some systems will require a technician physically remove the on-board storage while others will require downloading raw video files.

Learn more: [Should You Use Cameras with Built-In Storage?](#) and [SD Card's Future for Video Surveillance Storage](#)

## **Mesh Wireless Networks**

Potential Benefits: Video surveillance is often wanted in areas that are remote from buildings, such as in parking lots and along fencelines. Running network cabling can be

---

cost prohibitive requiring expensive and disruptive trenching.

IP wireless systems offer a wire free alternative to transmit video in those area. Mesh wireless systems (a specialized form of IP wireless) allow video to be transmitted across longer distances and around areas of interference (like hills, trees, etc.).

Costs: Compared to long distance cable runs, mesh wireless is generally significantly less expensive. Even at about \$2,000 USD per wireless node, wireless is far less expensive than almost any form of trenching across roads or pavement.

- **End-User Risks:** Because of the bandwidth demanded, deploying wireless systems for video surveillance require specialized expertise. If end users do not choose experienced integrators, significant delays may occur. Additionally, risks exist in the long term performance of the system (as environmental or local changes can degrade performance). It is imperative that customers budget for long term maintenance of the system or major service issues could occur.
- **Integrator Risks:** Deploying wireless video surveillance networks may be the single most difficult technical task in all of video surveillance (even harder than video analytics). Wireless demands technical expertise in both IP networks and wireless systems. Furthermore, wireless systems can be impacted by external factors such as the weather and nearby wireless users (because most systems are license free). Two specific risks are: (1) systems that do not deliver as much bandwidth as the integrator plans and requires and (2) ongoing stability problems with the system that demand expensive service calls.

Learn more: [Wireless Video Surveillance Tutorial](#) and [Why Wireless Video Surveillance Systems Fail](#)

## **Panoramic Cameras**

Potential Benefits: To cover wide areas often requires 3 or 4 cameras, simply because traditional security cameras can only cover a small zone or portion of a facility (due to

---

lens and resolution restrictions).

Panoramic cameras generally combine megapixel resolution and super wide angle lenses to provide 360 degree coverage from a single physical camera.

Cost: While a single panoramic camera costs more than a single fixed traditional camera (often 2 -3 times more), the savings from replacing multiple traditional cameras usually justifies the additional cost.

- End-User Risks: The two key risks are (1) actual quality achieved and (2) integrating with one's existing system. Because these cameras cover such a large area, the resolution of the camera is spread thin. As such, the effective video quality of these cameras are often lower than a traditional fixed camera with a standard wide angle lens. Users should be aware of this and test the camera in the areas desired prior to install to verify that actual resolution is sufficient. Secondly, panoramic cameras are not supported by most VMS systems and there is no interoperability between different vendors of panoramic cameras/lenses. To use these cameras may force the use of a proprietary or (at least) limited set of VMS systems.
- Integrator Risks: Expectation management is the biggest risk. If integrators do not set realistic expectations on achieved video quality, end users could complain or reject the install.

Learn more: [Are Panoramic Cameras the Most Significant Advance in CCTV History?](#)

## **Video Analytics**

Potential Benefits: Video analytics may offer the greatest long term benefit for video surveillance.

By identifying suspects in real time, video analytics can help stop crimes in progress. This can be accomplished through a variety of forms of detection including alarming on people in restricted areas, crossing fencelines or loitering for an extended period of time.

---

By cataloging events over a period of time, video analytics can help solve investigations and provide information on trends. For instance, searching through large periods of video can be improved by returning only video where people are present.

Costs: The direct cost of adding video analytic software is moderately expensive today. The per camera premium is no usually no more than \$500 USD per camera (end user pricing) and often only about \$200 USD. The costs to optimize the software and modify the positions of cameras can be significantly more expensive.

- End-User Risks: The biggest risk to end users is that the video analytics system is abandoned or otherwise infrequently used because of performance limitations. Specifically, end users may find that adjustments that need to be made to camera positioning or lighting may be financially or logistically infeasible. Furthermore, end users must determine what level of false alerts they will receive and whether or not they can manage them.
- Integrator Risks: Video analytics that fail to meet customer expectations can make projects unprofitable and undermine customer relationships. Integrators should be very careful in testing video analytics and setting appropriate expectations with end users.

Learn more: [Top 3 Problems of Video Analytics](#), [How to Select Video Analytics](#) and [theState of Video Analytics 2009](#)

## **Remote Video Monitoring**

Potential Benefits: Almost all surveillance video is not monitored live on-site (major exceptions include larger retailers and casinos). For most organizations, it is hard to financially justify operators to watch surveillance video continuously (and those that do often have 1 operator watching hundreds of cameras).

Remote video monitoring is a service that allows a third party to watch your surveillance

---

video. Because the third party monitors a large number of customers, they can offer lower costs than if you did it yourself. The 'holy grail' of remote video monitoring is to use video analytics to identify the most likely threats, increasing the effectiveness of the monitoring.

Cost: While the cost depends on the type and frequency of monitoring, the cost is almost always far less than staffing one's own guards. As such, high cost is rarely a barrier to the use of remote video monitoring.

- End-User Risks: The three main risks are (1) the effectiveness of the video analytics used and (2) the remote monitor's support of an organization's existing video surveillance system and (3) information security risks of allowing remote access. The first risk, on video analytics, has been addressed in the preceding section. The second risk is a key practical issue. Quite simply, most remote monitoring system do not work with an organization's existing recorders/cameras. This generally requires the purchase of additional products and, in some cases, replacing existing systems. Finally, customers usually provide VPN access to their internal network for the remote monitors or establish a secondary network (like a dedicated cable modem/DSL line). The first can be against IT policy while the second could add a significant monthly fee (especially if this is to be done across multiple distributed locations).
- Integrator Risks: Outside of the general risk of video analytics, the technical risk of remote monitoring tend to be low.

### **Managed Video / Hosted Video Surveillance**

Potential Benefits: Managed and hosted video can reduce the cost and complexity of deploying video surveillance systems by eliminating most of the on-site setup. Hosted video, by definition, also eliminates the deployment of a video recorder on-site (sending the video directly from the camera to the hosted video service).

Costs: Many hosted video providers charge \$20 USD - \$30 USD per month. For more than a few cameras per site, the effective cost over a 3 year period can be significantly higher than purchasing a DVR/recorder.

- 
- **End-User Risks:** The technical risks tend to be low (as this is more of a new business model than a radical new technology). From an operational perspective, managed/hosted video providers generally offer very basic functionalities (e.g. most do they offer analytics or 3rd party integration). The risk here would be losing functionalities that may be important for one's operation. From a policy/procedure viewpoint, larger organizations may be concerned about the security risk of outsiders being able to watch one's live or recorded video.
  - **Integrator Risks:** The business risks is the most critical concern. While these services can provide attractive recurring revenue, the simplicity designed into these services reduces the value and need for security integrators. Indeed, it is likely that the most successful managed/hosted video providers will cut out the security systems integrator as a unnecessary middleman.

Learn more: [Value of Managed Video](#), [Top 5 Managed Video Surveillance Problems](#) and [Axis Hosted Video Test Results](#)

## **Physical Security Information Management**

**Potential Benefits:** Large organizations often use multiple security systems (e.g., access control, intrusion detection, CCTV, etc.). Additionally, many organizations use multiple vendors for some security systems (for examples, DVRs from Pelco and Dedicated Micros). The ability to integrate these various products into a single integrated whole is difficult.

Furthermore, individual security systems are often not optimized for overall security response (e.g., coordinating responders, tracking suspects, logging actions, etc.)

PSIM systems are designed to rectify both of these problems. PSIM is a software system that integrates various security systems, providing a unified front end to coordinate responses. **Cost Comparison:** PSIM systems generally cost hundreds of thousands of dollar, far more expensive than the less powerful but often sufficient alternative of

---

integration using one's access control system.

- **End-User Risks:** End users should be careful that the PSIM system fully supports their existing security systems. They also should carefully evaluate any deficiencies of using the PSIM system relative to use existing individual systems directly. This problem arises because PSIM vendors often do not support advance functions of individual security systems. For instance, PSIM systems generally support searching video by time but often do not support searching by motion or advanced analytics.
- **Integrator Risks:** Implementing and managing PSIM systems can be very time consuming and pose a risk of long-term management issues. Not only are PSIM systems not 'plug and play', many security systems may not be supported. Furthermore, support for systems may break in the future. These elements place integrator at risk for cost overruns and extended support calls.

Learn more: [PSIM Problems](#)