

# IPVideoMarket.info

## Video Surveillance Guide

Version 4.0 / March 2010

John Honovich

[IPVideoMarket.Info](http://IPVideoMarket.Info)



## Contents

Chapter 1: <a href="#">How to Design Video Surveillance Solutions</a> .....	7
Chapter 2: <a href="#">Introduction to NVRs / IP Video Software</a> .....	18
Chapter 3: <a href="#">Bandwidth Basics for Video Surveillance</a> .....	23
Chapter 4: <a href="#">Examining Video Analytics</a> .....	28
Chapter 5: <a href="#">Wireless Video Surveillance Tutorial</a> .....	32
Chapter 6: <a href="#">API and System Integration Tutorial</a> .....	36
Chapter 7: <a href="#">How to Integrate Video With Other Systems</a> .....	40
Chapter 8: <a href="#">Should I Use IP Cameras?</a> .....	44
Chapter 9: <a href="#">Value of Hybrid DVRs/NVRs</a> .....	50
Chapter 10: <a href="#">Examining 'Open' Systems</a> .....	54
Chapter 11: <a href="#">The Danger of Buying Packages</a> .....	57
Chapter 12: <a href="#">How to Read Marketing Material</a> .....	60
Chapter 13: <a href="#">How to Evaluate New Technology</a> .....	64
Chapter 14: <a href="#">How to Calculate Video Surveillance ROIs</a> .....	71

# Be a Video Surveillance Expert

IP Video Market's "[Video Surveillance Professional Service](#)" offers the world's leading resource for video surveillance information. With over 900 total posts and at least 10 new reports each month, subscribers have access to:

- Product Test Results
- Company Competitive Analysis
- Market and Technology Trends
- Best Practices on Using Video Surveillance

[Subscribers can access all of these reports for as low as \\$99 USD.](#)

The [Video Surveillance Professional Service](#) has gained over 100 subscribers in its first year, becoming the most important reference for video surveillance users, integrators, manufacturers and investors.

## About the Author

John Honovich is the founder of [IP Video Market Info](#), the leading website dedicated to video surveillance. John researches and writes extensively for IP Video Market Info, providing ongoing and timely analysis of new technologies and emerging products. Additionally, John developed software that allows IP Video Market Info to constantly track and organize new video surveillance information from company websites and across the web.

Prior to founding [IP Video Market Info](#), John was a successful manager and engineer working closely with Security Managers to develop video surveillance solutions. As Director of Product Management for [3VR Security](#), John helped design and deploy industry leading video analytic and facial recognition software for the banking and retail market. As General Manager of [Sensormatic Hawaii](#), John lead large scale military and critical infrastructure deployments of video analytics, IP video and wireless video surveillance. Before entering the Physical Security industry, John was a senior engineer designing IP Video over DSL networks for telecommunication carriers.

John graduated from Dartmouth College and, over the years, has achieved Cisco certifications and the ASIS International Board Certification in Physical Security (PSP).

# Preface

## Who is this Book for?

This book is designed for the security manager who uses video surveillance/CCTV systems. You should be able to understand this book if you have used a DVR system. The book's goal is to help you make better decisions about evaluating and selecting video surveillance systems.

Integrators and manufacturers should also be able to learn from this, especially to gain a better appreciation of drivers for security managers.

## May I Share this Book with Others?

Yes. This is a free and “open source” book. You can share and copy the book as long as you attribute the source (John Honovich, IPVideoMarket.info) and do not restrict other's ability to share the book. This is technically called a “[Creative Commons Attribution-Share Alike 3.0 Unported License](#).” Email me at [jhonovich@ipvideomarket.info](mailto:jhonovich@ipvideomarket.info) with any questions.

## Will this Book be Updated?

Yes, this book will be updated 2 to 3 times per year and is designed to be a living book that reflects ongoing developments in video surveillance. Go to <http://ipvideomarket.info/book> to check for updates.

## May I Suggest Improvements or New Topics for the Book?

Yes, I strongly encourage you to suggest improvements or new topics. Please email me at [jhonovich@ipvideomarket.info](mailto:jhonovich@ipvideomarket.info).

I

# Introduction to Video Surveillance

## ***Chapter 1: How to Design Video Surveillance Solutions***

Designing a video surveillance solution requires decisions on 7 fundamental questions. This tutorial walks the reader through each issue explaining the basic options and the rationale for selecting different options.

This is a survey to help those new to video surveillance. Its goal is to quickly identify the key aspects of video surveillance design, not to examine the many details and edge cases in such designs.

The 7 fundamental questions are:

- What type of cameras should I use?
- How should I connect cameras to video management systems?
- What type of video management system should I use?
- What type of storage should I use?
- What type of video analytics should I use?
- How should I view my surveillance video?
- How should I integrate video with my other systems?

### **1. Cameras**

Cameras are literally the eyes of a video surveillance system. Cameras should be deployed in critical areas to capture relevant video.

The two basic principles of camera deployment are (1) use choke points and (2) cover assets.

Choke points are areas where people or vehicles must pass to enter a certain area. Examples include doorways, hallways and driveways. Placing cameras at choke points is a very cost-effective way to document who entered a facility.

Assets are the specific objects or areas that need security. Examples of assets include physical objects such as safes and merchandise areas as well as areas where important activity occurs such as cash registers, parking spots or lobbies. What is defined as an asset is relative to the needs and priorities of your organization.

Once you determine what areas you want to cover, there are 4 camera characteristics to decide on:

1. **Fixed vs PTZ:** A camera can be fixed to only look at one specific view or it can be movable through the use of panning, tilting and zooming (i.e., moving left and right, up and down, closer and farther away). Most cameras used in surveillance are fixed. PTZ cameras are generally used to cover wider fields of views and should generally only be used if you expect a monitor to actively use the cameras on a daily basis. A key reason fixed cameras are generally used is that they cost 5 -8 times less than PTZs (fixed cameras average \$200 - \$500 USD whereas PTZ cameras can be over \$2,000 USD).
2. **Color vs Infrared vs Thermal:** In TV, a video can be color or black and white. In video surveillance today, the only time producing a black and white image makes sense is when lighting is very low (e.g., night time). In those conditions, infrared or thermal cameras produce

black and white images. Infrared cameras require special lamps (infrared illuminators) are fairly inexpensive for producing clear image in the dark. Thermal cameras require no lighting but produce only outlines of objects and are very expensive (\$5,000 - \$20,000 on average) In day time or lighted areas, color cameras are the obvious choice as the premium for color over black and white is trivial.

3. **Standard Definition vs. Megapixel:** This choice is similar to that of TVs. Just like in the consumer world, historically everyone used standard definition cameras but now users are shifting into high definition cameras. While high definition TV maxes out at 3 MP, surveillance cameras can provide up to 16 MP resolution. In 2008, megapixel cameras only represent about 4% of total cameras sold but they are expanding very rapidly. See a [demonstration of megapixel cameras](#) to learn more.
4. **IP vs Analog:** The largest trend in video surveillance today is the move from analog cameras to IP cameras. While all surveillance cameras are digitized to view and record on computers, only IP cameras digitize the video inside the camera. While most infrared and thermal cameras are still only available as analog cameras, you can only use megapixel resolution in IP cameras. Currently, 20% of cameras sold are IP and this percentage is increasing rapidly.

Most organizations will mix and match a number of different camera types. For instance, an organization may use infrared fixed analog cameras around a perimeter with an analog PTZ overlooking the parking lot. On the inside, they may have a fixed megapixel camera covering the warehouse and a number of fixed IP cameras covering the entrance and hallways.

## 2. Connectivity

In professional video surveillance, cameras are almost always connected to video management systems for the purpose of recording and managing access to video. There are two main characteristics to decide on for connectivity.

- **IP vs. Analog:** Video can be transmitted over your computer network (IP) or it can be sent as native analog video. Today, most video feeds are sent using analog but migration to IP transmission is rapidly occurring. Both IP cameras and analog cameras can be transmitted over IP. IP cameras can connect directly to an IP network (just like your PC). Analog cameras cannot directly connect to an IP network. However, you can install an encoder to transmit analog feeds over IP. The encoder has an input for an analog camera video feed and outputs a digital stream for transmission over an IP network. Learn more about the choice between [IP and analog transmission](#).
- **Wired vs Wireless:** Video can be sent over cables or through the air, whether you are using IP or analog video. Over 90% of video is sent over cables as this is generally the cheapest and most reliable way of sending video. However, wireless is an important option for transmitting video as deploying wires can be cost-prohibitive for certain applications such as parking lots, fence lines, remote buildings. Learn more about [when and how to use wireless video surveillance](#).

## 3. Video Management System

Video management systems are the hub of video surveillance solutions, accepting video from cameras, storing the video and managing distribution of video to viewers.

There are 4 fundamental options in video management systems. Most organizations choose 1 of the 4. However, as companies may have multiple types when they transition between one and another.

- **DVRs** are purpose built computers that combine software, hardware and video storage all in one. By definition, they only accept analog camera feeds. Almost all DVRs today support remote viewing over the Internet. DVRs are very simple to install but they significantly limit your flexibility in expansion and hardware changes. DVRs are still today the most common option amongst professional buyers. However, DVRs have definitely fallen out of favor and the trend is to move to one of the 3 categories below.
- **HDVRs** or hybrid DVRs are DVRs that support IP cameras. They have all the functionality of a DVR listed above plus they add support for IP and megapixel cameras. Most DVRs can be software upgraded to become HDVRs. Such upgrades are certainly a significant trend and is attractive because of the low migration cost (supports analog and IP cameras directly). Learn more about the [value and issues in selecting HDVRs](#).
- **NVRs** are like DVRs in all ways except for camera support. Whereas a DVR only supports analog cameras, an NVR only supports IP cameras. To support analog cameras with an NVR, an encoder must be used.
- **IP Video Surveillance Software** is a software application, like Word or Excel. Unlike DVRs or NVRs, IP Video Surveillance Software does not

come with any hardware or storage. The user must load and set up the PC/Server for the software. This provides much greater freedom and potentially lower cost than using DVR/NVR appliances. However, it comes with significant more complexity and time to set up and optimize the system. IP Video Surveillance Software is the hottest trend in video management systems currently and is the most frequent choice for very large camera counts (hundreds or more). Learn more about [choosing software only systems](#).

#### **4. Storage**

Surveillance video is almost always stored for later retrieval and review. The average storage duration is between 30 and 90 days. However, a small percentage of organization store video for much shorter (7 days) or for much longer (some for a few years).

The two most important drivers for determining storage duration is the cost of storage and the security threats an organization faces.

While storage is always getting cheaper, video surveillance demands huge amount of storage. For comparison, Google's email service offers about 7 GB of free email storage. This is considered to be an enormous amount for email. However, a single camera could consume that much storage in a day. It is fairly common for video surveillance systems to require multiple TBs of storage even with only a few dozen cameras. Because storage is such a significant cost, [numerous techniques exist to optimize the use of storage](#).

The type of security threats also impacts storage duration. For instance, a major threat at banks is the report of fraudulent investigations. These incidents are often not reported by affected customers until 60 or 90 days after the incident. As such, banks have great need for longer term storage.

By contrast, casinos usually know about issues right away and if a problem is to arise they learn about it in the same week. Casinos then, very frequently, use much shorter storage duration (a few weeks is common).

Three fundamental types of storage may be selected:

1. **Internal** storage is the hard drives that are built inside of a DVR, NVR or server. This today is still the most common form of storage. With hard drives of up to 1 TB common today, internal storage can provide total storage of 2TB to 4TB. Internal storage is the cheapest option but tends to be less reliable and scalable than the other options. Nonetheless, it is used the most frequently in video surveillance.
2. **Directly Attached** storage is when hard drives are located outside of the DVR, NVR or server. Storage appliances such as NAS or SANs are used to manage hard drives. This usually provides greater scalability, flexibility and redundancy. However, the cost per TB is usually more than internal storage. Attached storage is most often used in large camera count applications.
3. **Storage Clusters** are IP based 'pools' of storage specialized in storing video from large numbers of cameras. Multiple DVRs, NVRs or servers can stream video to these storage clusters. They provide efficient, flexible and scalable storage for very large camera counts. Storage clusters are the most important emerging trend in video surveillance storage. Learn more about [storage clusters for video surveillance](#).

## 5. Video Analytics

Video analytics scan incoming video feeds to (1) optimize storage or (2) to identify threatening/interesting events.

Storage optimization is the most [commonly used application of video analytics](#). In its simplest form, video analytics examines video feeds to identify changes in motion. Based on the presence or absence of motion, the video management system can decide not to store video or store video at a lower frame rate or resolution. Because surveillance video captures long periods of inactivity (like hallways and staircases, buildings when they are closed, etc.), using motion analytics can reduce storage consumption by 60% - 80% relative to continuously recording.

Using video analytics to identify threatening/interesting events is the more 'exciting' form of video analytics. Indeed, generally when industry people talk of video analytics, this is their intended reference. Common examples of this are perimeter violation, abandoned object, people counting and [license plate recognition](#). The goal of these types of video analytics is to pro-actively identify security incidents and to stop them in progress (e.g., perimeter violation spots a thief jumping your fence so that you can stop him in real time, license plate recognition identifies a vehicle belonging to a wanted criminal so you can apprehend him).

These video analytics have been generally viewed as a disappointment. While many observers believe that video analytics will improve, the video

analytics market is currently contracting (in response to its issues and the recession). Learn more about [the challenges of video analytics](#).

## 6. Viewing Video

Surveillance video is ultimately viewed by human beings. Most surveillance video is never viewed. Of the video that is viewed, the most common use is for historical investigations. Some surveillance video is viewed live continuously, generally in retail (to spot shoplifters) and in public surveillance (to identify criminal threats). Most live video surveillance is done periodically in response to a 'called-in' threat or to check up on the status of a remote facility.

4 fundamental options exist for viewing video.

- **Local Viewing** directly from the DVR, NVR or servers is ideal for monitoring small facilities on site. This lets the video management system double as a viewing station, saving you the cost of setting up or using a PC. This approach is most common in retailers, banks and small businesses.
- **Remote PC Viewing** is the most common way of viewing surveillance video. In this approach, standard PCs are used to view live and recorded video. Either a proprietary application is installed on the PC or a web browser is used. Most remote PC viewing is done with an installed application as it provides the greatest functionality. However, as web applications mature, more providers are offering powerful web viewing. The advantage of watching surveillance video

using a web browser is that you do not have to install nor worry about upgrading a client.

- **Mobile Viewing** allows security operators in the field to immediately check surveillance video. As responders and roving guards are common in security, mobile viewing has great potential. Though mobile clients have been available for at least 5 years, they have never become mainstream due to implementation challenges with PDAs/phones. Renewed interest and optimism has emerged with the introduction of the Apple iPhone. Learn more about how [Apple's iPhone is impacting video surveillance](#).
- **Video Wall Viewing** is ideal for large security operation centers that have hundreds or thousands of cameras under their jurisdiction. Video walls provide very large screens so that a group of people can simultaneously watch. This is especially critical when dealing with emergencies. Video walls generally have abilities to switch between feeds and to automatically display feeds from locations where alarms have been triggered.

## 7. Integrating Video with Other Systems

Many organizations use surveillance video by itself, simply pulling up the video management systems' client application to watch applications.

However, for larger organizations and those with more significant security concerns, this is an inefficient and poor manner to perform security operations. Instead, these organizations prefer an approach similar to the military's common operational picture (COP) where numerous security systems all display on a singular interface. Three ways exist to deliver such integration with video surveillance:

- **Access Control as Hub:** Most organizations have electronic/IP access control systems. These systems have been designed for many years to integrate with other security systems such as intrusion detection and video surveillance. This is the most common way to integrate video surveillance and relatively inexpensive (\$10,000 - \$50,000 USD). However, access control systems are often limited in the number and depth of integration they support.
- **PSIM as Hub:** In the last few years, manufacturers now provide specialized applications (called PSIM or physical security information management) whose sole purpose is to aggregate information from security systems (like video surveillance) and provide the most relevant information and optimal response policies. These applications tend to be far more expensive (\$100,000 - \$1,000,000 USD) yet support a far wider range of security manufacturers and offer more sophisticated features.
- **Video Management System as Hub:** Increasingly, video management systems are adding in support for other security systems and security management features. If you only need limited integration, your existing video management system may provide an inexpensive (yet limited) solution.

Learn more about options for [integrating video with other systems](#).

## Conclusion

If you feel comfortable with the key decisions to be made, you may want to start examining what companies provide the best products for your need. You can learn more about companies for each component at the [IP Video Market Companies Overview directory](#).

## **Chapter 2: Introduction to NVRs / IP Video Software**

IP Video Surveillance and Network Video Recorders (NVRs) are two of the most common terms describing the use of IP cameras and network based computers in physical security. Both of these terms are marketing phrases and are not controlled by a standards body. As such, no authoritative definition is possible and many diverging opinions are held. This article attempts to document the most agreed upon assumptions and highlight the most widely debated elements.

Moreover, a debate exists in the industry over what to call these solutions. Reflecting the legacy of DVRs, many call these systems NVRs. However, this term suggests hardware and proprietary appliances. Many feel strongly that these solutions should be open architecture and 'software only'. As such, many do not consider their products to be 'NVRs'. Frequently manufacturers refer to their products as "IP Video Management" solutions or "IP Video Surveillance" solutions. For purposes of brevity, I use the acronym "NVR" in this document instead of the long and unwieldy alternatives such as "IP Video Surveillance Software, etc". Do note that manufacturers feel very strongly about the naming of the categories their products are placed in. I would recommend you ignore the category names and focus on understanding the differences in benefits.

### **NVRs Must Support IP Cameras**

Almost everyone agrees that to be designated an NVR a solution must support IP cameras. Indeed, the network in "network video recorder" is generally accepted as referring to the use of an IP network to connect IP cameras to an NVR.

### **NVRs are Software Only Applications (DEBATED)**

Most NVR suppliers offer their products as software only. That is to say the NVR provides the user with files that are loaded on a computer of the user's choosing. The user does not have to purchase the hardware of the NVR supplier. This is widely considered to be a major benefit of NVRs and is referred to by [Milestone Systems](#) as [busting out of proprietary jail](#). Choosing your own hardware can reduce total costs and increase flexibility to design and deploy a system that best meets your needs.

However, many NVRs suppliers do offer appliances. Appliances in IT refers to bundles of hardware and software that you must purchase together. A cellular phone is a common example of an appliance. You cannot mix and match phone software from one supplier and load it on the hardware of another. On the small scale, companies such as [VideoProtein](#) offers appliances that offer the potential of reducing setup and installation complexity. On the large scale, companies such as [Steelbox](#) offer appliances with the potential of reducing costs and hardware necessary for deploying 100 or 1000s of cameras.

### **DVRs Cannot Support IP Cameras**

By generally accepted definition, a product referred to as a DVR does not support IP cameras. The digital in “digital video recorder” generally refers to analog camera feeds being converted to digital inside of the recorder and therefore not being sent over the IP network. By definition, a DVR can only support analog inputs. Therefore, a DVR can only support an IP camera if the video feed from the IP camera is first converted back to analog using a 'decoder.'

### **NVRs Support Analog Cameras by Encoders**

Encoders are appliances that converts the video feed from an analog camera into

an IP stream that can be transmitted over a computer network like an email or a “You Tube” video. Almost all NVRs support encoders. Commonly held benefits of encoders include:

- Allowing existing analog cameras to be used with NVRs
- Eliminating the use of proprietary coaxial, twisted pair or fiber networks

### **Some Systems are Both DVRs and NVRs (DEBATED)**

Some appliances support both IP cameras and directly connected analog cameras. Specifically, these appliances do not require encoders to support analog cameras. Analog cameras can be directly connected to the back of the appliance. This eliminates the need for encoders. Such appliances are generally referred to a hybrid DVR/NVRs. The main benefits cited for hybrid systems is that they can be cheaper than software only NVRs and that they ease the transition from analog cameras to IP cameras.

Many debate the validity of hybrid systems as true NVRs or IP Video Surveillance systems. Major concerns include the lock into proprietary hardware and the often incomplete choices of IP camera support and number of IP cameras a hybrid system can support.

### **All NVRs Support Certain Basic Functionalities**

It is widely agreed that all NVRs support certain basic functionalities:

- Record Video
- View Live Video
- Search for Recorded Video
- View Recorded Video

Conduct these functionalities from a remote computer

### **NVRs can Differ Significantly in Advanced Functionalities**

While all NVRs are software applications, the software functionalities that NVRs offer can vary significantly. This variance can appear between suppliers and even amongst supplier's offerings.

For instance, Milestone Systems offers [4 categories of IP Video Surveillance / NVR solutions](#) and a number of options. Examples of categories include:

- Basic: small camera systems, basic functionality
- Medium: medium camera systems, more advanced camera and system controls
- Multi-Site: large camera systems with servers in multiple locations
- Global: super-large camera systems with fail over and central management

While all versions offer basics like video recording, viewing and searching, different versions offer more powerful tools to improve reliability and usability as well as the number of cameras and locations supported. Likewise, significant differences can exist among NVR suppliers in the functionalities, reliability and scalability they offer.

NVRs can also differ in the types of options they offer. Examples include:

- Options for Different Verticals/Applications (Retail, Banking, Perimeter Protection)
- Options for Different Video Analytics (Virtual Tripwire, LPR, Facial

Recognition)

- Options for Access Control integration, Central Alarm Management integration, etc.

Not all suppliers will support all categories and options. So, even within NVR solutions, buyers must examine what combination of features are most relevant for the operational and security needs they possess.

### **Large and Growing Number of NVR Suppliers**

Worldwide, there are easily a few dozen suppliers of NVR solutions. That number is expected to grow as (1) DVR suppliers launch NVR offerings and (2) new entrants, attracted by growth, add offerings.

## **Chapter 3: Bandwidth Basics for Video Surveillance**

When using IP cameras, Megapixel cameras, NVRs or even DVRs, understanding the basics about how much bandwidth is available and how much is needed is critical in planning, designing and deploying IP video surveillance systems. Everyone in the industry should have an understanding of the basics as bandwidth is a critical factor in video surveillance

### **How Much Bandwidth is Available?**

To figure out how much bandwidth is available, you first need to determine what locations you are communicating between. Much like driving, you will have a starting point and destination. For example, from your branch office to your headquarters. However, unlike driving, the amount of bandwidth available can range dramatically depending on where you are going.

The most important factor in determining how much bandwidth is available is whether or not you need connectivity between two different buildings. For instance:

	<b>Bandwidth Generally Available</b>
Same Building	70Mb/s to 700 Mb/s
Different Buildings	.5 Mb/s to 5 Mb/s

The amount of bandwidth available going from your office to a co-worker's office in the same building can be 200 times more than the bandwidth from your office to a branch office down the block.

This is true in 90% or more cases. More bandwidth may be available in the following conditions:

- Different buildings but on the same campus
- In a central business district of a major city
- You are a telecommunications or research company

### **Different Buildings**

The key driver in bandwidth availability is the cost of deploying networks between buildings. Generally referred to as the Wide Area Network or WAN, this type of bandwidth is usually provided by telecommunications companies. One common example is cable modem or DSL, which can provide anywhere from .5 Mb/s to 5 Mb/s at \$50 to \$150 per month. Another example is a T1, which provides 1.5Mb/s for about \$300 to \$600 per month. Above this level, bandwidth generally becomes very expensive. In most locations, getting 10Mb/s of bandwidth can cost thousands per month.

Many talk about fiber but this will not be widely available for years. Fiber to the home (FTTH) or to the business promises to reduce the cost of bandwidth significantly. Nevertheless, it is very expensive to deploy and despite excited discussions for the last decade or more, progress remains slow. If you have it great, but do not assume it.

### **Same Buildings**

By contrast, bandwidth inside of buildings (or campuses) is quite high because the costs of deploying it are quite low. Non technical users can easily set up a 1000Mb/s networks inside a building (aka Local Area Networks or LANs) for less than \$1,000 installation cost with no monthly costs. Contrast this to the WAN, where the same bandwidth could cost tens of thousands of dollars per month.

The cost of deploying networks in buildings is low because there are minimal to no construction expenses. When you are building a network across a city, you need to get rights of way, trench, install on telephone poles, etc. These are massive projects that can easily demand millions or billions of dollars in up front expenses. By contrast, inside a building, the cables can often be quickly and simply fished through ceilings (not the professional way to do it but the way many people do it in deployments).

A lot of discussion about wireless (WiMax, WiFi, 3G, etc) exists but wireless will not provide significantly greater bandwidth nor significantly better costs than DSL or cable modem. As such, wireless will not solve the expense and limitations of bandwidth between buildings. That being said, wireless absolutely has benefits for mobility purposes and connecting to remote locations that DSL or cable modem cannot cost effectively serve. The point here is simply that it will not solve the problem of bandwidth between buildings being much more expensive than bandwidth inside of buildings.

### **How Much Bandwidth Do IP Cameras Consume?**

For the bandwidth consumption of an IP camera, use 1 Mb/s as a rough rule of thumb. Now, there are many factors that affect total bandwidth consumption. You can certainly stream an IP camera as low as .2 Mb/s (or 200 Kb/s) and others as high as 6 Mb/s. The more resolution and greater frame rate you want, the more bandwidth will be used. The more efficient the CODEC you use, the less bandwidth will be used.

For the bandwidth consumption of a Megapixel camera, use 5 Mb/s to 10 Mb/s as a rough rule of thumb. Again, there are a number of factors that affect total bandwidth consumption. A 1.3 megapixel camera at 1fps can consume as little as .8 Mb/s (or 800 Kb/s) yet a 5 megapixel camera can consume as much as 45

Mb/s.

### **What Does this Mean for my IP Video System?**

Just like dealing with personal finance, we can now figure out what we can 'afford':

	<b>Bandwidth Budget Available</b>
Between Buildings	.5 Mb/s to 5 Mb/s
Inside Buildings	70 Mb/s to 700 Mb/s

	<b>Bandwidth Cost</b>
IP cameras	1 Mb/s
Megapixel cameras	5 Mb/s to 10 Mb/s

Using this chart, we can quickly see what combination of IP and megapixel cameras we can use between buildings or inside of buildings.

1. Inside of buildings, it is easy to stream numerous IP and megapixel cameras.
2. Between buildings, it is almost impossible to stream numerous IP and megapixel cameras.

Because of this situation, the standard configuration one sees in IP Video systems is:

- A local recorder at each building/remote site. The local recorder receives the streams from the building and stores them.
- The local recorder only forwards the streams (live or recorded) off-site

when a user specifically wants to view video. Rather than overloading the WAN network with unrealistic bandwidth demands all day long, bandwidth is only consumed when a user wants to watch. Generally, remote viewing is sporadic and IP video coexists nicely with the expensive Wide Area Network.

- The local recorder has built-in features to reduce the bandwidth needed to stream video to remote clients. Most systems have the ability to reduce the frame rate of the live video stream or to dynamically reduce the video quality to ensure that the video system does not overload the network and that remote viewers can actually see what is going on the other side. Generally, the live video stream is sufficient to identify the basic threat. In any event, bandwidth is generally so costly, especially the upstream bandwidth needed to send to a remote viewer, that this is the best financial decision.

## **Conclusion**

Knowing how much bandwidth is available for DVRs and NVRs and how much bandwidth IP and megapixel cameras consume are key elements in planning and deploying viable IP video systems. Though this is simply a broad survey, my hope is that this helps identify fundamental elements in understanding the impact of bandwidth on IP video.

## **Chapter 4: Examining Video Analytics**

For 5 years now, the promise of using video analytics to stop trespassers crossing fences, catch thieves in stores, detect abandoned objects, etc has been a frequent topic of discussion.

While video analytics holds great promise, people are still asking about the viability of using analytics in the real world. Indeed, as stories of video analytic problems have spread, concerns about the risks of video analytics now seem higher than a few years ago when the novelty of the technology spurred wide excitement.

This article surveys the main problems limiting the use and growth of video analytics. It is meant to help security managers gain a better sense of the core issues involved.

Top 3 Problems:

1. Eliminating False Alerts
2. System Maintenance Too Difficult
3. Cost of System Too High

### **Eliminating False Alerts**

Since the goal of video analytics is to eliminate human involvement, eliminating false alerts is necessary to accomplish this. Each false alerts not only requires a human assessment, it increases emotional and organizational frustration with the system.

Most are familiar with burglar alarm false alarms and the frustration these cause. On average, burglar alarm false alarm per house or business are fairly rare. If you have 1 or 2 per month, that is fairly high. Many people do not experience false alarms of their burglar system for months.

By contrast, many video analytic systems can generate dozens of false alarms per day. This creates a far greater issue than anything one is accustomed to with burglar alarms. Plus, with such alarms happening many times throughout the day, it can become an operational burden.

Now, not all video analytics systems generate lots of false alarms but many do. These issues have been the number one issue limitation of the integrators and end-users that I know using and trying video analytics.

### **System Maintenance Too Difficult**

System maintenance is an often overlooked and somewhat hidden issue in video analytics.

Over a period of weeks or months, the number of a video analytic system's false alerts can start rising considerably due to changes in the environment, weather and the position of the sun. This can suddenly and surprisingly cause major problems with the system.

Not only is the increase in false alerts a problem, the risk now that the system could unexpectedly break in the future creates a significant problem in trust. If your perimeter surveillance one day stops functioning properly, you now have a serious flaw in your overall security plan.

This has been a cause of a number of video analytic system failures. The systems,

already purchased, simply are abandoned becoming a very expensive testament to not buying or referring one's colleagues to video analytics.

This being said, not all video analytic systems exhibit this behavior but you would be prudent to carefully check references to verify that existing systems have been operating for a long period of time without any major degradation.

### **Cost of System Too High**

While you can find inexpensive video analytic systems today, these systems tend to exhibit problems 1 and 2, high false alerts and poor system maintenance. Indeed, in my experience, video analytic systems that are either free or only cost \$100-\$200 more generally have significant operational problems.

One common feature of systems that work is that the complete price for hardware and software is usually \$500 or more per channel for the analytics. Now just because a video analytic system is expensive obviously does not mean it is good. However, there are necessary costs in building a systems that is robust and works well in the real world.

The cost of video analytic systems comes in making them robust to real world conditions that we all take for granted. The developer needs to make the video analytic system “intelligent” enough to handle differences in lighting, depth, position of the sun, weather, etc. Doing this involves building more complex or sophisticated programs. Such programs almost always require significantly more computing hardware to execute and significant more capital investment in writing, testing and optimizing the program. All of these clearly increase costs.

The challenge is that it is basically impossible to see this from marketing demonstrations because from a demo all systems invariably look exactly alike.

This of course has the vicious effect of encouraging people to choose cheaper systems that are more likely to generate high false alerts and be unmaintainable.

If you select a system that works, the cost per camera can make it difficult to justify the expense. Indeed, many of the first generation video analytic deployments came from government grant money, essentially making their cost secondary or not relevant. Nevertheless, for video analytics to grow in the private sector, they will not only need to work they will need to generate a positive financial return.

When video analytics allow for guard reduction or reduce high value frequent losses, it is easy to justify and you see companies having success here (in terms of publicly documented cases, [ioimage](#) is the leader here). For other cases, where humans are not being eliminated, the individual loss is small or the occurrence of loss is low, the cost can be a major barrier.

## **Conclusion**

Though I anticipate video analytics successes to increase, I believe such success will be constrained to applications where the loss characteristics and/or the human reduction costs are high. While analytics will certainly become cheaper, such cost decreases will take time and in the interim, it is these high value applications where analytics can gain a foothold of success.

Both testing and reference testing are critical to the use of video analytics.

## **Chapter 5: Wireless Video Surveillance Tutorial**

While wireless can uniquely solve certain challenges, it is far riskier to deploy and use than wired networks. As such, it is critical to understand when to use wireless systems and the key risks in designing such systems. If you use wireless networks prudently for video surveillance systems, the financial benefits can be quite significant. However, miscalculation in choice and design can result in significant reliability and scalability problems.

As a general rule, you should avoid using wireless networks unless wired networks costs are significantly higher than a wireless system. This is because deploying and maintaining wireless networks is far more risky and expensive than it is for a wired network. Wireless systems face much more serious problems than wired networks do such as constrained bandwidth, signal obstruction, higher maintenance cost and scalability restrictions.

### **Bandwidth**

Wireless networks have far lower bandwidth than wired networks. On a wired network, bandwidth available for video surveillance can be easily 70 Mb/s to 700 Mb/s. On a wireless network, your available bandwidth is often no more than 5 Mb/s to 25 Mb/s. It is a dramatic and often overlooked aspect of wireless video surveillance design.

Wireless video surveillance usually provide significantly less bandwidth than their nominal specifications. This is because the way bandwidth is calculated in wireless systems is the opposite of the more traditional wired approach. With a wired network, if you say you have 100 Mb/s bandwidth, this means you have

100 Mb/s going up and another 100 Mb/s going down. In a wireless network, if you say you have 11 Mb/s bandwidth, that is the total for both upstream and downstream. Some wireless systems are fixed to allow half the bandwidth for upstream and half for downstream. This is a big problem for video surveillance because almost all the bandwidth used is in one direction (upstream). Make sure your wireless system lets the upstream take up the whole bandwidth if needed. This is common with wireless systems dedicated to video but none in common commercial gear.

Environmental conditions often reduce the bandwidth further. Wireless networks are much more prone to effects from the environment than wired networks. Wireless networks will only achieve their maximum if the strength of the signal (signal to noise) is sufficiently high. If there are partial obstructions or if the antenna shifts slightly, the bandwidth from wireless systems can drop further. In our previous example, the 11 Mb/s wireless system only offers 5.5 Mb/s for streaming video. However, common environmental conditions can drop the bandwidth to 2.75 Mb/s.

### **Distance of Cameras**

It is quite hard to set up multi-mile wireless links to video surveillance cameras. A number of factors including obstructions, frequency limitations, power limitations, and installation precision drive this. Note: this tutorial assumes the use of unlicensed frequency, by far the most common choice for deploying wireless video systems. If you are using licensed frequency, where you can use much higher power and ensure no interference, these issues are not as significant. However, obtaining licenses are expensive and time consuming so most application use unlicensed spectrum. The rest of the discussion assumes unlicensed frequencies.

You are constrained in how powerful your signal can be, significantly reducing

the distance that you can transmit. The government restricts the power of your signal so that you do not drain out other users. However, this means it is much harder to push through obstacles and go greater distances. It also means that other users of the same frequency can reduce the bandwidth or block your signal. This is a major factor in the emergence of the 4.9 GHz range for use in video surveillance projects as that range is dedicated to public safety.

Obstacles are very serious problems for wireless video surveillance systems. Most wireless video surveillance system use frequency ranges that are easily absorbed by buildings and trees (2.4 GHz through 5.8 GHz). Practically speaking, you may want to transmit to a building 100 meters away but if another building is in between, the signal will be absorbed and the link will not be possible. You can and should use mesh networks to accommodate this but you must factor in the impact on the cost of the overall network.

Installation precision is key but issues can go wrong that may increase long term maintenance. Because of power restrictions, wireless video systems commonly use high gain antennas that increase signal power by concentrating it into a narrower area. This can help greatly in going longer distances or overcoming obstacles, however, it means the antennas must line up very precisely. If they do not, the performance of the system will degrade significantly. Also, if during the life of the system, either antenna shifts, the performance of the system could degrade 'out of the blue.'

### **Number of Cameras**

The number of cameras on a wireless system is severely constrained due to bandwidth limitations and constraints on how far cameras can be placed. For any given wireless connection, the maximum number of cameras that can be supported is generally between 5 and 15 with the cameras being less than a mile from the receiver. Even 'VCR' quality video using a good CODEC will take about

1 Mb/s. This is significant when you are dealing with wireless links that may only support 5 - 20 Mb/s. The total number of wireless cameras can be increasing by using multiple wireless connections or by combining wireless and wired networks.

A prudent practice is to use both wireless and wired networks with the wireless portion minimized to only the specific scenarios where deploying a wired connection would be cost-prohibitive. A typical example is getting a network drop in a building (either off the internal LAN or from a telco) and deploying a wireless link from the building to camera locations close to that building on poles or fence lines.

In any of these approaches, CODEC choice and resolution selection are key factors in the number of cameras that can be supported. In a wired network where 70 - 700 Mb/s networks are common, not compressing video heavily can work. However, in a wireless network, with 5 Mb/s to 15 M/bs available total, a single MJPEG standard definition camera could consume all of the available bandwidth by itself. Similarly, given the bandwidth constraints, megapixel cameras are especially challenging. Even with various optimizations, megapixel cameras can consume far greater bandwidth than standard cameras (assuming you use the same frame rate).

## **Conclusion**

Wireless networks can solve applications where wired networks are far too expensive. By relieving the need for expensive construction projects, video surveillance can be deployed in places where it would otherwise be cost prohibitive. However, wireless networks offer far greater challenges and risks in design and maintenance. As such, a clear understanding of these elements and when to prudently use wireless systems will contribute to successful wireless video surveillance systems.

## **Chapter 6: API and System Integration Tutorial**

APIs are the most frequently misunderstood and over-hyped aspects of physical security. While APIs can provide great benefits, using them is much more complex than often mentioned in sales calls and magazines.

The goal of APIs (or Application Programming Interfaces) in physical security is to allow different applications to work together. Examples include:

- Integrating your DVR/NVR with your access control system
- Integrating your alarm system with a central monitoring system
- Integrating your IP cameras or analytics with your NVR
- Building a PSIM system that integrates with all your security systems

You most commonly hear APIs discussed in pre-sales situations where a customer or integrator asks a vendor: "Does your system work with 'X'?" where X could be any number of security systems by any number of manufacturers.

The routine answer by the sales person is:

"Sure, we have an API."

For as long as I have been in security I have been hearing this response.

This is the most dangerous and misleading statement in all of physical security. Because it is so common and so dangerous, it is a great place to start reviewing APIs.

### **Lesson #1: No such thing as an API**

There is no such thing as an API. Numerous APIs exist. In larger systems, hundreds of APIs exist. Generally, there is an API for each function in a system. Want to watch live video, use the live video API. Want to change the time, use the time change API. Want to increase the frame rate for recording, use the recording frame rate API, etc.

### **Lesson #2: Not all Functions have an API**

Here's the first gotcha. Not all functions have an API available. Let's say you need to get a list of all health alerts from another application. This application may have 'an API' but not a specific API for sending health alerts. As you can imagine because most systems today have hundreds of functions, it is common that dozens of these functions are not accessible via an API.

### **Lesson #3: Having an API does not mean it will work with your system**

Let's say you have Genetec for your NVR and Software House for your access control. Both of these companies certainly have APIs but there is no guarantee that these two products will work together. Both companies having APIs is a prerequisite for integration but it is not sufficient. At least, both of these companies need to work together to ensure the integration works reliably. Many companies certify their API works with partners but frequently your product combination will not be included.

### **Lesson #4: Doing the Integration Takes Time**

Vendors often claim a few weeks for integration. This can happen but often technical details need to be worked out that can take significantly longer. Be careful in the time and dollar amount you commit for such projects. This is the

type of risk that is often unknown and unknowable until you dig into the technical details about how each vendor implements their APIs. Generally, these projects are ultimately successful, but the time and cost can vary.

### **Lesson #5: API Changes can Break You**

Just like a product, over time, APIs change. The difference is with APIs, their change can break your system. Reasons for change include eliminating bugs, enhancing performance, adding new functionality. Other system depend on the APIs staying the same. Let's say your system works with "Vendor B" version 3.1. Now let's say "Vendor B" comes out with 3.2 but this version "breaks the API". In other words, the new version is not backwards compatible with the old version. Your system could suddenly stop working with "Vendor B" if you upgrade Vendor B to version 3.2. The result is your security command center no longer displays video or access or whatever the system that just got the upgrade.

### **Lesson #6: You are Stuck with what the API does**

Unless you are a very large customer, you are stuck with whatever the API does in whatever way it does it. Often, for what you need, this works out fine. However, if you need some change for your specific use case, this can be hard to accomplish. Make sure someone on your technical team knows specifically what the API can and cannot do so you can anticipate any potential problems up front. If a change needs to be made, the change will usually take a lot of time and testing. This occurs not because people are slow but because the vendor must ensure that they do not break the 1000s of other security organizations using this API.

The use of APIs are certainly beneficial for physical security and their use will certainly grow. Understanding the realities of using APIs will ultimately help us maximize our value of system integration.



## **Chapter 7: How to Integrate Video With Other Systems**

It's tough and getting tougher to figure out the best approach to integrate video surveillance with other security systems. While the industry conversation centers on the value of integration, the real challenge is how to make this happen, effectively, cost-efficiently and simply.

This challenge is growing and is not simply the standard issues in technology selection and design. A few years ago, the options were fairly clear (if exceedingly limited). Or speaking more precisely, the *option* was fairly clear: The access control system functioned as the command center and the other systems, such as video feed into the access control's platform.

Today, we have three categories, contenders if you will, for the role of master application in security systems:

1. The Access Control System: the classic approach
2. The PSIM system: the emerging trend of deploying a dedicated application managing traditional security systems
3. The Video Surveillance System: a growing movement by video vendors to manage other systems

Which one do you choose? Which one is best? Which one will win?

### **Access Control**

Access control is the most well developed of the options available, having been fostered over the last decade. Most access control systems can interface with a variety of video management systems. Key advantages include the fact that almost everyone has access control and adding in the interfaces is fairly inexpensive. The main customer drawback of access control systems as the central platform is that they tend to limit 3rd party support to products that most

help their immediate sales. The largest incumbents such as GE, Tyco (Software House) and Honeywell have all been cited on these issues. Also, access control systems almost never support other access control system so if you need to support multiple access control systems, this generally will not work.

### **PSIM System**

While PSIM stands for the concept of managing physical security information, it also covers a group of companies that are building dedicated applications whose sole purpose is to manage security systems such as access control and video management systems. Notable vendors include [Orsus](#), [Proximex](#) and [Vidsys](#). Because they are not owned or controlled by access control or video vendors, they can and do offer a wide variety of support for different manufacturers. They also are optimizing their solution for large-scale security management rather than extending an existing access control system. The downside is that you have to buy a new product that is neither cheap nor trivial to implement (\$100,000 USD - \$1,000,000+ USD).

### **Video Management**

More and more, video management vendors are adding in PSIM functionalities into their system. For instance, [VideoNEXT](#), traditionally a video management vendor, is now marketing a video + PSIM solution. Verint's Nextiva and OnSSI's Ocularis are bringing in PSIM features such as mapping, third party system integration, workflow management, etc. A key advantage is that it can be cheap and easy to add functionalities into a User Interface that a customer may already be using. However, limited or no support of other video systems is an important downside. To make it even more confusing, two of the PSIM vendors, Orsus and Proximex, offer powerful video monitoring solutions that provide better large scale camera monitoring than many video management vendors.

### **Recommendations**

Making this decision is not easy as no single approach is broadly applicable. You

should start by investigating the abilities of your current access control system. This is probably the least costly and simplest way to do integration. If you have concerns with this approach (and you certainly may because it has limitations), I would then recommend investigating the PSIM providers. This will be expensive and complex but the probability for integrating all of your systems is high.

## II

# Examining Key Trends and Technologies

## **Chapter 8: *Should I Use IP Cameras?***

IP cameras have become accepted by the security industry. Yet most cameras are still analog and most video management systems are still DVRs. When and how do we make the transition? Is it a fast transition? When does a security manager, manufacturer or integrator know when to make the move?

Though the big picture seems settled, with much of the actual transition still come to, how to execute and navigate the transition becomes a critical business decision.

### **Key Strategic Points**

To help make this transition, here are 3 key strategic points that shape the timing and execution of transition tactics.

- The larger the facility being secured, the more valuable an immediate transition to IP cameras.
- The more mature megapixel cameras become, the more valuable an immediate transition to IP cameras.
- DVRs will continue to catch up to NVRs and will as such extend the life of analog systems.

This report examines these key strategic points and concludes with specific recommendations for integrators and end-users.

### **Strategic Point #1: The Larger the Facility**

The larger the facility being secured, the more valuable an immediate transition to IP cameras. It is not so much how many facilities but the size of each specific facility. Because of the intrinsic limitations of coaxial cable, when facilities become too large, the costs of system installation increase dramatically. Think of office towers, corporate campuses, military bases. Low cost coaxial cable runs could not solve the problem. Proprietary networks were needed.

The elimination of proprietary networks is the one advantage of IP cameras that dwarfs all others and has been driving IP cameras/encoders. This is where the business case is absolutely rock solid.

For large scale surveillance projects, you can save \$1,000 to \$4,000 per camera relative to analog long distance transmission systems. If you can eliminate trenching, the cost savings are even more dramatic.

It is no surprise that most of the biggest IP camera systems are among schools, corporate campuses, municipalities, the military. That's not to say that IP cameras are not deployed elsewhere but many if not most of the biggest success stories are in applications where long distances exist between cameras.

Likewise, we should not be surprised that quick serve restaurants, bank branches, small and medium size businesses and other organizations with small footprints are slow in the uptake of IP cameras. Coax works just fine there making the business case much harder to justify.

### **Strategic Point #2: The more mature megapixel cameras become**

Economically speaking, the increase in quality between standard definition IP cameras and analog cameras recorded by a DVR is minimal. The quality of IP cameras is certainly better but it is not so much better that many more crimes can be solved. Without a clear and sizable increase in such drivers, the quality of IP cameras does not drive IP adoption (that does not mean IP won't be adopted but it is more likely IP is adopted because of strategic point #1 and the quality is a nice throw in).

By contrast, megapixel cameras absolutely have the potential to solve more crimes. We are seeing the beginning of this with the use of megapixel cameras in casinos. By being able to show a level of detail impossible with analog cameras, losses are being prevented and mitigated, generating sizable business value to the organization.

However, the business case of megapixel cameras is still weak due to its increases in overall system cost. It is still very unclear when and how those costs and complexities will be overcome, triggering widespread mainstream adoption.

While megapixel has the potential, it is not yet actualized. This will hasten the transition but when and how?

### **Strategic Point #3: DVRs will continue to catch up to NVRs**

One of the most interesting and underappreciated elements in the transition to IP cameras is how DVR manufacturers have responded in this transition. This undoubtedly will continue, making it easier to extend the life of analog cameras.

Here are 5 areas where DVRs have traditionally been faulted in comparison to NVRs and how DVRs have narrowed the gap:

- **IP camera support:** Almost all mainstream DVRs have become hybrid systems supporting a wide variety of IP cameras. This trend will continue as the technical implementation is not very hard and customers clearly want the flexibility. While hybrid DVRs will not support as many brands of cameras as NVRs, the range of support is likely to be good enough for most users. And given, the deep installed base, hybrid DVRs will often have an economic advantage over system that require IP cameras or encoders.
- **Remote Access:** While early DVRs might have been limited in remote access, today all DVRs offer a variety of ways and functions for remote access including thick client and web access. From a customer's perspective, the difference between DVRs and NVRs will rarely be noticeable.
- **Scalability:** While NVRs had the early head start here, it is common for today's DVRs to be able to manage systems of thousands of cameras. DVRs offer health monitoring, centralized administration, virtual matrices, etc., etc. This is not a claim that DVRs are better or are somehow going to knock NVRs out. Simply that DVRs have addressed the key deficiencies making it hard for IP to win solely on this point.
- **Integrating Applications:** DVRs have always been strong at integrating with access control, intrusion detection, POS, ATMs, etc. I find claims by either side on this point to be more marketing hype than actual differentiation. I suspect most customers will see that either type supports their needs.
- **Analytics:** With the rise of hybrid systems and the continued increase in CPU speeds, DVRs are becoming powerful analytic platforms. The fact that DVRs are hybrid systems now means they can support the same OV or Io Image cameras that an NVR can. The fact that lots of extra CPU speed can be obtained in DVRs for minimal cost, means that DVRs are

going to be running analytics inside their systems. With dual and quad core becoming common place, the economics of performing analytics in DVRs are becoming very competitive relative to smart cameras.

So many of the core IP camera advantages have been co-opted by DVRs. Though it certainly will not stop IP cameras, this is going to make further inroads harder and reinforce the value of existing and replacement analog cameras.

### **Recommendations**

Let's start with general recommendations that apply across the industry and then examine specifically end-users and integrators.

#### **General Recommendation #1: The growth is in large facilities**

If you are looking to grow responsibilities in new areas, the growth area will certain be large facilities. Why? Because IP cameras change the business model of deploying cameras in large facilities and areas. Where once it was too expensive to deploy, IP is enabling new use of cameras.

We will certainly see this continue in schools, corporate campuses, municipalities, outdoor facilities, anywhere that long distances separate cameras from recording/ monitoring stations.

#### **General Recommendation #2: The absolute decline in analog cameras and DVRs will be slow**

Because DVRs are moving up and analog cameras will remain a good value for smaller facilities, expect the decline in the use of analog cameras and DVRs to be slow. In other words, it is very unlikely that they we will see a mass exodus from these system in the next 5 years. This should change as the price competitiveness of IP cameras increases and as NVR solutions become simpler to setup and

manage. However, this is a process that will evolve over a number of years.

**General Recommendation #3: Pay Close Attention to Megapixel Cameras**

Megapixel cameras are the wild card here. If and when the total cost of ownership (camera, bandwidth, storage) of megapixel cameras gets close to analog cameras, the financial incentive to switch to IP could become very strong. Right now, it is hard to tell when and how that will be happening. However, if you want to benefit from this transition, focus your energies on understanding and anticipating this emergence.

**Security Manager Recommendations**

For the 10 or 20% of you that are already all IP, continue course.

For the rest of you, your decisions should be driven by two factors:

1. Size of the facilities you manage: If they are small like quick serve restaurants or boutique retailers, take your time with IP, no rush. If the facilities are large, you want to move aggressively to IP.
2. The state of your DVR: Check the advances your DVR supplier is making. If they are making advances like going hybrid, supporting analytics, providing central management, etc., you will likely be in good shape for years to come. If they are not supporting this, you may be missing out on this generation's wave of operational savings and loss reduction. In this case, start investigating migration to a new IP based system.

## **Chapter 9: Value of Hybrid DVRs/NVRs**

Almost all security managers have DVRs. A minority have already moved to NVRs and some still use VCRs but 80% of security managers have DVRs today. As such, what to do with your DVRs and where to go next is a very critical question. Hybrid systems will be a key part of your solution.

Hybrid NVR/DVRs are appliances (purposed built computers) that can simultaneously support IP cameras and directly connected analog cameras. This provides simplicity and flexibility. Customers can start with their existing analog cameras and slowly migrate to IP. Specifically, unlike a 'pure' NVR, a hybrid NVR/DVR eliminates the need for a separate video encoder when connecting to analog cameras.

Hybrid NVR/DVRs are now being offered by almost all of the traditional DVR companies. However, many have questioned whether this meets a customer need or is done simply because it is easy for the traditional DVR companies to do.

Nevertheless, the hybrid NVR/DVR is quite legitimate and plays a critical role in very common scenarios in video surveillance:

- 80%+ of cameras today are analog and most of those cameras have many years of service left in them.
- In many applications (perhaps 30% or more of all systems), bandwidth constraints force customers to deploy recorders at the remote site near the on-site cameras.

In these scenarios, hybrid NVR/DVR systems will be very attractive. And since this scenario is very common, it will be a major factor for many security managers and the industry as a whole. To see why this will be a major factor, let's

examine general NVR benefits and why they are reduced in these scenarios.

A main benefit of a pure NVR is consolidation of video management and storage functionalities. Rather than managing video in chunks of 16 or 32 across potentially dozens of appliances, centralized servers and storage clusters can be used. These servers and storage clusters can reduce equipment cost, power consumption and service costs. Indeed, many of the early adopters of pure NVRs and IP video systems did so because of this advantage.

The biggest challenge in consolidation is bandwidth availability. Consolidating requires video feeds from various parts of a facility/facilities be transmitted to a central location(s). To do this, requires sufficient bandwidth. Inside the local area network (usually inside a building), bandwidth availability is plenty and fairly inexpensive. However, in the wide area network (usually between buildings or campus), bandwidth is scarce and quite expensive. To centralize video management and storage across the WAN could easily cost hundreds or thousands of dollars per month, negating the benefits of consolidation.

In many distributed facilities with 4 to 32 cameras, organizations will have to manage and store their local feeds in their local premises. This is, of course, not new as it is the common practice with DVRs. However, it does affect the NVR business case and create incentive to choose hybrid NVR/DVR systems.

### **Economic Comparison of Hybrid DVR/NVR to pure NVR**

When you have less than 32 cameras and you need to store and manage those cameras locally, the economics of hybrid NVR/DVRs are far better than pure NVRs.

A mid-tier 16 to 32 channel hybrid NVR/DVR costs about \$6,000 to \$8,000 (using online Google pricing for all estimates). The hybrid NVR/DVR does

encoding, storage, management and serving of the video, all in one, with minimal on-site setup and configuration.

By contrast, a pure NVR solution can cost 20% – 50% more than a hybrid system and is more complex to setup and maintain. The additional costs come from having to (1) purchase standalone encoders to convert the analog cameras to IP (\$200 to \$300 per camera), (2) purchase software licenses for the NVR(\$100 to \$150 per camera) and (3) purchase a PC/server with storage (\$75 to \$125 per camera). Additionally, the server needs to be set up, software loaded, OS tuned, encoders configured and connections established between encoders and NVR. It also takes more space, more IP addresses and because there are now multiple systems, increases the risk of integration or future service issues.

The NVR approach is much more complex and time consuming than the comparative hybrid NVR/DVR which is relatively plug and play. In a large scale environment where 100s of cameras were being consolidated, the cost savings often justify the additional complexity and setup time. However, in a small setup, the costs are quite significant.

### **Hybrid DVR/NVRs Provide a Smooth Transition**

For any given customer, the most attractive hybrid DVR/NVR will be the unit from their existing DVR supplier. Even if the customer does not especially like their DVR vendor, all of their staff is trained on using that DVR's client software. Moreover, often, all of the DVRs are from one vendor, so the staff never has to worry about which software client to use. The same client software for the DVR can usually be used for the hybrid systems. This makes the switch seamless and transparent to the users. Customer are willing to switch but when it's close, the comfort of the staff is a major factor in sticking with existing processes and products.

### **What's the Downside of Hybrid DVR/NVRs**

The biggest downside of Hybrid DVR/NVRs is that many are not truly hybrid. A genuine hybrid would be equally flexible with IP and analog. Mixing and matching many combinations of analog and IP would be standard. Supporting a variety of IP and megapixel cameras would also be standard. [Exacq](#) is a good example of a true hybrid. The problem is a lot of so called 'hybrid' systems offer only token support for mixing and matching and for different IP cameras. One common technique is to offer only a few additional IP cameras, constrained to 1 or 2 IP suppliers, in addition to the 16 analog inputs. [GE's Symdec](#) is an example of a "fake" hybrid. Hybrid systems are supposed to give you flexibility to grow into IP. This approach is more of a trick than a benefit.

## **Chapter 10: Examining 'Open' Systems**

While being “open” is the trend, “openness” is vague, claimed by all and underestimated in its difficulty to achieve. If you are buying or specifying video management systems, you need to carefully consider this.

Not too long ago, I was sitting with one of the most known and respected experts in CCTV. He expressed his frustration and dismay that a vendor who told him they were open were actually not. This was having a serious impact on systems he was designing. Now, if he could get caught by this, this could happen to any of us.

Here are the top 3 problems I see:

- "Openness" is vague - what does it actually mean?
- Everyone claims to be open - even if they are not really
- Being open is hard but it's routinely assumed as easy

Because of this, you may never know the truth and be stuck with a system that is locking you in.

### **Openness is Vague**

At a basic level, being open means that a system can work with other systems from different manufacturers. But how many other systems should a system work with to be called open? And how many other manufacturers do you need to work with to be called open?

Respected industry leaders often define openness as a vendor working with one or two other manufacturers in a single category. Certainly this is somewhat open but is it open enough? For most users, it is not and poses a big risk that when the day comes for you to [integrate with a different system or product that it just will not work.](#)

## **Everyone Claims to be Open**

To me, this is the most dangerous element in the 'openness' discussion. Politicians have learned that racism is no longer acceptable. So is the result that no politician is racist anymore? Of course not. The result is that politicians know to avoid racist language and make claims to racial equality. This is analogous situation with video surveillance systems.

Regardless of how closed a system is, all sales and marketing people know that you must claim to be open regardless of how open you really are. To publicly state to a client that you are not open is very risky so to solve that problem vendors simply claim that they are open. And because the commonly accepted definition of openness is so vague, it's easy to do it without reservation.

## **Openness is Hard**

It seems as if vendors simply will openness into existence; as if the act of saying you are open makes you open. It's backed up by the [absurd claim that "We have an API."](#) Though you need an API, simply having an API is just the beginning. It's like saying you are a Chef because you can barbecue hamburgers.

The reality is that truly being open takes a huge commitment from the vendor. It means optimizing your API to make it easier for other parties to use. It means doing custom integrations to support other people who use legacy technologies or are not as open. And perhaps most of all it means a huge development effort to actually support the hundreds of devices out there.

One of my favorite questions to ask is, "What products do you actually support today?" This smokes out a lot of spin and hype of 'open systems.' Most vendors take the approach that if it's theoretically possible for them to integrate with another product that they can claim to a customer that they support the product. Beware of this. Push for the details and smoke out the truth.

## **Conclusion**

As a first step, we all need to be careful about properly assessing openness. I also think we may need to start getting better definitions and assessments of how open systems are.

## **Chapter 11: The Danger of Buying Packages**

A dangerous and mass movement is underway for video surveillance companies to sell you packages. Packaging together cameras, encoders and IP video management systems, vendors hope to entice you with an integrated, optimized end to end solution.

One of the great ironies is that while everyone is paying lip service to open platforms, the industry is clearly moving to more tightly bundled packages. I think this is very risky and you should carefully consider the dangers of buying "~~solutions~~" "packages". Originally I called this solutions. I believe this is a poor choice of words. I have now changed to packages to better connote the phenomenon.

Who's selling packages? Verint, March, American Dynamics, Pelco, Cisco, DvTel, Bosch, IndigoVision, Avigilon. You can even see the beginning of this with Axis with their [expansion of Cam Station](#). Today, Panasonic announced it was [moving to selling "solutions", i.e packages](#). It's almost easier to ask who is not selling packages (Milestone being the most obvious large player). And what's key is that, 5 years ago, a lot of these companies specialized in just management systems or cameras. The trend is expanding.

Vendors love the thought of selling packages because it has the potential to increase revenue (by cross selling) and to increase margins (by bundling). They can also tell themselves that they have moved up market and are delivering greater value, etc, etc.

I do not doubt that some vendors can but when you have more than a dozen vendors all selling fundamentally the same package, you have a very risky situation for everyone involved.

### **Danger 1: Packages Are Too General**

Video surveillance buyers have a wide variety of needs. However, most packages are horizontally positioned (that is, they are not optimized for any specific use case). Packages can restrict flexibility and adaptability to different use cases. Be careful that the package properly addresses your need.

### **Danger 2: You are screwed if you choose a Market Lagging Package**

Since there are so many vendors selling packages, some of them are going to lose. You cannot expect to have a dozen companies all basically offering the same thing to all succeed. If you choose a packages that loses, you are in trouble. It will be very hard to expand the package and you will likely be locked in to its limitations.

### **Danger 3: You are controlled if you choose a Market Leading Package**

If the package wins, you become at the mercy of the vendor. This is why so much ill will exists towards companies like GE Security and Tyco. They got you into their package and they know it. Requests for supporting third party products or new features are slow or unlikely to be approved even if you are a giant customer. This move to IP video solutions seems to risk replicating the same problems we have been struggling with for the last decade.

I am not saying you should not buy packages. I think some of them are particularly strong (especially to the extent they focus on a vertical). However, you should clearly understand these moves and factor in the risks of them.

# III

# Evaluating New Products

---

## **Chapter 12: How to Read Marketing Material**

Almost all IP video info is vendor marketing. Good decision making requires critically reading and analyzing this material.

At first, I did not believe that most information was vendor marketing material. Obviously, web sites and press releases are marketing materials but you also have articles and reports from magazines. However, almost every article I find across a dozen magazines is written by a vendor (usually the head of marketing). Moreover, most of those articles are clearly promotion pieces for the vendor's offerings. They argue the merits of the trends behind their company's offerings with minimal attention or fair treatment of opposing views. Even news reports are routinely copies or excerpts of press releases.

As such, you really need to be careful and cognizant of the motivation and structure of the information you are reading. I have had to re-train myself to be more critical of what I read as I realize how consistently this is an issue. If you want to make good decisions and quickly discern what is the true value of what you are reading, I encourage you try the techniques I share here.

Better analysis of this information can really save you from mistakes or future problems.

At the same time, I am hoping vendor's consider modifying their marketing materials. As I will discuss throughout, in the long run, I believe all parties will benefit from clearer communication.

Here are my key recommendations for reading marketing material:

1. Determine how well the offering works
2. Determine what benefits the offering provides over the next best alternative
3. Determine what the cost of the offering is

### **1. How well it works**

Marketing material routinely speak in glowing terms of what their offering does. This is great for establishing the conceptual potential of a product, which is a necessary element of communicating value. It sets the stage for what is fundamentally different and what customers might expect to gain from the offering.

The problem is that it is so vague that it is impossible for readers to determine how well it fits for their environment. Most importantly, very rarely does the material discuss how well the offering works or how well it might work in different applications. I have seen this happen for 2 reasons: (1) the vendor is not sure which segment the product is a fit or (2) the vendor wants to launch the widest possible net and not lose any prospects. In either scenario, it becomes very hard for a reader to make a realistic determination of the fit for their needs.

I do not think this is ultimately beneficial for any of the parties. The vendor might get a short term win by an immediate sale. However, even for the vendor, it still could be a problem. If the deployment goes poorly (and often does if the fit is poor), the chances for repeat business and referrals is low. Essentially it becomes a very high cost sale that does not grow the long term market.

As a reader, you need to clearly ask yourself how well this offering will work. Consider what operational or environmental issues may undermine the project. Since it is unlikely you will get a clear and fair assessment from a vendor, you

need to do this yourself to make good decisions.

## **2. The next best alternative**

Most marketing material glosses over the benefits of your existing systems or processes. For instance, NVR vendors routinely claim benefits that any low end DVR can deliver. Megapixel vendors make assumptions about camera deployments that you would almost never use in deployment. Essentially, the comparisons are skewed to maximize the positive positioning of their products. (Note: this is not unique to any product category, NVRs and megapixel cameras are simply two of the big products of the day).

This causes confusion about the specific differentiators of the product offering. Truly innovative aspects can be lost in long lists of routine existing features and functionalities. End users can be motivated to purchase more complex or expensive products that do not truly generate more value for their organizations.

While it is hard for vendors to truly understand competitor's offerings deeply, more clearly and fairly stating actual advantages can help customers make better decisions more quickly. Though I honestly have little hope of this element changing, clearly considering what truly is a new benefit can help determine the actual value for your organization.

## **3. The cost of the offering**

Vendors rarely discuss costs of their offering. Generally, vague statements are offered like 'substantial ROI' or 'significantly increased value.' Vendors are justifiably concerned about interfering with their dealer's ability to set end user pricing. They are also often worried that disclosing price will scare off some

buyers and that it is better to promote their general benefits and handle pricing once the customer is engaged.

The huge downside of not discussing costs is that it's impossible for readers to determine 'value' or 'ROI'. Without having an idea of cost, by definition, you cannot calculate financial return. And it's not just a mathematical issue. This is a very practical issue as readers cannot discern whether an offering is feasible for their budgets. I see this all the time with articles on RAID, QoS, IP multicast, redundant servers. The costs for these features/products can be very expensive. It is hard for anyone to assess fit without having a ballpark sense of cost.

It would be very valuable if vendors provided rough costs for their products. It does not need to be a negotiated price, a simple MSRP would work fine. Readers need to know the general range pricing is in. For instance, is your megapixel camera close to \$500, \$1000, \$1500, \$2000? Setting an approximate range is good enough to allow a reader to assess how that would fit in their budgets and how much value the product would need to deliver.

Keeping these points in my mind when you read marketing material can help you better assess the true value of the offerings being promoted. Until marketing materials become more clear (if ever), applying this should help in evaluating this information.

## ***Chapter 13: How to Evaluate New Technology***

Most new technology fails but when it is successful, the business benefits can be enormous. The challenge then is how to efficiently determine what new technology is legit so that you simultaneously avoid disaster and reap the rewards of the rare gem.

You may have dozens of companies to review. Each new promising technology spurs the entrance of many companies hoping to enable the technology. So it's not just evaluating the technology, it's figuring out which companies, if any, has the winning solution.

You usually cannot make the evaluation based purely on your own knowledge. Most of the time when you are evaluating a new technology, you lack specific technical expertise in that area. As such, you need to figure out tactics and techniques to give yourself the best chance of projecting winners.

This article explores 5 key tips I have learned over the years working as an integrator and manufacturer. Here they are:

1. Verify Marketing Materials Provide Technical Details
2. Ask Specific Questions About Problems with the Product
3. Verify that the Vendor is not a Pathological Liar
4. Ask the Vendor how the product will work with all elements of your operations
5. Test Under Stress

### **Do the Marketing Materials provide Technical Details?**

The very first thing you should do is check how technical the marketing materials are. You do not need to know the technical jargon. At first, simply scan and notice how much of the marketing materials are prose (like an essay) versus how much are acronyms, numbers, diagrams, etc.

Few technical details are a strong indicator that the product is either conceptual or vaporware. Often, the lack of technical details arises because the company is promoting an idea but they are weak in engineering. Other times, their engineering is fine but the product is still so early that they have not gotten far enough to figure out a lot of the technical details.

I generally discard companies from further consideration that do not meet this criteria. On the other hand, just because a company does have technical details, does not mean it will definitely work. The company may be especially sophisticated in marketing or there may be more issues. As such, simply treat this as a first gate.

### **Are you asking Specific Questions about Problems?**

Most people will not lie to you but are OK with not telling you the truth. Since people are generally uncomfortable lying, a common tactic is to ignore discussing damaging issues. If you ask a vendor "How many companies are using your product in production?", most vendors will tell something close to the truth. If you do not ask anything, almost no one will volunteer that the product has never been deployed or only deployed at 1 or 2 sites. Strictly speaking, they are not lying to you but the outcome is similar because it leads you to believe incorrectly about a key element in the decision making process. Unlike mature products where it is

reasonable to take things for granted, this is a great risk with new technology products.

The challenge is new technology products always have problems. That does not mean you should not use them but you have to be aware of what those problems are. Be explicit and ask things like:

- How many sites have the product deployed?
- What was the cause of the last 3 failures of your product in the field?
- What was the cause of the product failing in previous pilots? (all products fail in at least some pilots)
- Can I have a reference? (Do not accept the excuse that they cannot tell you because of security issues. Any product with success has at least a few customers willing to talk, especially if you are a security manager.)

Just remember, do not takes things for granted, make sure to ask.

### **Is the Vendor a Pathological Liar?**

Pathological liars are a very dangerous force in new technology products. Every once in a while, a vendor will consistently spin and deflect any problems or criticisms. They will be so good that you will relax your guard and in your enthusiasm for the benefits of the problem will overlook problems. This is doubly dangerous. First, this undermines your due diligence but, secondly, and much worse, pathological liars usually have worse products because they are too busy spinning rather than building.

I experienced this when I was an integrator. We would go into meetings and this guy would consistently spin our offerings, deflecting any legitimate issues and

creating the perception of no risk and huge reward. One time, a customer asked a technical question like "Do you use Protocol X?" and this guy shot back "Of course." The customer, who was fairly technical, and myself were both taken aback. Unfortunately, what my colleague did not understand was that this was an outdated protocol that no one wanted to use anymore. When we left the meeting I asked him why he said that. His response was, "I was trying to tell them what they wanted to hear." Make sure vendors are not simply telling you what they think you want to hear.

The best tactic to handle this is to ask another person at the vendor (usually a technical person) questions away from the potential liar. Now most people know whether their colleagues are liars but they are going to be quite reluctant to say it directly. Talk to them about operational issues and ask this person direct questions. You will get a good sense of issues and discrepancies quite quickly this way.

### **How Does it affect the Elements of Your Operation?**

New technology products usually fail because of unforeseen operational issues. Generally it is fairly easy to figure out if the technology solves a business problem. On the other hand, it is very hard to determine what the operational issues you might have deploying and using this technology.

This is the most important step in evaluating new technology products. Regardless of whatever has been said or promised, regardless of the potential, how the technology impacts your operations makes or breaks its viability. Very often, the technology results in hidden increases in cost or can simply not be made to work with your existing systems or procedures.

You must make sure you understand how new technology interacts with existing

systems. You have existing systems and you want those systems to continue to work. You often find out that this technology does not work with a key component of your existing system. As an integrator, I once had a major problem designing a video analytic system because it did not integrate with the customer's existing matrix switch. A minor technical detail but it was a very serious operational issue. For all aspect of your system, go through them and make sure that there are no hidden operational incompatibilities.

Similarly, while it is easy to determine the direct cost of the new technology product, you must be careful about indirect costs this product might result in. Often new technologies will have requirements that cannot easily be met with your operations. This technology might require much greater amounts of bandwidth or client PCs that are much more powerful than your existing ones or significant amounts of training or maintenance. When you are estimating your costs, be sure to consider what the indirect costs can be - they often turn a promising project into an unrealistic one.

The technology may be good but not good enough for your business objectives. You have to be sure that it is truly good enough or you will cause a serious operational problem. Often, technology exists to automate existing processes managed by people. It is quite common that new technology can do a job 90% to 95% as good as a person. However, in many situations, from an operational or customer support standpoint, sacrificing that 5% or 10% can be a significant business problem. If you use facial recognition to verify a person coming through a door (automating access control guard verification), if that facial recognition system makes a mistake only 5% of the time, that can be 5 to 20 people a day that are frustrated. This might be a very good system and strong technology but it may not be good enough to meet the other business objectives or your organization.

If you do a careful assessment of system interoperability, indirect costs and conformance with business objectives and it passes, you are very likely to have a

winner.

### **How Does it work under Stress?**

One key way to determine how the new technology product affects your operations is by doing a pilot. Pilots are common so I only have 2 pieces of advice here.

One, make sure your pilot places the system under the highest level of stress you expect the product to be used at in production. Often, the test is done in a lab or in your office. This is a very bad idea. Office or lab test hide issues and works to the advantage of unscrupulous vendors.

How capable a product is to handling extreme conditions and loads is a very common difference between new and mature products. It takes a lot of time and experience for a product to incorporate real world challenges and be optimized for performance in extreme conditions.

Placing the product in your toughest operational environment is the best way to show how ready the product is for production use. This way, any shortcomings are exposed quickly rather than months later after the project is well under way and it is very hard to adjust.

Using new technology products is the most powerful way to generate a business advantage. If you are a security manager, it can enable you to truly stand out and advance in your career. If you are an integrator, it can drive incredible growth. I am a big proponent of using new technology products.

Making the right decisions about new technology products is critical. Consider

using these steps and hopefully you will be able to make better decisions in less time.

## **Chapter 14: How to Calculate Video Surveillance ROIs**

ROI calculations are powerful but can be distorted. While they hold the promise of identifying objective value, they can often obscure the truth.

The goal of this review is to help the security manager better understand supplier ROI calculations and allow the manager to modify or adjust for accurate and realistic results. Integrators and manufacturers could also benefit from applying these principles.

Good ROI calculation require understanding operational details more than they do math or money. Once you understand the operational details, the math and money are simple.

Here are the 4 principles in preparing a ROI calculation:

- Understand the alternative to this proposed investment
- Understand the full cost
- Understand the technological deficiencies of this investment
- Verify that operational assumptions are correct

### **Principle #1: Alternatives**

The most basic trick to play in ROI analysis is to choose an alternative that is clearly bad but not relevant to your case. Most vendor ROIs do this. One topical example is with NVRs. Frequently, NVRs make claims that they drive ROI by enabling centralized monitoring or integrating with applications like POS or access control. While certainly true, from an ROI perspective, this is irrelevant

because DVRs do the same things. It does not make sense for a security manager to compare an NVR to a VCR or to nothing because almost everyone has a DVR or would consider a DVR as an alternative to an NVR. To make a business case for the NVR, it needs to be compared to a DVR.

For instance, if an NVR cost "\$10,000" and a DVR cost "\$8,000", the investment for purpose of calculating the ROI would be \$2,000 (the premium for the NVR over the DVR). At the same time, the NVR could only claim returns on abilities that it uniquely has over the DVR, thereby eliminating from consideration aspects such as centralized monitoring and application integration. If you do not take this approach and simply calculate an ROI of an NVR versus a VCR, you could be wasting money by paying extra for an NVR when a DVR could have delivered the same value.

NOTE: I think NVRs often generate more value than DVRs so this is not a criticism of NVRs. This is a critique of the process often used to justify NVR purchasing decisions.

Megapixel camera suppliers often advocate camera elimination but this can sometimes distort ROI calculations. For instance, a recent whitepaper examined a scenario where 13 analog cameras could be replaced by (2) 3 Megapixel cameras for covering a 100 foot wide outdoor area. The paper concluded that the megapixel camera solution was actually cheaper. This assumption is misleading because the alternative here is really using 2 or 3 analog cameras. That is what most security managers use today and with that as the alternative the cost of the megapixel camera scenario is significantly higher than analog cameras.

NOTE: The megapixel cameras in this scenario may deliver much higher ROI by being able to solve previously unsolvable cases due to their greater quality. I am not objecting to the design, simply the method on how the financial justification was being made.

The security manager and megapixel vendor should concentrate on demonstrating the increased return delivered specifically by the enhanced image quality. Specifically, only cases solved with a megapixel camera that could not be solved by an alternative analog camera should be factored in the ROI for megapixel cameras. If identifying a license plate was critical in solving a case, the megapixel camera should get credit for it. But if the case could be solved by identifying that the car was a white Civic, an analog camera would be equally capable and the megapixel camera should not get credit.

This distinction is routinely blurred but if you are to truly determine an accurate ROI, this is a critical factor.

### **Principle #2: Understand the full cost**

Often, vendor supplied ROIs leave out indirect costs. These become hidden costs that can drag your true ROI down significantly.

One of the hidden costs of video analytics is the need for monitoring. Depending on the level of false alerts, you may need to dedicate resources to assess and verify the alerts. This cost could become quite significant. You may be able to get the technology to work as advertised but you may need to dedicate extra operational resources to bring it to that level. Make sure you understand what if any indirect costs are needed and factor this in.

Megapixel cameras are another example of indirect costs. With megapixel cameras, it is not only the increased camera cost but the increased cost of the storage and bandwidth. Almost all megapixel cameras in production use much more inefficient compression than analog cameras. Also, if you truly want enhanced resolution in megapixel cameras, this will further increase storage costs

(and often network costs).

Again, these both may be justifiable but a fair analysis most include any additional cost for them.

### **Principle #3: Technological Deficiencies**

When a vendor provides you an ROI, usually it assumes that the technology works as advertised. With new technology that sometimes turns out not to be the case. Also, sometimes, the technology works but not in the circumstances you need it in.

This is one of the key issues with video analytics. It is easy to say that perimeter violation has the potential to reduce losses significantly. However, it depends on how well it works. If it turns out that your facilities have a lot of snow, the system may not work properly during those times. This can reduce the potential loss reduction projected. Similarly, you may want to use a megapixel camera to capture license plates and faces in a very dark area at night. Many megapixel cameras work poorly with low light conditions. If you were projecting to solve cases during this time, this may not actually work.

Similarly, the system may turn out to be too hard to use so that your operators fail to solve as many cases as the technology might potentially deliver.

Carefully review what the vendor's projections are and make sure that any technological deficiencies are reflected in the ROI calculation.

### **Principle #4: Operational Assumptions**

Suppliers can only make best guesses as to the operational realities of a security manager. Often those guesses are very optimistic or simply do not match your organization's situation. Examples of these assumptions include loss per incident, number of incidents per month, number of incidences that this system will solve.

First, you need to ask and understand what these operational assumptions are in a vendor provided ROI. Compare that to your actual metrics and re-adjust to determine appropriate levels. How much time does the system really save you? How many incidents per year can you really solve with the new system that you could not with old?

It's probably going to differ from the vendor assumptions, so be ready to adjust the ROI calculations.

The challenge in all financial models is the assumptions made. By using these 4 principles, you can better assess and determine the right assumptions to make. Identify hidden costs and problems that a theoretical ROI may ignore and keep your suppliers honest.

Untangle common ROI confusions and distortions and you will be rewarded with an accurate ROI providing clarity on genuine business value.

**IPVideoMarket.info**

**Thank You.**

For more information, contact:

(646) 867-1965

info@ipvideomarket.info

[IPVideoMarket.Info](http://IPVideoMarket.Info)